Cyberscope

Audit Report

Bitscrow

September 2022

Type	BEP20
Network	BSC
Address	0x9d55f5a65c4e8a7563a668c12364ecc42c4481a6
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	BitscrowToken
Compiler Version	v0.8.2+commit.661d1103
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x9d55f5a65c4e8a7563a668c12364ecc42c4481a6
Symbol	BTSCRW
Decimals	18
Total Supply	250,000,000
Domain	https://bitscrow.site

Source Files

Filename	SHA256
contract.sol	aa5ac4f26e41bba99296ce9c0f9b2d76cb7456b459d669a19d6978b70e5b0b88

Audit Updates

Initial Audit	23rd September 2022
Corrected	

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Contract Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	PITD	Proportional Initial Token Distribution	Unresolved
●	DFDP	Dev Funds Distribution Precision	Unresolved
●	RRAC	Redundant Role Access Check	Unresolved
●	L01	Public Function could be Declared External	Unresolved
●	L02	State Variables could be Declared Constant	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L05	Unused State Variable	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L09	Dead Code Elimination	Unresolved

PITD - Proportional Initial Token Distribution

Criticality	minor / informative
Location	contract.sol#L73
Status	Unresolved

Description

The initial token shares are distributed to the addresses in a fixed amount that is summed up to the total supply.

```
...
/* 18.4 % of the supply will be sent to the owner,
this funds will be entirely used for the presale on pinkswap,
and for the initial liquidity pool on pancakeswap */
uint initialownerbalance = 46000000 * 10 **18;
_balances[owner] = initialownerbalance;
emit Transfer(address(0), owner, initialownerbalance );
...
```

Recommendation

The contract could use proportional calculation in order to make the distribution more clear and more readable. For instance, instead of `46000000 * 10 **18` it could be `_totalSupply * 184/1000`

DFDP - Dev Funds Distribution Precision

Criticality	minor / informative
Location	contract.sol#L172
Status	Unresolved

Description

The dev funds distribution is divided into 3 equal shares. Since Solidity has not have floating types, then the result of a deviation may miss the decimals precision. As a result, the split shares will not have the exact precision and some funds may not be transferred as expected.

```
function DistributeDevsFunds()public  returns(bool success){
    require(msg.sender == TimelockedDevswallett);
    require(balanceOf(TimelockedDevswallett) == LOCKEDFUNDSDEVS);
    uint singleDevAmount = LOCKEDFUNDSDEVS  / 3 ;
    transferNoTax(msg.sender, dev1, singleDevAmount);
    transferNoTax(msg.sender, dev2, singleDevAmount);
    transferNoTax(msg.sender, dev3, singleDevAmount);

    LOCKEDFUNDSDEVS = 0;
    return true;
}
```

Recommendation

The contract could send the subtraction of the distributed funds in the last transfer in order to avoid the deviation rounding issue. For instance, the contract could calculate the last amount using a formula similar to: `transferNoTax(msg.sender, dev3, LOCKEDFUNDSDEVS - (singleDevAmount + singleDevAmount));`

RRAC - Redundant Role Access Check

Criticality	minor / informative
Location	contract.sol#L217
Status	Unresolved

Description

The isOwner modifier checks if the caller is the contract owner role. The statement `require(msg.sender == owner` also performs the same check. As a result, the check is performed twice.

```
function ChangeNoTaxAddress(address newWallet) public isOwner returns(bool) {
    require(msg.sender == owner, "you have to be the owner to change the no
tax address");
    noTaxWallet = newWallet;

    return true;
}
```

Recommendation

The contract could remove one of the two role access checks.

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contract.sol#L144,330,168,326,263,118,234,278,188,206,154,254,283,247,318,110,133,273,213,226,268,314,197,288,322,304
Status	Unresolved

Description

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

```
burn
currentTxFee
DistributeDevsFunds
declaredFee
name
transfer
ChangeTxFees
totalSupply
declareOwnerChange
...
```

Recommendation

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

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contract.sol#L144,330,168,326,263,118,234,278,188,206,154,254,283,247,318,110,133,273,213,226,268,314,197,288,322,304
Status	Unresolved

Description

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

```
burn
currentTxFee
DistributeDevsFunds
declaredFee
name
transfer
ChangeTxFees
totalSupply
declareOwnerChange
...
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor / informative
Location	contract.sol#L14,25,23,16,24,26,15,20,22,13,21
Status	Unresolved

Description

Constant state variables should be declared constant to save gas.

```
_symbol
dev2
stakingWallet
_MAXTXFEE
dev1
dev3
_decimals
marketingWallet
timelockedTokensWallet
...
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L213,288,21,309,33,154,30,144,168,234,16
Status	Unresolved

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.

```
ChangeNoTaxAddress
WarningTime
TimelockedDevswallett
Address
RequiredeDaysBeforeChange
_from
LOCKEDFUNDSDEVS
_value
DistributeDevsFunds
...
```

Recommendation

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

L05 - Unused State Variable

Criticality	minor / informative
Location	contract.sol#L15
Status	Unresolved

Description

There are segments that contain unused state variables.

```
_decimals
```

Recommendation

Remove unused state variables.

L07 - Missing Events Arithmetic

Criticality	minor / informative
Location	contract.sol#L247,226
Status	Unresolved

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.

```
_declaredWarningTime = newWarningTime
_declaredFee = newTxFee
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor / informative
Location	contract.sol#L414
Status	Unresolved

Description

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

```
transferToHolder
```

Recommendation

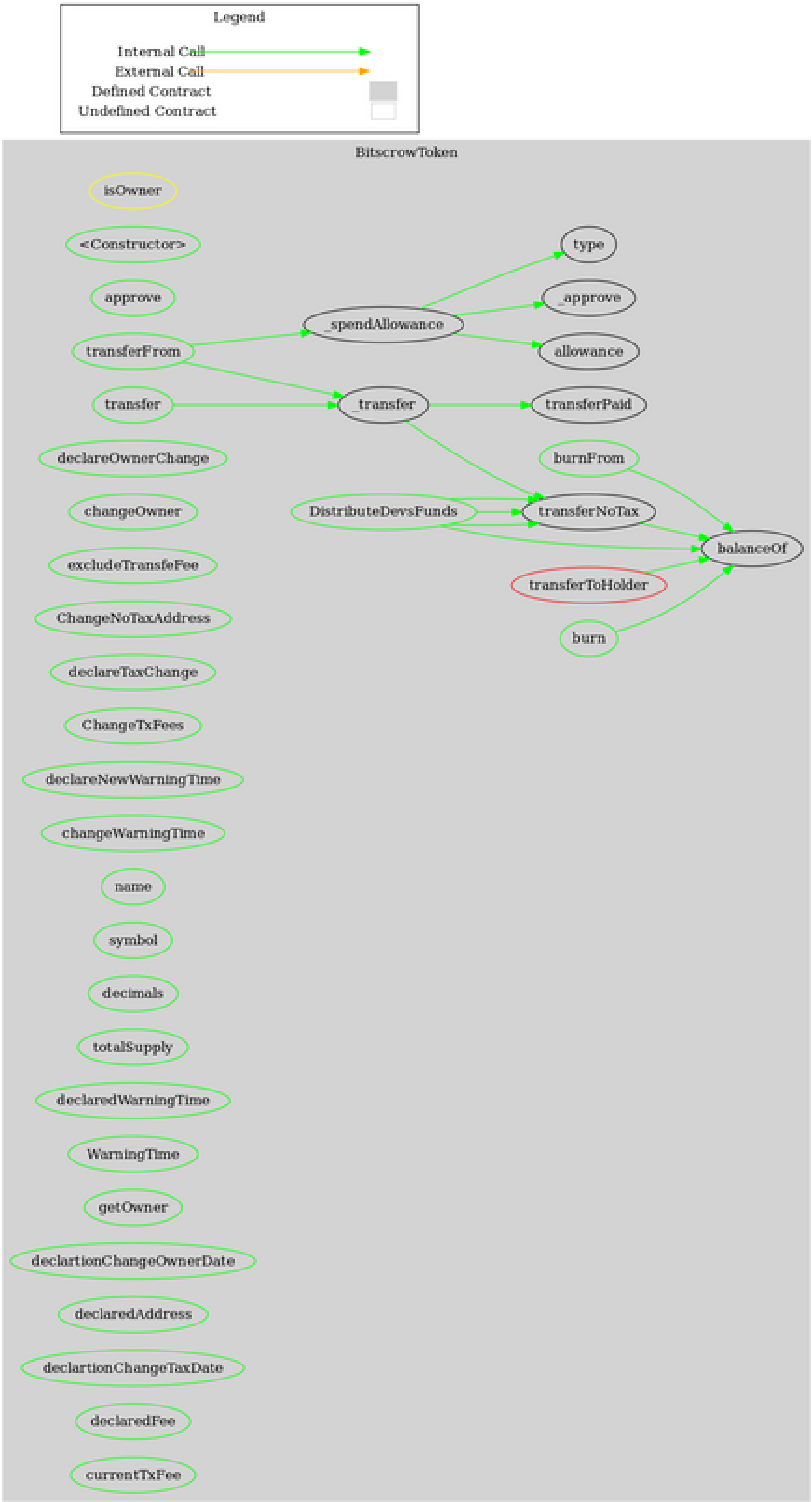
Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
BitscrowToken	Implementation			
	<Constructor>	Public	✓	-
	approve	Public	✓	-
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	burn	Public	✓	-
	burnFrom	Public	✓	-
	DistributeDevsFunds	Public	✓	-
	declareOwnerChange	Public	✓	isOwner
	changeOwner	Public	✓	isOwner
	excludeTransfeFee	Public	✓	isOwner
	ChangeNoTaxAddress	Public	✓	isOwner
	declareTaxChange	Public	✓	isOwner
	ChangeTxFees	Public	✓	isOwner
	declareNewWarningTime	Public	✓	isOwner
	changeWarningTime	Public	✓	isOwner
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	declaredWarningTime	Public		-
	WarningTime	Public		-
	allowance	Public		-
	getOwner	Public		-
	balanceOf	Public		-
	declartionChangeOwnerDate	Public		-
	declaredAddress	Public		-
	declartionChangeTaxDate	Public		-

	declaredFee	Public		-
	currentTxFee	Public		-
	transferNoTax	Private	✓	
	transferPaid	Private	✓	
	_transfer	Private	✓	
	_spendAllowance	Private	✓	
	_approve	Private	✓	
	transferToHolder	Private	✓	

Contract Flow



Domain Info

Domain Name	bitscrow.site
Registry Domain ID	D259615537-CNIC
Creation Date	2021-11-16T08:22:38+00:00
Updated Date	2021-12-23T12:07:24+00:00
Registry Expiry Date	2022-11-16T23:59:59+00:00
Registrar WHOIS Server	whois.1api.net
Registrar URL	http://www.1api.net
Registrar	1API GmbH
Registrar IANA ID	1387

The domain was created 10 months before the creation of the audit. It will expire in about 2 months.

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

Summary

Bitscrow is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 5% fees.

The contract implements a feature that warns the users about changes in the fees and in ownership. The contract initially states that in x period the change will be performed. If the x period is set to zero, then the feature will essentially be disabled.

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 provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io