Cyberscope

Audit Report

ApeSwap

March 2022

Commit e3fdaedc7442077c15075b999793d6b8a183d44a

Github https://github.com/ApeSwapFinance/apeswap-swap-core

Audited by © cyberscope

Table of Contents

Contract Review

Github	https://github.com/ApeSwapFinance/apeswap-swap-core
Commit	e3fdaedc7442077c15075b999793d6b8a183d44a

Pair Contract

Contract Name	ApePair
Compiler Version	v0.5.16+commit.9c3226ce
Optimization	200 runs
Licence	GNU GPLv3
Explorer	https://bscscan.com/token/0x7Bd46f6Da97312AC2DBD1749f82E202764C0B914
Symbol	APE-LP
Decimals	18
Total Supply	2,383,980

Factory Contract

Contract Name	ApeFactory
Compiler Version	v0.5.16+commit.9c3226ce
Optimization	200 runs
Licence	GNU GPLv3
Explorer	https://bscscan.com/token/0x0841BD0B734E4F5853f0dD8d7Ea041c241fb0Da6

Source Files

Filename	SHA256
ApeERC20.sol	4192d00e01f2b22514318b904493a6f10e09f222ddef9a4161e262d84e87d3b2
ApeFactory.sol	bf10168bef30753679997a4c8154100b9509db75612faf699a4bf10b266b5e61
ApePair.sol	c1fbb376efa9a5a9509c40c25391824c7a9b5936cebe647c6b100e7129a0e4bb
interfaces/IApeCallee.sol	15a42ba1b9dcb3c50704fc5d685f3ec90ade2562c90f5dfe2f52e0e3d2c1f01b
interfaces/IApeERC20.sol	71d67e6b7ac68e82e18d83ca892c699d4745d8574cc78774a2b096941a5ab56c
interfaces/IApeFactory.sol	ae1dd4557a21c16e00909290bcb980a4a6c3e4cf1f765c1426061e29b67e976f
interfaces/IApePair.sol	4358153e0c66071fee0897581a1bd6205009c41e12f334658baf3ab5b7f57bd2
interfaces/IERC20.sol	587de61c2ac2e289bd5f1a99a5ce3b1496559093538ea7435428e5a1512c8949
libraries/Math.sol	e4a9d451964a0689be2b244322a353de143ca4248d8736d91aca4ffadca4325f
libraries/SafeMath.sol	4b1c95ff75de7342e0fadff58064820a4eb7c2fcb422a75b4994980ce8e216ae
libraries/UQ112x112.sol	6633b57b0723b1d72e08cc3e8b29f0af838294e59863b6cdcce95a141ed02cdb

Audit Updates

Initial Audit	22nd March 2022
Corrected	

Contract Analysis

The ApeSwap features that are combined by the Factory and the Pair contract are:

- Pairs between ERC20 interfaces
- Price Oracle
- Fast assets transaction
- Fees distribution to the liquidity providers

This audit focuses on the pair contract that stores liquidity providers' funds and the factory contract used to instantiate pair contracts.

Price Oracle

The approximate price that is provided by Apeswap is a heuristic that takes in account the reserves of the two tokens and the time elapsed since the last swap.

To compute the average price given two cumulative price observations, take the difference between the cumulative price at the beginning and end of the period, and divide by the elapsed time between them in seconds.

Pairs contain both `price0CumulativeLast` (First token) and `price1CumulativeLast` (second token), which are ratios of reserves of token1/token0 and token0/token1 respectively. The price of token0 is expressed in terms of token1/token0, while the price of token1 is expressed in terms of token0/token1.

Liquidity Providers

ApeSwap implements an automated liquidity protocol. Every ApeSwap pair contains a pool of two tokens and provides liquidity.

There is a 0.3% fee for swapping tokens. This fee is split by liquidity providers proportional to their contribution to liquidity reserves.

Swapping fees are immediately deposited into liquidity reserves. This increases the value of liquidity tokens, functioning as a payout to all liquidity providers proportional to their share of the pool. Fees are collected by burning liquidity tokens to remove a proportional share of the underlying reserves.

traders will continue to pay a 0.30% fee on all trades; 83.3% of that fee (0.25% of the amount traded) will go to liquidity providers, and 16.6% of that fee (0.05% of the amount traded) will go to the feeTo address

Transfers permit

Users can authorize a transfer of their pool shared with a signature. Hence, user's may use this signature by calling the permite function.

All the ApeSwap pool tokens support meta-transaction approvals via the permit function. This obviates the need for a blocking approved transaction before programmatic interactions with pool tokens can occur.

In pure ERC20 implementations, the owners may only register approvals by directly calling a function which uses msg.sender to grant permission itself. In contrast, meta-approvals, ownership and permissioning are derived from a signature passed into the function by the caller. Because signing data with private keys is complicated, ApeSwap relies on the ERC712 protocol, a signature standard with widespread community support, to ensure user safety and wallet compatibility.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L04	Conformance to Solidity Naming Conventions
	DSV	Different Solidity Versions
	MZC	Missing Zero Check

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract/ApeERC20.sol#L26 contract/interfaces/IApeERC20.sol#L28,29 contract/ApeFactory.sol#L52,57 contract/ApePair.sol#L76 and 1 more files

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.

```
MINIMUM_LIQUIDITY
PERMIT_TYPEHASH
DOMAIN_SEPARATOR
_token1
_token0
_feeToSetter
_feeTo
...
```

Recommendation

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

DSV - Different Solidity Versions

Criticality	minor
Location	contract/ApeERC20.sol#L1 interfaces/IApeERC20.sol#L1

Description

Different pragma directives are used

```
pragma solidity =0.5.16;
pragma solidity >=0.5.0;
```

Recommendation

Use one Solidity version.

MZC - Missing Zero Check

Criticality	minor
Location	contract/ApePair.sol#L76

Description

Some parameters should be checked to not equal with the zero address.

```
function initialize(address _token0, address _token1) external {
    require(msg.sender == factory, 'ApeSwap: FORBIDDEN'); // sufficient check
    token0 = _token0;
    token1 = _token1;
}
```

Recommendation

Check that the address is not zero.

Contract Functions

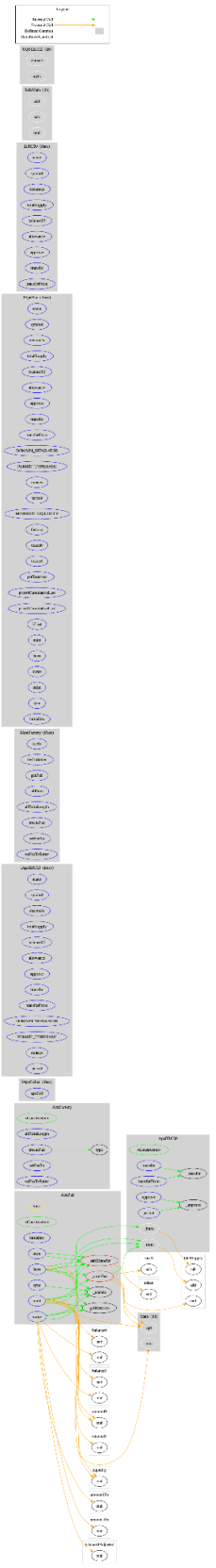
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
ApeERC20	Implementation	IApeERC20		
	<Constructor>	Public	✓	-
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Private	✓	
	_transfer	Private	✓	
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	permit	External	✓	-
ApeFactory	Implementation	IApeFactory		
	<Constructor>	Public	✓	-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
ApePair	Implementation	IApePair, ApeERC20		
	getReserves	Public		-
	_safeTransfer	Private	✓	
	<Constructor>	Public	✓	-
	initialize	External	✓	-
	_update	Private	✓	
	_mintFee	Private	✓	
	mint	External	✓	lock
	burn	External	✓	lock
	swap	External	✓	lock

	skim	External	✓	lock
	sync	External	✓	lock
IApeCallee	Interface			
	apeCall	External	✓	-
IApeERC20	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
IApeFactory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IApePair	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-

	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
IERC20	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-

Math	Library			
	min	Internal		
	sqrt	Internal		
SafeMath	Library			
	add	Internal		
	sub	Internal		
	mul	Internal		
UQ112x112	Library			
	encode	Internal		
	uqdiv	Internal		

Contract Flow



Summary

ApeSwap is a decentralized exchange that offers a wide variety of services. It provides a full suite of tools for users and partners to take advantage of decentralized finance opportunities. Cyberscope's audit focuses on the Pairing and Factory features. The audit investigates the main features, mentions security recommendation, performance improvements and potential optimizations.

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