Cyberscope

Audit Report

SpaceRace Miner

April 2022

Type	BEP20
Network	BSC
Address	0xf49E9665F9f54FC3d1aEa6Bf558B1031c0676944
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	SapceRace
Compiler Version	v0.8.9+commit.e5eed63a
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xf49E9665F9f54FC3d1aEa6Bf558B1031c0676944
Domain	space-race.money

Source Files

Filename	**SHA256**
contract.sol	ad605c88ed2abe5c2611d6454696efac6a701419e89074445c8a7781273203cb

Audit Updates

Initial Audit	21st April 2022
Corrected	

Contract Analysis

- The users have the ability to buy spaces by paying in the native currency.
- The price of spaces depends on some variations like the current spaces supply and the SpaceRace contract's native currency balance.
- The buy and sell amount is taxed by 5% dev fee, the taxed amount is moved directly to dev wallet.
- The users gathered spaces in order to redeem miners.
- The redeem process is called "hatchSpaces".
- During the hatch process the referred user takes 8% of the user's spaces as a reward.

Contract Diagnostics

🔴 Critical 🟠 Medium ● Minor

Severity	Code	Description
●	DPN	Deterministic Pseudo-Random Number
●	CBD	Contract Balance Dependency
●	IAD	Initial Amount Distribution
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L07	Missing Events Arithmetic
●	L13	Divide before Multiply Operation

Deterministic Pseudo-Random Number

Criticality	minor
Location	contract.sol#L475

Description

The determinism of the Blockchain prohibits the entropy required to make a pseudo-random number as random as possible. The randomization logic should implement a number of variants in order to make the pseudo-random generation as spreaded as possible. The SpaceRace contract is using a very simple technique that combines only the block.difficulty and block.timestamp. Thus, it can be easily manipulated by the users under some specific circumstances. This method can potentially affect the hatchSpaces and sellSpace.

```
function rand(uint256 _length) internal view returns (uint256) {
    uint256 random = uint256(
        keccak256(abi.encodePacked(block.difficulty, block.timestamp))
    );
    return random % _length;
}
///
uint256 r = SafeMath.rand(100);
if (r < HACTH_PERCENT) {
    newMiners = 0;
    coinState[raffleTicket] = 2;
} else {
    newMiners = newMiners * 2;
    rewardsMiner[msg.sender] = SafeMath.add(
        rewardsMiner[msg.sender],
        newMiners
    );
    coinState[raffleTicket] = 1;
}
```

Recommendation

The contract should implement a more complex randomization algorithm with more variables in order to hardener the potential manipulations. The contract could also

use a third-party on-chain solution like
https://docs.chain.link/docs/get-a-random-number/

Contract Balance Dependency

Criticality	minor
Location	contract.sol#L398

Description

The calculation of the sell and buy price heavily depends on the SapceRace contract's amount. That means that the same amount of spaces can be bought and sold at quite different prices according to the contract's balance. This calculation may be abused by the users and produce unexpected results in the financial ecosystem.

Below is the calculated spaces quantity as a result of the amount, contract balance and spaces supply:

Amount	Contract Balance	Supply	Result
1	1000000	108000000000	107999.8
10	1000000	108000000000	1079989.2
100	1000000	108000000000	107892107.8

The following is the same amounts with different contract balance:

Amount	Contract Balance	Supply	Result
1	1000	108000000000	107892107.8
10	1000	108000000000	857142857.1
100	1000	108000000000	9818181818.1

Recommendation

The contract could exclude the contract’s balance from the price calculations or use a weight in the calculations so it cannot heavily affect the prices.

Initial Amount Distribution

Criticality	minor
Location	contract.sol#L475

Description

The price calculations depend on the initial contract’s funds.

For instance, if the contract’s funds are less than the acquisition funds, then the purchase will not be able to complete since the calculation will underflow.

```
uint256 spacesBought = calculateSpacesBuy(
    msg.value,
    SafeMath.sub(address(this).balance, msg.value)
);
```

Recommendation

The contract should check if the contract’s amount is sufficient in order to proceed with the buy and sell methods.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L296,305,405,449,455,511,539,551,555,559,566,570,574,578,582,586,590,594,614,618

Description

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

```
getCoinResult
getUserCount
getMyMiners
getBalance
getRaffleLimit
getCoinSellState
getCoinHatchState
setCoinSellState
setCoinHatch
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L336,337,333,334,332,357,335

Description

Constant state variables should be declared constant to save gas.

```
devFeeVal
devAdd
SPACES_TO_HATCH_1MINERS
PSNH
PSN
HACTH_PERCENT
BOOST_PERCENT
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L117,332,333,334,336,337

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.

```
HACTH_PERCENT
BOOST_PERCENT
PSNH
PSN
SPACES_TO_HATCH_1MINERS
_length
```

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#L566

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.

```
raffleLimit = value
```

Recommendation

Emit an event for critical parameter changes.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L364

Description

Performing divisions before multiplications may cause lose of prediction.

```
newMiners = SafeMath.div(spacesUsed,SPACES_TO_HATCH_1MINERS)
```

Recommendation

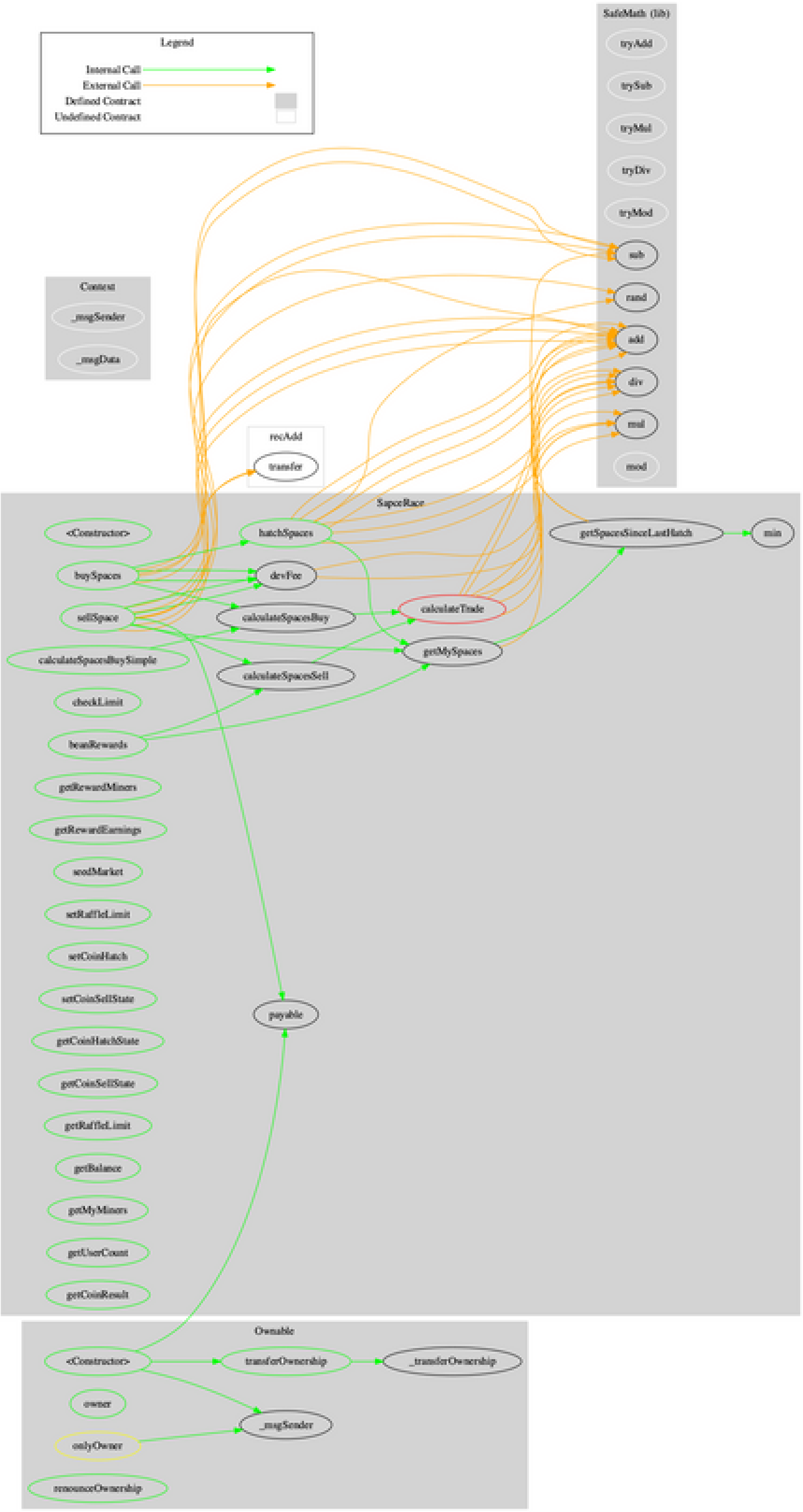
The multiplications should be prior to the divisions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
SafeMath	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		
	rand	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	Internal		
	div	Internal		
	mod	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
SapceRace	Implementation	Context, Ownable		

	<Constructor>	Public	✓	-
	hatchSpaces	Public	✓	-
	sellSpace	Public	✓	-
	beanRewards	Public		-
	buySpaces	Public	Payable	-
	calculateTrade	Private		
	checkLimit	Public		-
	calculateSpacesSell	Public		-
	calculateSpacesBuy	Public		-
	calculateSpacesBuySimple	Public		-
	devFee	Private		
	getRewardMiners	Public		-
	getRewardEarnings	Public		-
	seedMarket	Public	Payable	onlyOwner
	setRaffleLimit	Public	✓	onlyOwner
	setCoinHatch	Public	✓	onlyOwner
	setCoinSellState	Public	✓	onlyOwner
	getCoinHatchState	Public		-
	getCoinSellState	Public		-
	getRaffleLimit	Public		-
	getBalance	Public		-
	getMyMiners	Public		-
	getMySpaces	Public		-
	getSpacesSinceLastHatch	Public		-
	getUserCount	Public		-
	getCoinResult	Public		-
	min	Private		

Contract Flow



Domain Info

Domain Name	space-race.money
Registry Domain ID	44dad5aeddbe43d69ab38a86aa675d5e-DONUTS
Creation Date	2022-04-14T14:16:54Z
Updated Date	2022-04-19T14:17:49Z
Registry Expiry Date	2023-04-14T14:16:54Z
Registrar WHOIS Server	whois.godaddy.com/
Registrar URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created 7 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

SpaceRace minor is a novel project where users have the ability to buy spaces in order to redeem miners. The users can later claim the awarded amount that is based on the time period that has elapsed, the number of spaces/miners and the contract's balance. This audit focuses on the business logic, the security concerns and performance improvements.

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