Cyberscope

Audit Report

Baby Stepn

May 2022

Network	BSC
Address	0x883fc560d3be5c2a4f1dd9006d70ee5a17aae047
Audited by	© cyberscope

Table of Contents

Table of Contents 1
Source File 2
Source Files 2
Audit Updates 2
Contract Analysis 3
BC - Blacklisted Contracts 4
Description 4
Recommendation 4
Contract Diagnostics 5
L04 - Conformance to Solidity Naming Conventions 6
Description 6
Recommendation 6
L07 - Missing Events Arithmetic 7
Description 7
Recommendation 7
L14 - Uninitialized Variables in Local Scope 8
Description 8
Recommendation 8
Contract Functions 9
Contract Flow 13
Domain Info 14
Summary 15
Disclaimer 16
About Cyberscope 17

Source File

Contract Name	BABYSTEPN
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	Unlicense
Explorer	https://bscscan.com/token/0x883fc560d3be5c2a4f1dd9006d70ee5a17aae047
Symbol	$BABYSTEPN
Decimals	18
Total Supply	1,000,000,000
Domain	babystepn.io

Source Files

Filename	**SHA256**
contract.sol	d40f06cfc249e39c596221ae837f76b080e9c116162f8abe4ae21a02fd7df9f5

Audit Updates

Initial Audit	27th April 2022
Corrected	5th May 2022

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

BC - Blacklisted Contracts

Criticality	critical
Location	contract.sol#L486

Description

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

```
require(!isBlacklisted[sender] && !isBlacklisted[recipient],"Blacklisted");
```

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
	L04	Conformance to Solidity Naming Conventions
	L07	Missing Events Arithmetic
	L14	Uninitialized Variables in Local Scope

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L106,208,161,169,183,346,603,681,690,696,722,735,748,756,765,772,348,352,353,354,356,358,359,364,400

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.

```
maxFee
_markerPairs
_maxWalletAmount
_maxTxAmount
_totalSupply
_decimals
_symbol
_name
WBNB
...
```

Recommendation

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

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L208

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.

```
minPeriod = _minPeriod
```

Recommendation

Emit an event for critical parameter changes.

L14 - Uninitialized Variables in Local Scope

Criticality	minor
Location	contract.sol#L683

Description

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

```
i
```

Recommendation

All the local scoped variables should be initialized.

Contract Functions

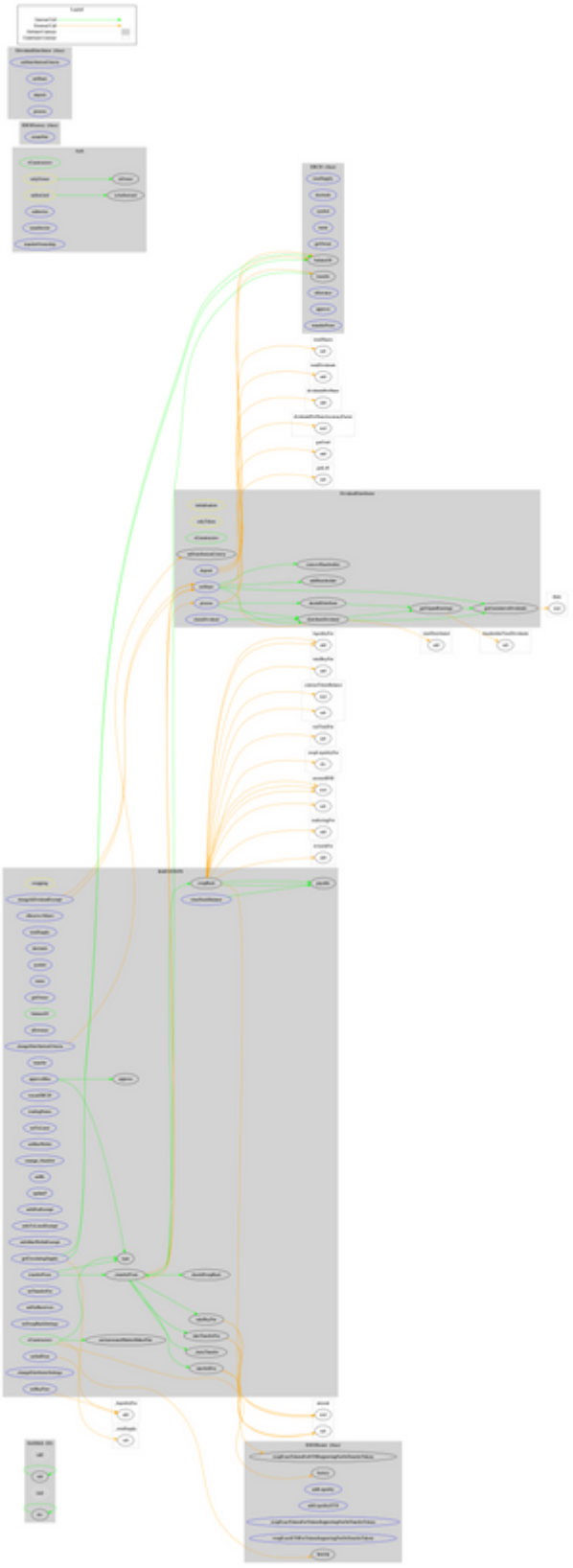
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
ERC20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Auth	Implementation			
	<Constructor>	Public	✓	-
	authorize	External	✓	onlyOwner
	unauthorize	External	✓	onlyOwner
	isOwner	Public		-
	isAuthorized	Public		-
	transferOwnership	External	✓	onlyOwner
IDEXFactory	Interface			

	createPair	External	✓	-
IDEXRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IDividendDistributor	Interface			
	setDistributionCriteria	External	✓	-
	setShare	External	✓	-
	deposit	External	Payable	-
	process	External	✓	-
DividendDistributor	Implementation	IDividendDistributor		
	<Constructor>	Public	✓	-
	setDistributionCriteria	External	✓	onlyToken
	setShare	External	✓	onlyToken
	deposit	External	Payable	onlyToken
	process	External	✓	onlyToken
	shouldDistribute	Internal		
	distributeDividend	Internal	✓	
	claimDividend	External	✓	-
	getUnpaidEarnings	Public		-
	getCumulativeDividends	Internal		
	addShareholder	Internal	✓	
	removeShareholder	Internal	✓	
BABYSTEPN	Implementation	ERC20,		

		Auth		
	<Constructor>	Public	✓	Auth
	<Receive Ether>	External	Payable	-
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	Public		-
	allowance	External		-
	approve	Public	✓	-
	approveMax	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	_transferFrom	Internal	✓	
	_basicTransfer	Internal	✓	
	takeBuyFee	Internal	✓	
	takeSellFee	Internal	✓	
	takeTransferFee	Internal	✓	
	shouldSwapBack	Internal		
	clearStuckBalance	External	✓	authorized
	rescueERC20	External	✓	onlyOwner
	tradingStatus	External	✓	onlyOwner
	swapBack	Internal	✓	swapping
	setTxLimit	External	✓	authorized
	setMaxWallet	External	✓	authorized
	manage_blacklist	External	✓	onlyOwner
	setBL	External	✓	onlyOwner
	updateF	External	✓	onlyOwner
	setIsFeeExempt	External	✓	authorized
	setIsTxLimitExempt	External	✓	authorized
	setIsMaxWalletExempt	External	✓	authorized
	setBuyFees	External	✓	authorized
	setSellFees	External	✓	authorized
	setTransferFee	External	✓	authorized

	setFeeReceivers	External	✓	authorized
	setSwapBackSettings	External	✓	authorized
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	changeIsDividendExempt	External	✓	authorized
	changeDistributionCriteria	External	✓	authorized
	changeDistributorSettings	External	✓	authorized
	getCirculatingSupply	External		-

Contract Flow



Domain Info

Domain Name	babystepn.io
Registry Domain ID	5b32c2b67b014e5bb71a72978c1ac962-DONUTS
Creation Date	2022-04-22T14:48:07Z
Updated Date	2022-04-22T14:48:07Z
Registry Expiry Date	2023-04-22T14:48:07Z
Registrar WHOIS Server	https://www.ascio.com/products/availability-check/whois
Registrar URL	http://www.ascio.com
Registrar	Ascio Technologies, Inc. Danmark - Filial af Ascio technologies, Inc. USA
Registrar IANA ID	106

The domain has been created 5 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

The Smart Contract analysis reported one critical severity issue. The contract owner has the authority to massively blacklist addresses. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats. There is also a limit of max 25% fees.

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

Cyberscope

Audit Report

Baby Stepn

April 2022

SHA256 da6f3ecaee613914f0ba81387fd8ba28aad688e2138f9c32db3b45433c814a14

Audited by © cyberscope

Table of Contents

Table of Contents 1
Source Files 3
Audit Updates 3
Contract Analysis 4
ST - Stop Transactions 5
Description 5
Recommendation 5
ELFM - Exceed Limit Fees Manipulation 6
Description 6
Recommendation 6
BC - Blacklisted Contracts 7
Description 7
Recommendation 7
Contract Diagnostics 8
L01 - Public Function could be Declared External 9
Description 9
Recommendation 9
L02 - State Variables could be Declared Constant 10
Description 10
Recommendation 10
L04 - Conformance to Solidity Naming Conventions 11
Description 11
Recommendation 11
L07 - Missing Events Arithmetic 12
Description 12
Recommendation 12

L11 - Unnecessary Boolean equality 13
Description 13
Recommendation 13
L14 - Uninitialized Variables in Local Scope 14
Description 14
Recommendation 14
Contract Functions 15
Contract Flow 19
Domain Info 20
Summary 21
Disclaimer 22
About Cyberscope 23

Source Files

Filename	SHA256
contract.sol	da6f3ecaee613914f0ba81387fd8ba28aad688e2138f9c32db3b45433c814a14

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	critical
Location	contract.sol#L561

Description

The contract owner has the authority to stop the sales or buys for all users excluding the owner. The owner may take advantage of it by setting the numerator denominator to the same value.

```
uint256 feeAmount = amount.mul(totalSellFee).div(feeDenominator);

_balances[address(this)] = _balances[address(this)].add(feeAmount);
```

Recommendation

Read more about the fees manipulation in the corresponding section.

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

Criticality	critical
Location	contract.sol#L732

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by setting a smaller value to the dominator in comparison to the enumerator.

```
function setSellFees(uint256 _liquidityFee, uint256 _marketingFee, uint256
_opsFee, uint256 _rewardsFee, uint256 _feeDenominator) external authorized {
    sellFeeLiquidity = _liquidityFee;
    sellFeeMarketing = _marketingFee;
    sellFeeOps = _opsFee;
    sellFeeRewards = _rewardsFee;
    totalSellFee =
_liquidityFee.add(_marketingFee).add(_opsFee).add(_rewardsFee);
    feeDenominator = _feeDenominator;
    require(totalSellFee <= maxFee, "Fees cannot be higher than 30%");

    emit SellFeesChanged(_liquidityFee, _marketingFee, _opsFee, _rewardsFee);
}
```

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	critical
Location	contract.sol#L486

Description

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

```
require(!isBlacklisted[sender] && !isBlacklisted[recipient],"Blacklisted");
```

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
	L07	Missing Events Arithmetic
	L11	Unnecessary Boolean equality
	L14	Uninitialized Variables in Local Scope

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L74,78,90,817

Description

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

```
getCirculatingSupply
transferOwnership
unauthorize
authorize
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L169,182,347,348,354,398

Description

Constant state variables should be declared constant to save gas.

```
maxFee
_totalSupply
ZERO
DEAD
dividendsPerShareAccuracyFactor
WBNB
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L105,207,160,168,169,601,679,688,694,720,732,744,752,761,768,346,347,348,350,351,352,356,357,362

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.

```
_markerPairs
_maxWalletAmount
_maxTxAmount
_decimals
_symbol
_name
ZERO
DEAD
WBNB
...
```

Recommendation

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

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L207

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.

```
minPeriod = _minPeriod
```

Recommendation

Emit an event for critical parameter changes.

L11 - Unnecessary Boolean equality

Criticality	minor
Location	contract.sol#L601

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
require(bool,string)(tradingEnabled == false,Can't pause trading)
```

Recommendation

Remove the equality to the boolean constant.

L14 - Uninitialized Variables in Local Scope

Criticality	minor
Location	contract.sol#L681

Description

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

```
i
```

Recommendation

All the local scoped variables should be initialized.

Contract Functions

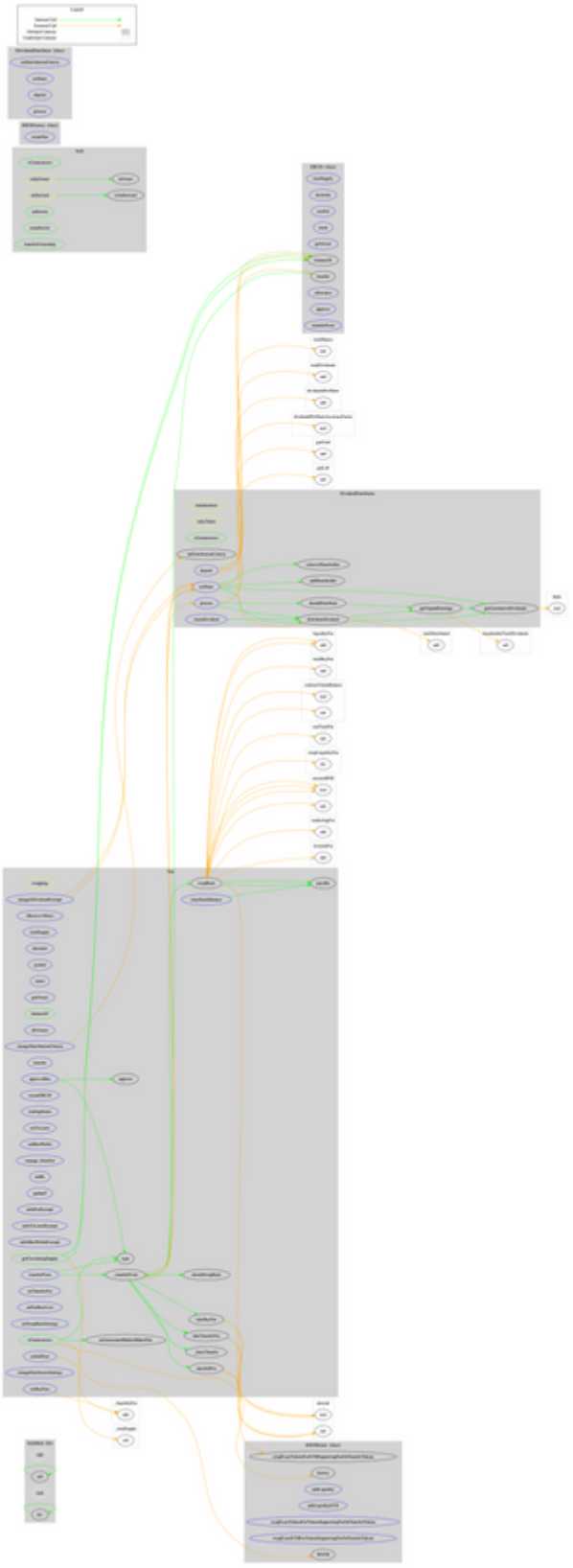
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
ERC20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Auth	Implementation			
	<Constructor>	Public	✓	-
	authorize	Public	✓	onlyOwner
	unauthorize	Public	✓	onlyOwner
	isOwner	Public		-
	isAuthorized	Public		-
	transferOwnership	Public	✓	onlyOwner
IDEXFactory	Interface			

	createPair	External	✓	-
IDEXRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IDividendDistributor	Interface			
	setDistributionCriteria	External	✓	-
	setShare	External	✓	-
	deposit	External	Payable	-
	process	External	✓	-
DividendDistributor	Implementation	IDividendDistributor		
	<Constructor>	Public	✓	-
	setDistributionCriteria	External	✓	onlyToken
	setShare	External	✓	onlyToken
	deposit	External	Payable	onlyToken
	process	External	✓	onlyToken
	shouldDistribute	Internal		
	distributeDividend	Internal	✓	
	claimDividend	External	✓	-
	getUnpaidEarnings	Public		-
	getCumulativeDividends	Internal		
	addShareholder	Internal	✓	
	removeShareholder	Internal	✓	
Test	Implementation	ERC20,		

		Auth		
	<Constructor>	Public	✓	Auth
	<Receive Ether>	External	Payable	-
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	Public		-
	allowance	External		-
	approve	Public	✓	-
	approveMax	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	_transferFrom	Internal	✓	
	_basicTransfer	Internal	✓	
	takeBuyFee	Internal	✓	
	takeSellFee	Internal	✓	
	takeTransferFee	Internal	✓	
	shouldSwapBack	Internal		
	clearStuckBalance	External	✓	authorized
	rescueERC20	External	✓	onlyOwner
	tradingStatus	External	✓	onlyOwner
	swapBack	Internal	✓	swapping
	setTxLimit	External	✓	authorized
	setMaxWallet	External	✓	authorized
	manage_blacklist	External	✓	onlyOwner
	setBL	External	✓	onlyOwner
	updateF	External	✓	onlyOwner
	setIsFeeExempt	External	✓	authorized
	setIsTxLimitExempt	External	✓	authorized
	setIsMaxWalletExempt	External	✓	authorized
	setBuyFees	External	✓	authorized
	setSellFees	External	✓	authorized
	setTransferFee	External	✓	authorized

	setFeeReceivers	External	✓	authorized
	setSwapBackSettings	External	✓	authorized
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	changeIsDividendExempt	External	✓	authorized
	changeDistributionCriteria	External	✓	authorized
	changeDistributorSettings	External	✓	authorized
	getCirculatingSupply	Public		-

Contract Flow



Domain Info

Domain Name	babystepn.io
Registry Domain ID	5b32c2b67b014e5bb71a72978c1ac962-DONUTS
Creation Date	2022-04-22T14:48:07Z
Updated Date	2022-04-22T14:48:07Z
Registry Expiry Date	2023-04-22T14:48:07Z
Registrar WHOIS Server	https://www.ascio.com/products/availability-check/whois
Registrar URL	http://www.ascio.com
Registrar	Ascio Technologies, Inc. Danmark - Filial af Ascio technologies, Inc. USA
Registrar IANA ID	106

The domain has been created 5 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

There are some functions that can be abused by the owner, like manipulating fees, stopping transactions and blacklisting contracts. The contract can be converted into a honeypot and prevent users from selling if the owner abuses the admin functions. The maximum fee percentage that can be set is 25%. 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