Cyberscope

Audit Report

Milk Cow

April 2022

Address	15ebdeb75eeadb557f4db5c4a8de18dc8e1b6639396a0eb13c7c16d57e171939
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	milkCow
Domain	milkcow.money

Source Files

Filename	SHA256
contract.sol	15ebdeb75eeadb557f4db5c4a8de18dc8e1b6639396a0eb13c7c16d57e171939

Audit Updates

Initial Audit	20th April 2022
Corrected	

Contract Analysis

- The users have the ability to buy milk by paying in the native currency.
- The price of milk depends on some variations like the current milk supply and the MilkCow contract's native currency balance.
- The buy and sell amount is taxed by 4% dev and 2% marketing fee, the taxed amount is moved directly to dev and marketing wallet.
- The users gathered milk in order to redeem cows.
- The redeem process is called "hatch".
- During the hatch process the referred user takes 14% of the user's milk as a reward.

Contract Owner Privileges

The contract owner has the authority to manipulate the cows and vesting period of the users by using the whitelist method.

Contract Diagnostics

● Critical ● Medium ● Minor

Severity	Code	Description
●	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

Contract Balance Dependency

Criticality	minor
Location	contract.sol#L398

Description

The calculation of the sell and buy price heavily depends on the MilkCow contract's amount. That means that the same amount of milk 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 milk quantity as a result of the amount, contract balance and milk 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#L373

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 accountValue = max(SafeMath.sub(address(this).balance,msg.value),
INITIAL_MONEY);
```

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#L256,266,271,305,355,370,383,392,415,420,428,432,446

Description

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

```
checkLastHatch
getMyCows
getBalance
checkWhiteList
calculateCowsBuySimple
beanRewards
seedMarket
buyMilk
sellMilk
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L285,289,286,287,288

Description

Constant state variables should be declared constant to save gas.

```
devFeeVal
PSNH
PSN
MarketingFeeVal
MILK_TO_HATCH_1COW
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L282,383,402,450,284,285,286,287,289,292

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.

```
MarAdd
MarketingFeeVal
PSNH
PSN
MILK_TO_HATCH_1COW
INITIAL_MONEY
MarFee
Milk
initial_value
...
```

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#L383

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.

```
INITIAL_MONEY = initial_value
```

Recommendation

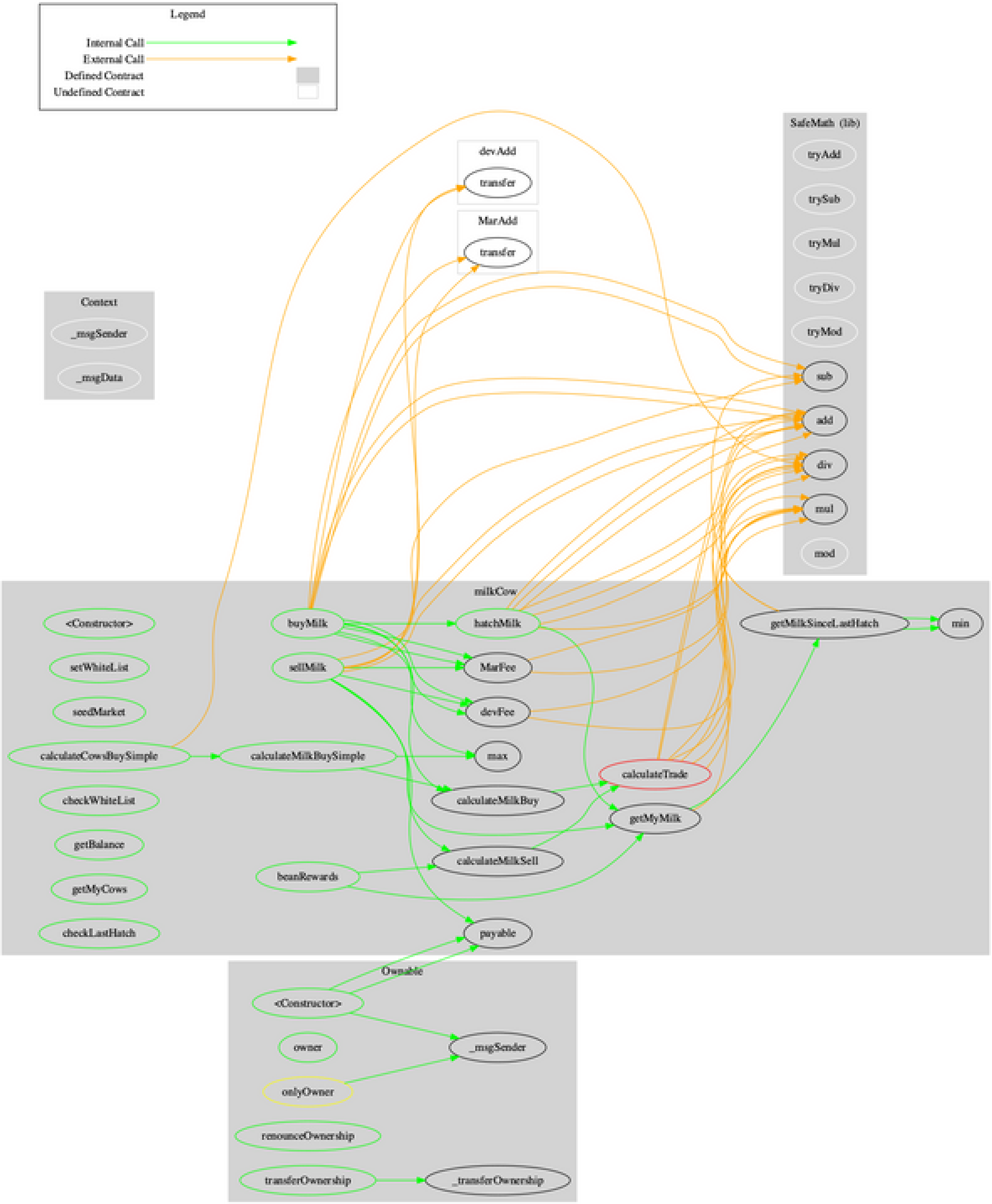
Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
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		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
milkCow	Implementation	Context, Ownable		
	<Constructor>	Public	✓	-

	setWhiteList	Public	✓	onlyOwner
	hatchMilk	Public	✓	-
	sellMilk	Public	✓	-
	buyMilk	Public	Payable	-
	seedMarket	Public	✓	onlyOwner
	beanRewards	Public		-
	calculateTrade	Private		
	calculateMilkSell	Public		-
	calculateMilkBuy	Public		-
	calculateMilkBuySimple	Public		-
	calculateCowsBuySimple	Public		-
	checkWhiteList	Public		-
	devFee	Private		
	getBalance	Public		-
	getMyCows	Public		-
	getMyMilk	Public		-
	getMilkSinceLastHatch	Public		-
	checkLastHatch	Public		-
	MarFee	Private		
	min	Private		
	max	Private		

Contract Flow



Domain Info

Domain Name	milkcow.money
Registry Domain ID	7042ff32d32247af9edcd98796271925-DONUTS
Creation Date	2022-04-17T03:51:16Z
Updated Date	2022-04-17T03:51:18Z
Registry Expiry Date	2023-04-17T03:51:16Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created 3 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

Milk Cow is a novel project where users have the ability to buy milk in order to redeem cows. The users can later claim the awarded amount that is based on the time period that has elapsed, the number of milk/cows 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