Cyberscope

Audit Report

Baby ApeCoin

April 2022

Type	BEP20
Network	BSC
Address	0xf8aa749821852bc54ea5dd84dd3842d28523fc86
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	BabyApeCoin
Compiler Version	v0.7.6+commit.7338295f
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xf8aa749821852bc54ea5dd84dd3842d28523fc86
Symbol	BabyApe
Decimals	18
Total Supply	10,000,000,000
Domain	babyapecoinnft.com

Source Files

Filename	**SHA256**
contract.sol	a3ef5c5b3376d0c31c7b08da1651da8c6bdac3104d23a25d728ba992e536e146

Audit Updates

Initial Audit	11th April 2022
Corrected	21th April 2022

Contract Analysis

Critical Medium Minor Pass

Severity	Code	Description	Status
●	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	Renounced
●	BT	Contract Owner is not able to burn tokens from specific wallet	Renounced
●	BC	Contract Owner is not able to blacklist wallets from selling	

MT - Mint Tokens

Criticality	critical
Location	contract.sol#L851
Status	Renounced Ownership

Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the `mint` function. As a result the contract tokens will be highly inflated

```
    function mint(address _to, uint256 _amount) public onlyOwner {
        _mint(_to, _amount);
        _moveDelegates(address(0), _delegates[_to], _amount);
    }
```

Recommendation

The owner should carefully manage the credentials of the owner's account. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one. The owner could also renounce the contract ownership for a period of time or pass the access to the zero address.

Update 21 April

The contract owner has renounced the ownership. As a result the threat has been eliminated.

BT - Burn Tokens

Criticality	critical
Location	contract.sol#L742
Status	Renounced Ownership

Description

The contract owner has the authority to burn tokens from a specific address without checking for allowance of the user. The owner may take advantage of it by calling the `burn` function. As a result the targeted contract address will lose the corresponding tokens.

```
    function _burn(address account, uint256 amount) internal virtual {
        require(account != address(0), "ERC20: burn from the zero address");

        _beforeTokenTransfer(account, address(0), amount);

        _balances[account] = _balances[account].sub(amount, "ERC20: burn amount
exceeds balance");
        _totalSupply = _totalSupply.sub(amount);
        emit Transfer(account, address(0), amount);
    }
```

Recommendation

The owner should carefully manage the credentials of the owner's account. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one. The owner could also renounce the contract ownership for a period of time or pass the access to the zero address.

Update 21 April

The contract owner has renounced the ownership. As a result the threat has been eliminated.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L01	Public Function could be Declared External
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L212,219,238,247,253,258,565,582,589,616,627,663,682,857

Description

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

```
burn
decreaseAllowance
increaseAllowance
approve
allowance
totalSupply
decimals
symbol
acceptOwnership
...
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L851,857,1007,813,825

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.

```
_delegates
BabyApeInAdvance
_amount
_to
_from
```

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#L408,340,350,365,375,390,400,287,314,780

Description

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

```
_setupDecimals
sendValue
isContract
functionStaticCall
functionCallWithValue
functionCall
_verifyCallResult
...
```

Recommendation

Remove unused functions.

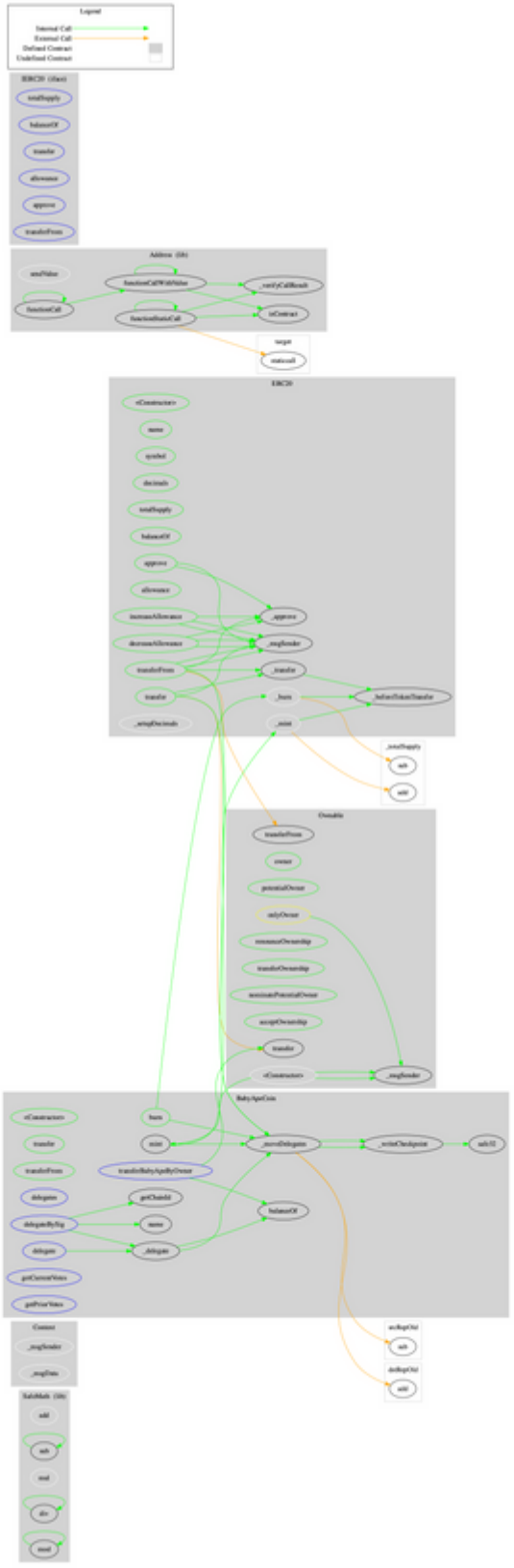
Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Internal	✓	
	owner	Public		-
	potentialOwner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	nominatePotentialOwner	Public	✓	onlyOwner
	acceptOwnership	Public	✓	-
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	

	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	_verifyCallResult	Private		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
ERC20	Implementation	Context, IERC20		
	<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	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_setupDecimals	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
BabyApeCoin	Implementation	ERC20, Ownable		

	<Constructor>	Public	✓	-
	mint	Public	✓	onlyOwner
	burn	Public	✓	onlyOwner
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	delegates	External		-
	delegate	External	✓	-
	delegateBySig	External	✓	-
	getCurrentVotes	External		-
	getPriorVotes	External		-
	transferBabyApeByOwner	External	✓	onlyOwner
	_delegate	Internal	✓	
	_moveDelegates	Internal	✓	
	_writeCheckpoint	Internal	✓	
	safe32	Internal		
	getChainId	Internal		

Contract Flow



Domain Info

Domain Name	babyapecoinnft.com
Registry Domain ID	2684690866_DOMAIN_COM-VRSN
Creation Date	2022-03-27T12:21:09.00Z
Updated Date	0001-01-01T00:00:00.00Z
Registry Expiry Date	2023-03-27T12:21:09.00Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain has been created 15 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

Baby ApeCoin is an interesting project that has a friendly and growing community. There are some functions that can be abused by the owner, like manipulating minting new tokens after initial deployment, and burning the tokens of a single user. The contract implements a typical governance feature that updates the voting power of the users according to their holdings. The governance feature does not disturb the token transactions. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

Update 21 April

The contract owner has renounced the ownership. As a result the threat has been eliminated.

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