Cyberscope

Audit Report

Baby Ape

April 2022

Table of Contents

Contract Review

Contract Name	BabyApe
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x9b7F20195A848072feaCB4D3A6A75e2BEb8F8CA1
Symbol	BAPE
Decimals	9
Total Supply	1,000,000,000
Domain	babyapeoriginal.com

Source Files

Filename	SHA256
contract.sol	b3622a28548de091f5ddaf4d2008ef49ed9329ea1abc3a31ea181ed72061f30b

Audit Updates

Initial Audit	27th April 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	medium
Location	contract.sol#L1055

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 `_maxTxAmount` or `_walletMax` to zero.

```
require(amount <= _maxTxAmount || isTxLimitExempt[sender], "tx");
//
require(_balances[recipient].add(amount) <= _walletMax, "wallet");
```

Recommendation

The contract could embody a check for not allowing setting the _maxTxAmount 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.

BC - Blacklisted Contracts

Criticality	critical
Location	contract.sol#L1051

Description

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

```
require(!bots[sender] && !bots[recipient]);
```

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
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L06	Missing Events Access Control
●	L07	Missing Events Arithmetic

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L425,433,802,806,836,890,897,905,922,929,948,971,995,1018,1038

Description

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

```
decreaseAllowance
increaseAllowance
transferFrom
approve
transfer
totalSupply
decimals
symbol
name
...
```

Recommendation

Use the external attribute for functions never called from the contract.

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L689,690,701,700,723,533

Description

Constant state variables should be declared constant to save gas.

```
dividendsPerShareAccuracyFactor
tradingStatus
launchedAt
hldFee
ZERO
DEAD
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L483,513,522,886,689,690,727,728

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.

```
_walletMax
_maxTxAmount
ZERO
DEAD
_distributorGas
RewardToken
_token
WETH
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L06 - Missing Events Access Control

Criticality	minor
Location	contract.sol#L869

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.

```
tokenOwner = newOwnerWallet
```

Recommendation

Emit an event for critical parameter changes.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L557,818

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.

```
lpFee = initialLpFee
minPeriod = newMinPeriod
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
Context	Implementation			
	_msgSender	Internal		
	_msgData	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		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
IBURNER	Interface			
	burnEmUp	External	Payable	-
IUniswapV2Factory	Interface			
	createPair	External	✓	-
IUniswapV2Router02	Interface			
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	removeLiquidityETH	External	✓	-
IDividendDistributor	Interface			
	setDistributionCriteria	External	✓	-
	setShare	External	✓	-
	deposit	External	Payable	-
	process	External	✓	-
DividendDistri	Implementation	IDividendDis		

butor		tributor		
	<Constructor>	Public	✓	-
	setDistributionCriteria	External	✓	onlyToken
	setShare	External	✓	onlyToken
	deposit	External	Payable	onlyToken
	process	External	✓	-
	shouldDistribute	Public		-
	distributeDividend	Internal	✓	
	claimDividend	External	✓	-
	getUnpaidEarnings	Public		-
	getCumulativeDividends	Internal		
	addShareholder	Internal	✓	
	removeShareholder	Internal	✓	
BabyApe	Implementation	Context, IERC20, IERC20Meta data		
	<Constructor>	Public	✓	-
	updateHldAdmin	Public	✓	onlyHldAdmin
	updateHldBurnerAddress	Public	✓	onlyHldAdmin
	setBots	External	✓	onlyHldAdmin
	changeFees	External	✓	onlyOwner
	removeHldAdmin	Public	✓	onlyOwner
	changeTxLimit	External	✓	onlyOwner
	changeWalletLimit	External	✓	onlyOwner
	changeRestrictWhales	External	✓	onlyOwner
	changeIsFeeExempt	External	✓	onlyOwner
	changeIsTxLimitExempt	External	✓	onlyOwner
	setDevWallet	External	✓	onlyOwner
	setLpWallet	External	✓	onlyOwner
	setOwnerWallet	External	✓	onlyOwner
	changeSwapBackSettings	External	✓	onlyOwner
	setDistributionCriteria	External	✓	onlyOwner
	delBot	External	✓	onlyOwner
	changeDistributorGas	External	✓	onlyOwner

	getCirculatingSupply	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	✓	
	_basicTransfer	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	
	takeFee	Internal	✓	
	swapBack	Internal	✓	lockTheSwap
	<Receive Ether>	External	Payable	-

Contract Flow
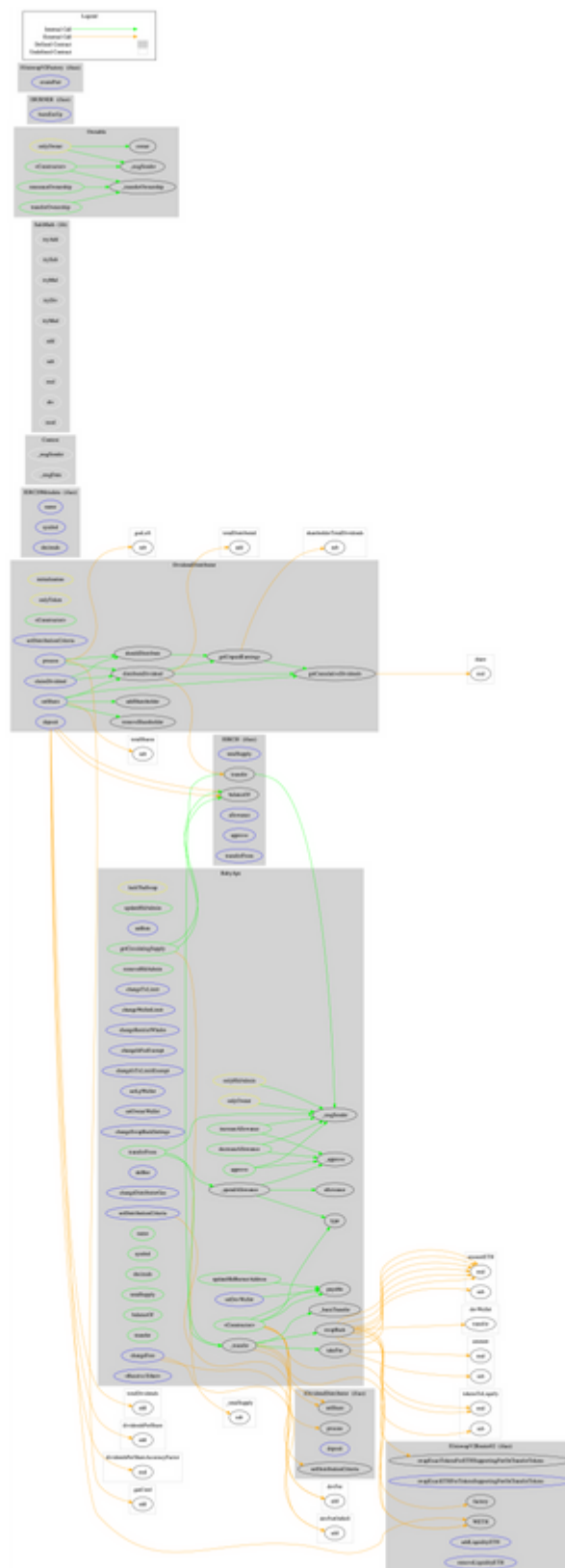
Domain Info

Domain Name	babyapeoriginal.com
Registry Domain ID	2687425410_DOMAIN_COM-VRSN
Creation Date	2022-04-07T00:48:33Z
Updated Date	2022-04-07T00:48:33Z
Registry Expiry Date	2023-04-07T00:48:33Z
Registrar WHOIS Server	whois.godaddy.com
Registrar URL	https://www.godaddy.com
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created 20 days before the creation of the audit. It will expire in 11 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 stopping transactions. The maximum fee percentage that can be set is 12% for purchases and 17% for sales. 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.

Cyberscope 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 Cyberscope 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 Cyberscope 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 Cyberscope team disclaims any liability for the resulting losses.

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

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.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provides all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io