Cyberscope

Audit Report

The Oil Club

June 2022

Type	BEP20
Network	BSC
Address	0x1dd969B56ec22e5D25E919C24330390C83184C67
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	oilClub
Compiler Version	v0.8.9+commit.e5eed63a
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x1dd969B56ec22e5D25E919C24330390C83184C67
Domain	oil.club

Source Files

Filename	**SHA256**
contract.sol	a246be5b742d9c4a51f21d7be2c42b83045bcaac04e9093dc93bb5083caee6da

Audit Updates

Initial Audit	9th July 2022
Corrected	

Contract Analysis

- The users have the ability to buy oil wells by paying in the native currency.
- The price of the oil wells depends on some variations like the quantity eths that are invested in the contract, the current market well and the Oil Club contract's native currency balance.
- The buy and sell amount is taxed by 2% dev, the taxed amount is moved directly to the owner of the contract.
- The users produce oil from the wells (miners) in order to redeem the generated oil from the last hatch.
- The redeem process is called "hatch".
- During the hatch process the referred user takes 50% of the user's generated oil as a reward.

Contract Owner Privileges

The contract owner does not disturb the user's experience in any means.

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
●	L05	Unused State Variable
●	L13	Divide before Multiply Operation

Contract Balance Dependency

Criticality	minor
Location	contract.sol

Description

The calculation of the sell and buy price heavily depends on the oilClub contract's amount. That means that the same amount of oil well 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 oil quantity as a result of the amount, contract balance and oil supply:

Amount	Contract Balance	Supply	Result
1	1000000	108000000000	107999.892000108
10	1000000	108000000000	1079989.200107999
100	1000000	108000000000	10798920.107989201

The following is the same amounts with different contract balance:

Amount	Contract Balance	Supply	Result
1	1000	108000000000	107892107.89210789
10	1000	108000000000	1069306930.6930693
100	1000	108000000000	9818181818.181818

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.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L45,55,60,141,155,161,192,200,206,210,214,218,222,230,234

Description

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

```
getSecondsPassed
getBlockTime
getLastHatch
getLastSell
getMyStreak
getMyMiners
getBalance
seedMarket
calculateWellsBuySimple
...
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L74,75,76,77,79,80,78

Description

Constant state variables should be declared constant to save gas.

```
strikeDailyPump
maxStrikeBonus
holdWeekBonus
devFeeVal
OIL_COEFH
OIL_COEF
LEASE_COEF
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L71,97,74,75,76

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.

```
OIL_COEFH
OIL_COEF
LEASE_COEF
seconds_hold
oilClub
```

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
Location	contract.sol#L78

Description

There are segments that contain unused state variables.

```
strikeDailyPump
```

Recommendation

Remove unused state variables.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L97,104

Description

Performing divisions before multiplications may cause lose of prediction.

```
bonusMiners = SafeMath.mul(SafeMath.div(newMiners,100),strike_bonus)
weekz = SafeMath.div(dayz,7)
```

Recommendation

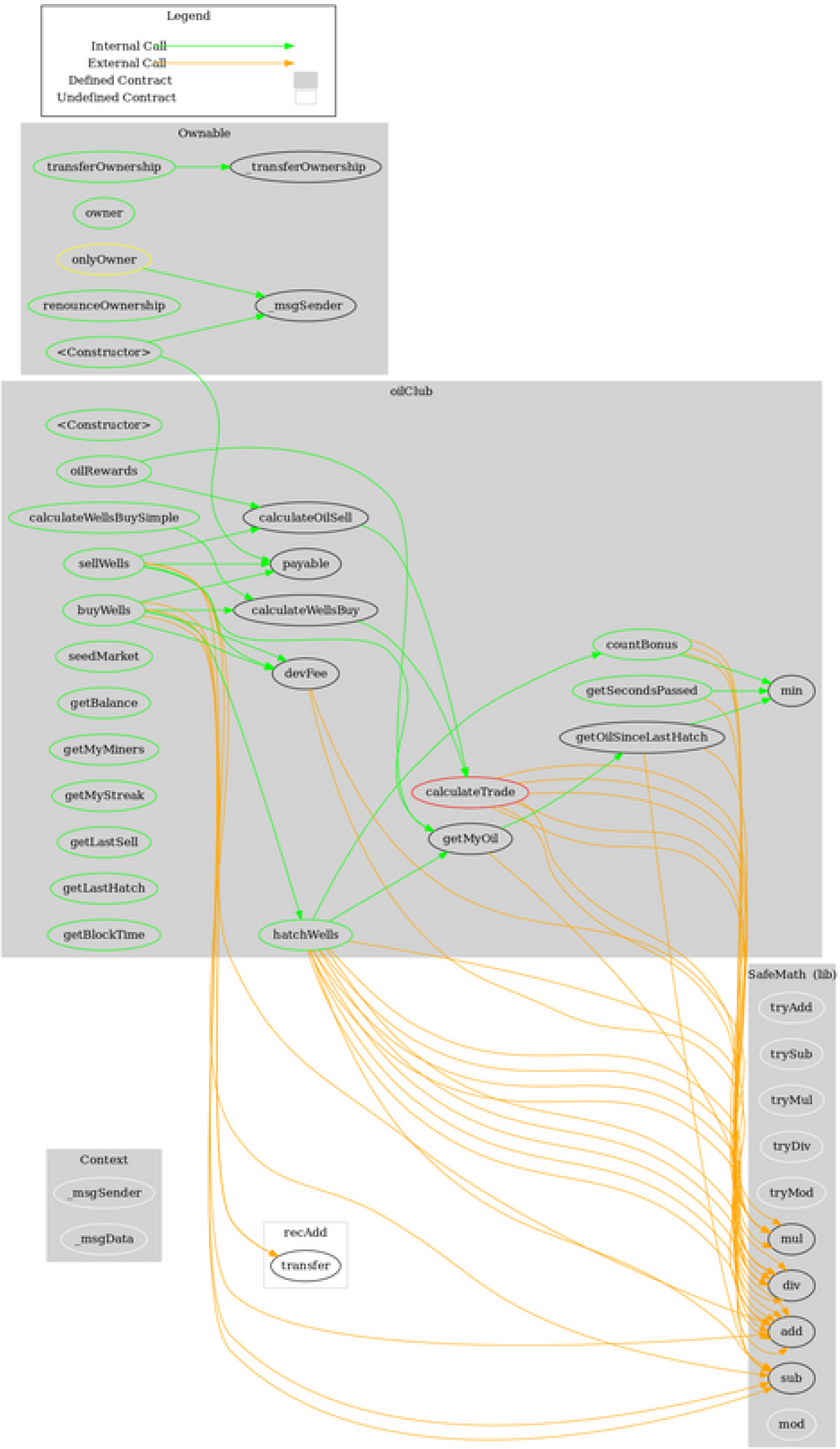
The multiplications should be prior to the divisions.

Contract Functions

Contract	**Type**	**Bases**		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
oilClub	Implementation	Context, Ownable		
	<Constructor>	Public	✓	-
	countBonus	Public		-
	hatchWells	Public	✓	-
	sellWells	Public	✓	-
	oilRewards	Public		-
	buyWells	Public	Payable	-
	calculateTrade	Private		
	calculateOilSell	Public		-
	calculateWellsBuy	Public		-
	calculateWellsBuySimple	Public		-
	devFee	Private		
	seedMarket	Public	Payable	onlyOwner
	getBalance	Public		-
	getMyMiners	Public		-
	getMyStreak	Public		-
	getLastSell	Public		-

	getLastHatch	Public		-
	getMyOil	Public		-
	getBlockTime	Public		-
	getSecondsPassed	Public		-
	getOilSinceLastHatch	Public		-
	min	Private		
SafeMath	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	Internal		
	div	Internal		
	mod	Internal		

Contract Flow



Domain Info

Domain Name	oil.club
Registry Domain ID	DC1EC116B7536447996A5DA46499899DC-GDREG
Creation Date	2022-04-19T10:06:24Z
Updated Date	2022-04-24T10:51:31Z
Registry Expiry Date	2024-04-19T10:06:24Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created in almost 2 years before the creation of the audit.

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

Summary

Oil Club is a novel project where users have the ability to oil wells in order to redeem oil. The users can later claim the awarded amount that is based on the time period that has elapsed, the quantity of oil 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 provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io