



S O L I D I T Y . F I N A N C E



# Artichain Token & Sale - Audit Report

## S U M M A R Y



Artichain intends to build a dex and coin tracker for meme tokens.

For this audit we reviewed the project's token and presale contracts at commit

32a2f4f3d6a3b2d03af889c5907feeabc17e0a36 and again later at commit  
68c9b5311c4b25dd5c26f49325413e96fedf83d3 on GitHub. The combined source code is available below.

Please note we have not reviewed the project's upcoming decentralized exchange.

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

- *Token holders can delegate their voting rights to any address. To save gas, users can also do so using an EIP-712 signature.*
- *The initial total supply of the token is 22,650.*
- *Tokens can be minted by the owner at any time. The owner is intended to be the MasterArt staking contract.*
- *No ownership-protected functions relating to the token are present.*
- *The contract utilizes SafeMath to prevent overflows.*

#### *Notes of the Presale Contract:*

- *This contract allows users to purchase tokens with BUSD at pre-determined prices.*
- *The team will set the price of the token at each stage upon deployment.*
- *Each stage of the presale has a price, cap, and bonus for purchases.*
- *Tokens can only be purchased between the opening and closing time of the presale, as set by the team.*
- *Once purchased, tokens will be minted by the contract and delivered to the user. The team should ensure a price is set in the liquidity pool prior to providing normal users their tokens.*
- *The team can update the price of the token for the current stage at any time.*
- *The contract utilizes SafeMath to prevent overflow issues.*
- *ReentrancyGuard is also used when purchasing tokens to prevent reentrancy attacks.*

#### *Notes of the MasterArt Staking Contract:*

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

- *The team can add additional pools at any time. The team must be careful not to add the same pool twice; or implement a check to prevent this.*
- *The team will set the reward rate upon deployment and can update it at any time.*
- *Rewards are minted by the staking contract and are claimed by users upon withdrawing.*
- *1% of rewards will be minted to the development team.*
- *The team has implemented gas optimizations on our recommendation.*
- *Utilization of SafeMath throughout the platform to prevent overflow issues.*

### *Audit Findings Summary*

- *No issues from external attackers were identified.*
- *As with any presale, ensure trust in the team prior to investing.*
- *Further, ensure trust in the team as they have some power in the ecosystem.*
- *Date: June 6th, 2021.*
- *Update Date: June 8th, 2021 - Minor fixes/improvements.*

## **EXTERNAL THREAT RESULTS**

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

Vulnerability Category	Notes	Result
Arbitrary Jump	N/A	PASS
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Deprecated Opcodes	N/A	PASS
Ether Thief	N/A	PASS
Exceptions	N/A	PASS
External Calls	N/A	PASS
Flash Loans	N/A	PASS
Integer Over/Underflow	N/A	PASS
Multiple Sends	N/A	PASS
Oracles	N/A	PASS
Suicide	N/A	PASS
State Change External Calls	N/A	PASS

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

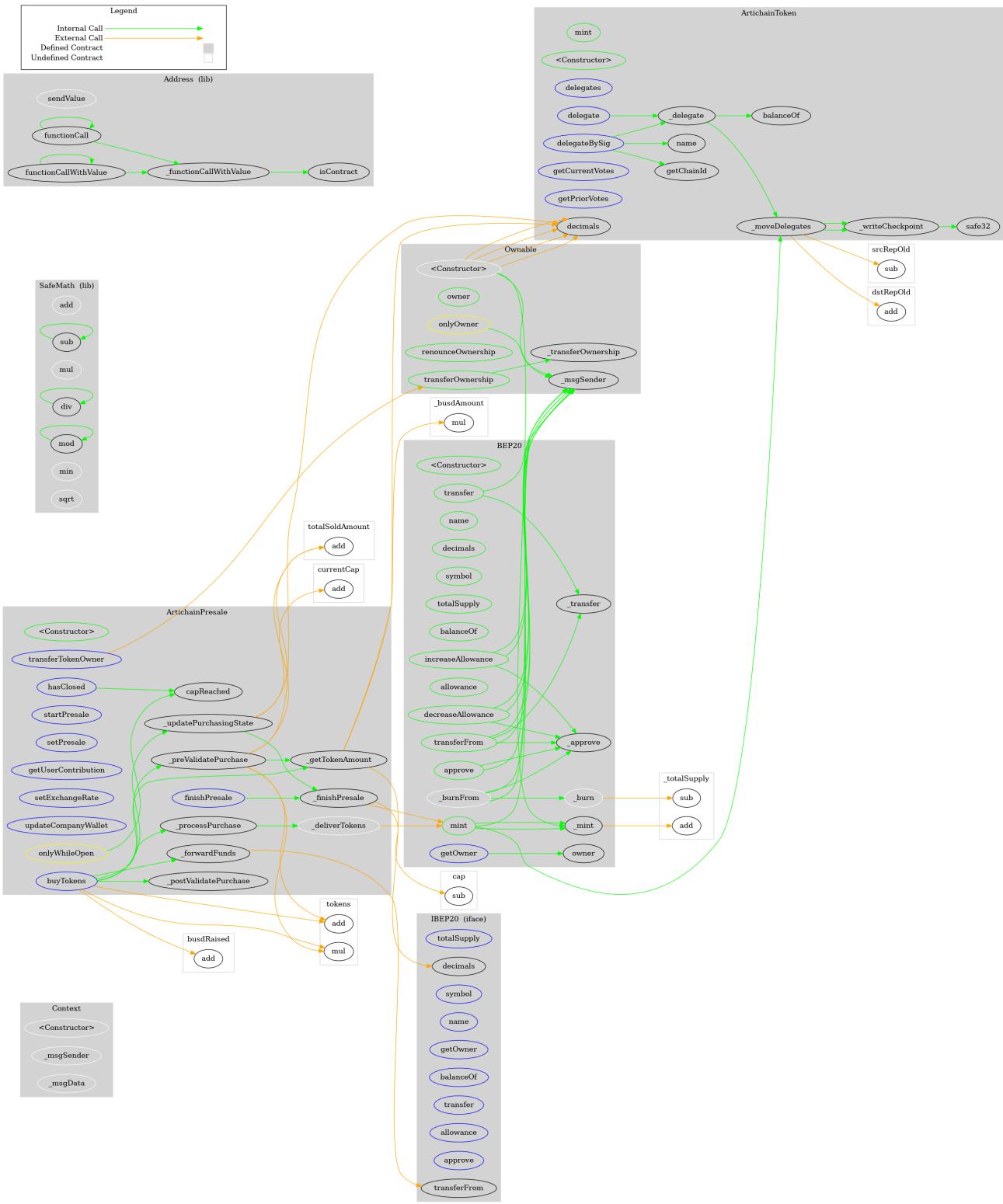
Vulnerability Category	Notes	Result
User Supplied Assertion	N/A	PASS
Critical Solidity Compiler	N/A	PASS
Overall Contract Safety		PASS

## Details: ArtichainPreSale

FUNCTION GRAPH

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

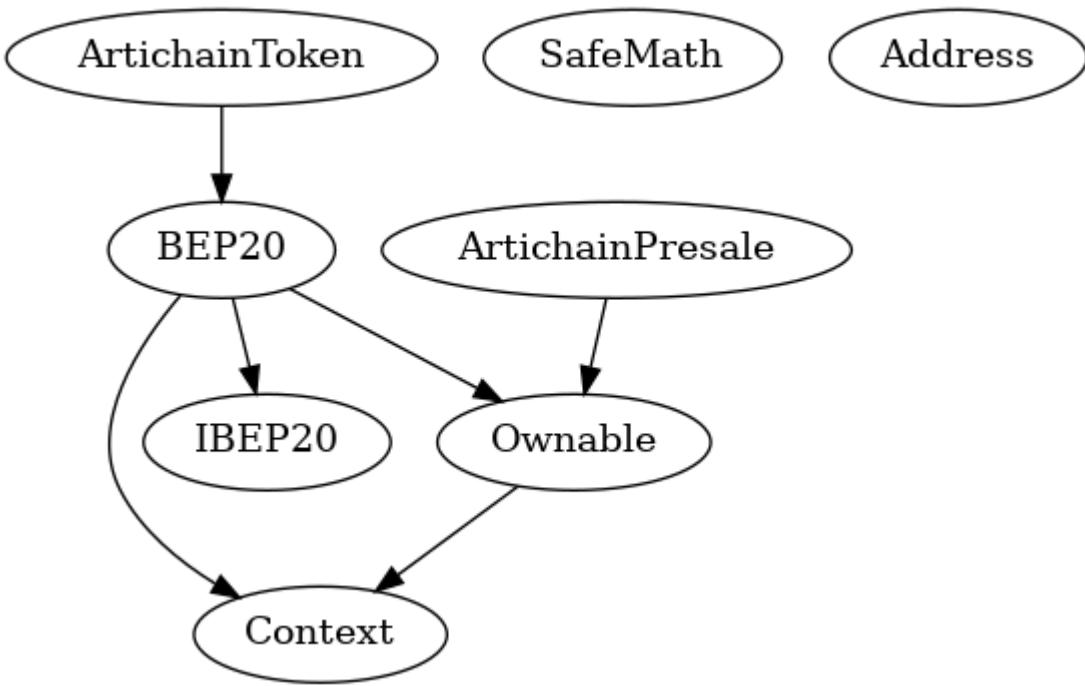
By using this site, you explicitly agree to these terms.



## INHERITANCE CHART

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.



## F U N C T I O N S   O V E R V I E W

`(\$)` = payable function

`#` = non-constant function

`Int` = Internal

`Ext` = External

`Pub` = Public

+ Context

- [Int] #
- [Int] `_msgSender`
- [Int] `_msgData`

+ Ownable (Context)

- [Int] #
- [Pub] `owner`
- [Pub] `renounceOwnership` #

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

```
- [Int] _transferOwnership #  
  
+ [Lib] SafeMath  
- [Int] add  
- [Int] sub  
- [Int] sub  
- [Int] mul  
- [Int] div  
- [Int] div  
- [Int] mod  
- [Int] mod  
- [Int] min  
- [Int] sqrt  
  
+ [Int] IBEP20  
- [Ext] totalSupply  
- [Ext] decimals  
- [Ext] symbol  
- [Ext] name  
- [Ext] getOwner  
- [Ext] balanceOf  
- [Ext] transfer #  
- [Ext] allowance  
- [Ext] approve #  
- [Ext] transferFrom #  
  
+ [Lib] Address  
- [Int] isContract  
- [Int] sendValue #  
- [Int] functionCall #  
- [Int] functionCall #  
- [Int] functionCallWithValue #
```

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

```
- [Pub]    #
- [Ext] getOwner
- [Pub] name
- [Pub] decimals
- [Pub] symbol
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] mint #
  - modifiers: onlyOwner
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve #
- [Int] _burnFrom #
```

```
+ ArtichainToken (BEP20)
- [Pub] mint #
  - modifiers: onlyOwner
- [Pub] #
- [Ext] delegates
- [Ext] delegate #
- [Ext] delegateBySig #
- [Ext] getCurrentVotes
- [Ext] getPriorVotes
- [Int] _delegate #
- [Int] _moveDelegates #
```

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

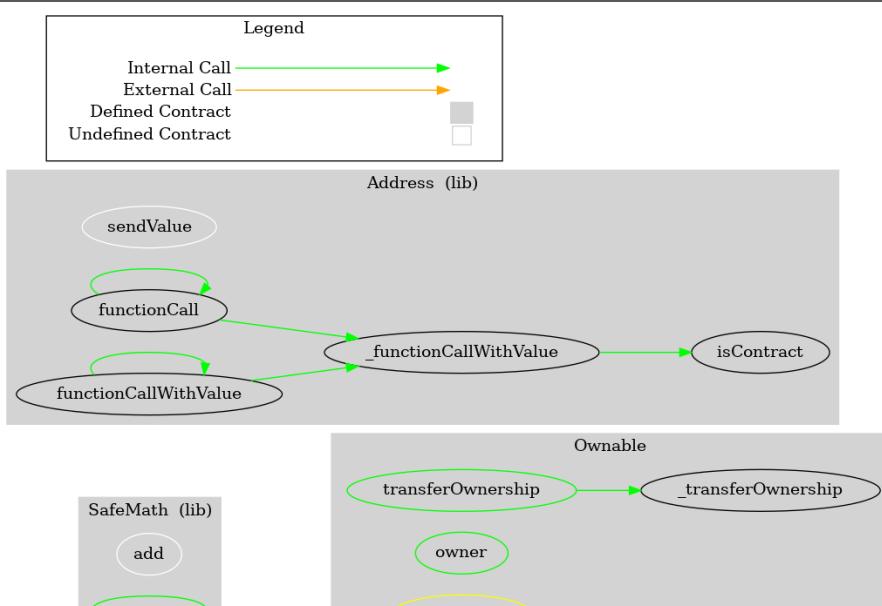
```

+ ArtichainPresale (Ownable)
  - [Pub] #
  - [Pub] capReached
  - [Ext] hasClosed
  - [Ext] startPresale #
    - modifiers: onlyOwner
  - [Ext] setPresale #
    - modifiers: onlyOwner
  - [Ext] finishPresale #
    - modifiers: onlyOwner
  - [Ext] getUserContribution
  - [Ext] setExchangeRate #
    - modifiers: onlyWhileOpen,onlyOwner
  - [Ext] updateCompanionsWallet #

```

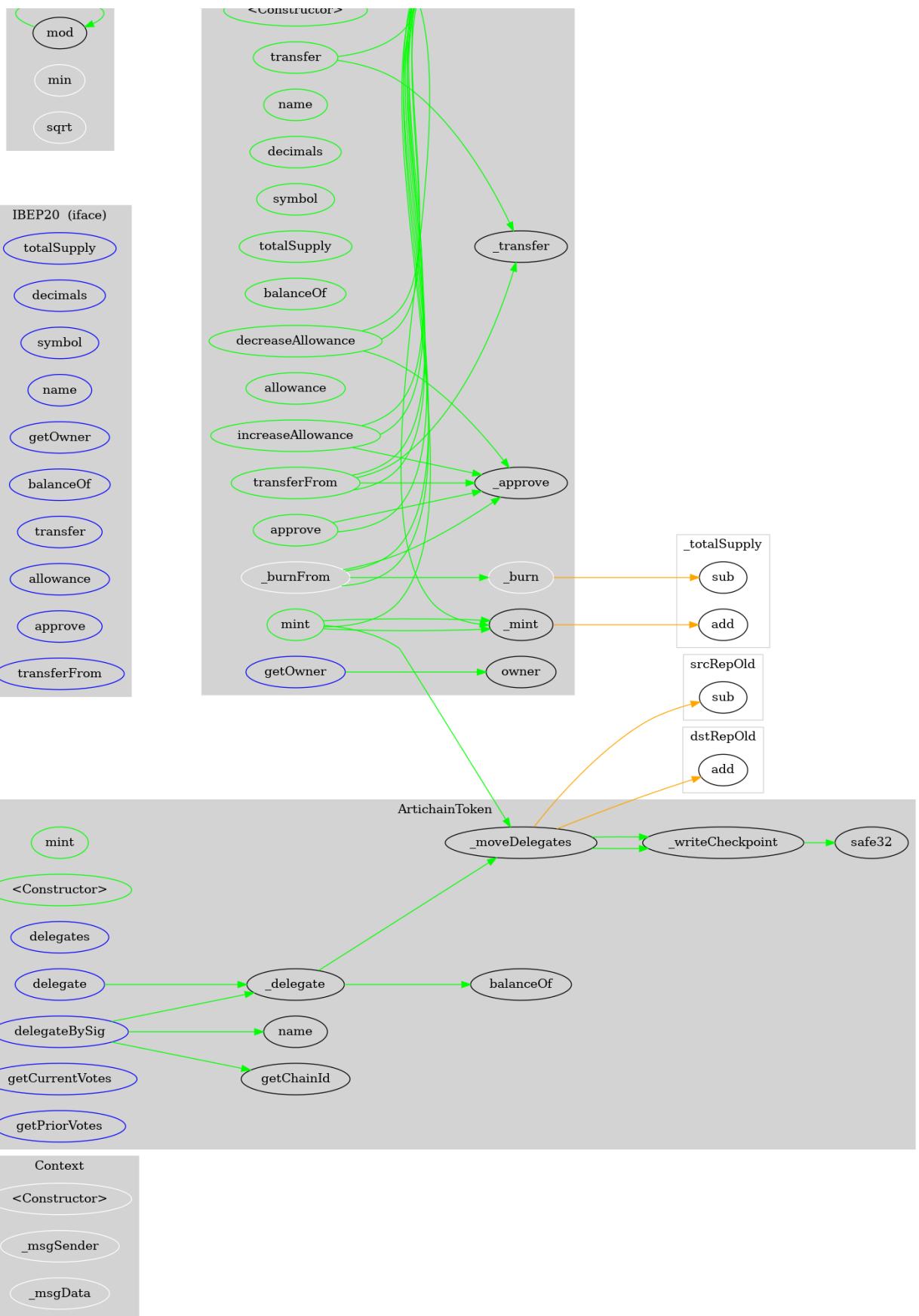
# Details: ArtichainToken

## FUNCTION GRAPH



Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

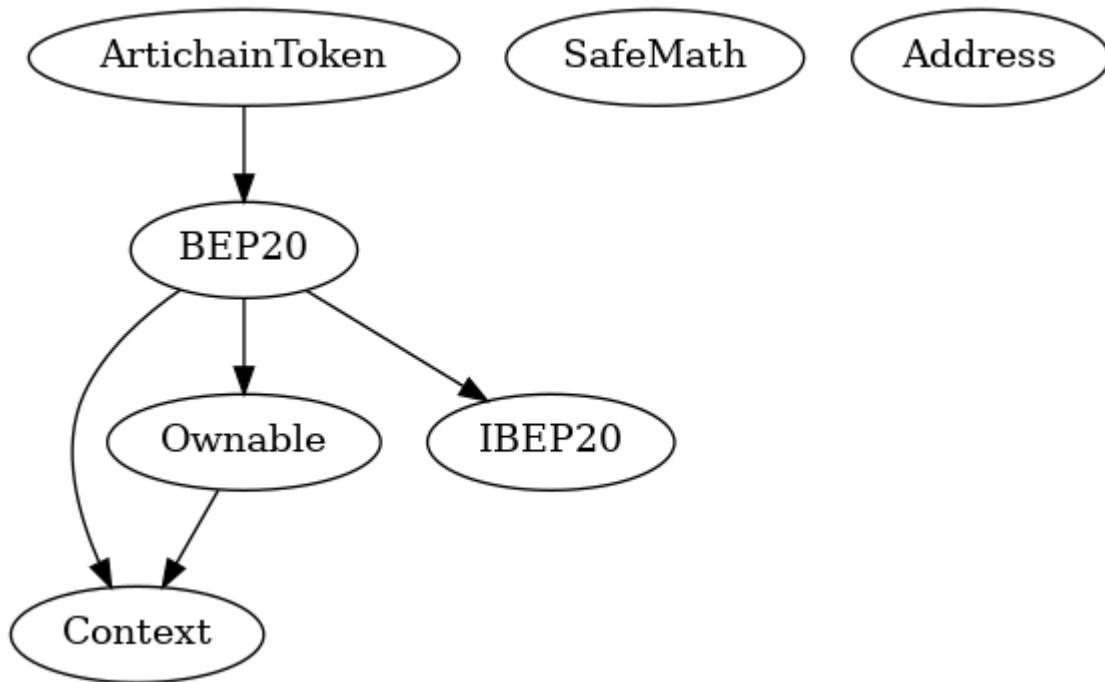
By using this site, you explicitly agree to these terms.



## INHERITANCE CHART

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.



## FUNCTIONS OVERVIEW

`(\$)` = payable function  
`#` = non-constant function

Int = Internal

Ext = External

Pub = Public

- + Context
  - [Int] #
  - [Int] \_msgSender
  - [Int] \_msgData

- + Ownable (Context)
  - [Int] #
  - [Pub] owner
  - [Pub] renounceOwnership #

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

```
- [Int] _transferOwnership #  
  
+ [Int] IBEP20  
- [Ext] totalSupply  
- [Ext] decimals  
- [Ext] symbol  
- [Ext] name  
- [Ext] getOwner  
- [Ext] balanceOf  
- [Ext] transfer #  
- [Ext] allowance  
- [Ext] approve #  
- [Ext] transferFrom #  
  
+ [Lib] SafeMath  
- [Int] add  
- [Int] sub  
- [Int] sub  
- [Int] mul  
- [Int] div  
- [Int] div  
- [Int] mod  
- [Int] mod  
- [Int] min  
- [Int] sqrt  
  
+ [Lib] Address  
- [Int] isContract  
- [Int] sendValue #  
- [Int] functionCall #  
- [Int] functionCall #  
- [Int] functionCallWithValue #
```

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

```
- [Pub]    #
- [Ext] getOwner
- [Pub] name
- [Pub] decimals
- [Pub] symbol
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] mint #
  - modifiers: onlyOwner
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve #
- [Int] _burnFrom #
```

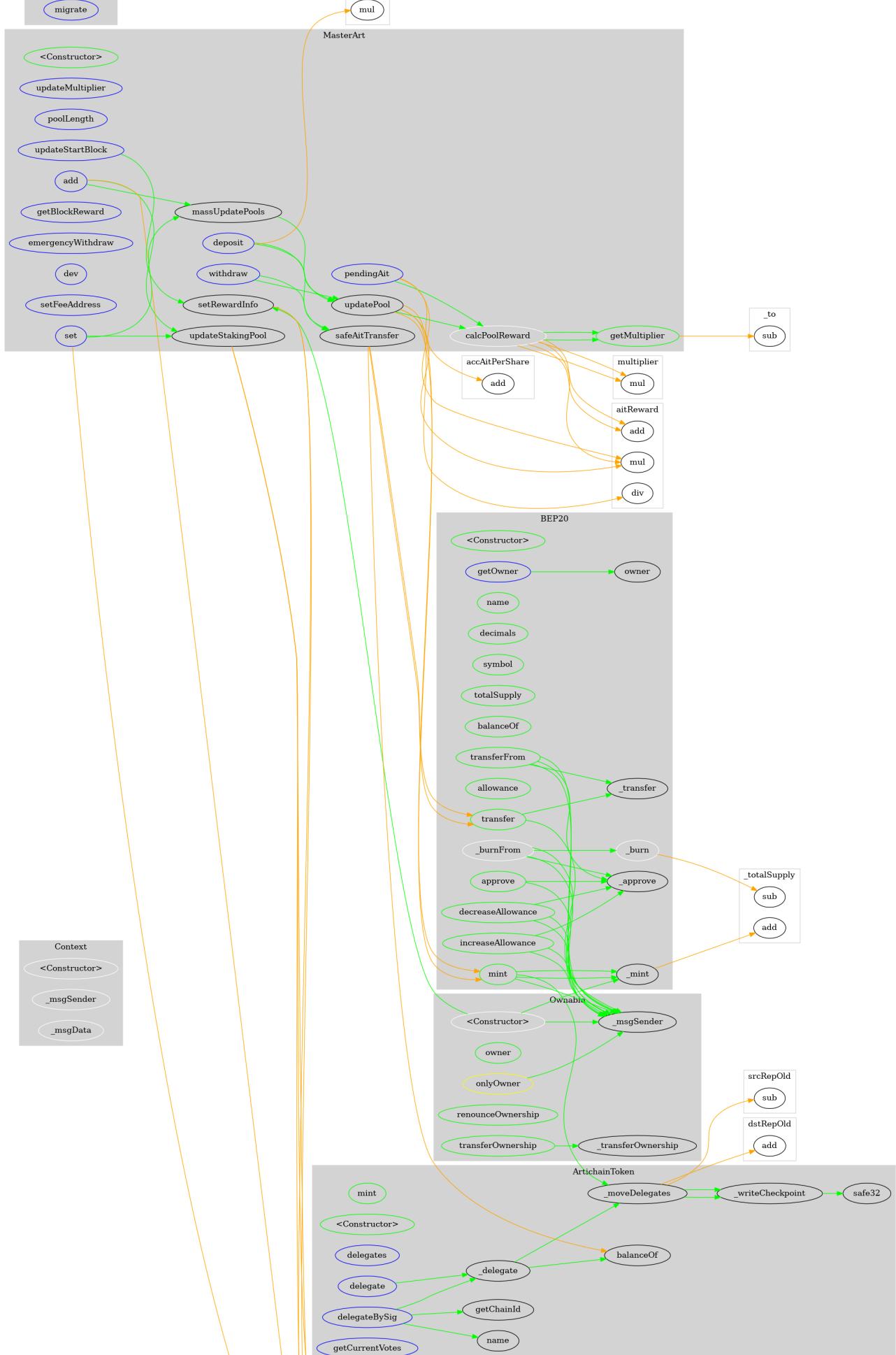
  

```
+ ArtichainToken (BEP20)
- [Pub] mint #
  - modifiers: onlyOwner
- [Pub] #
```

# Details: MasterArt

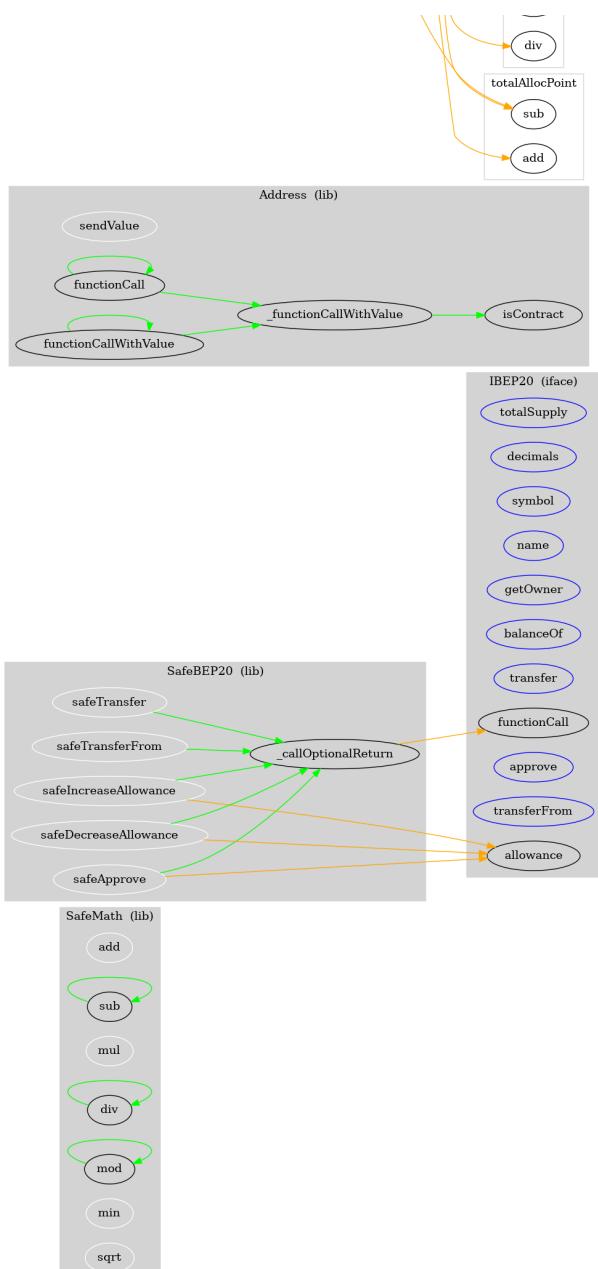
Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

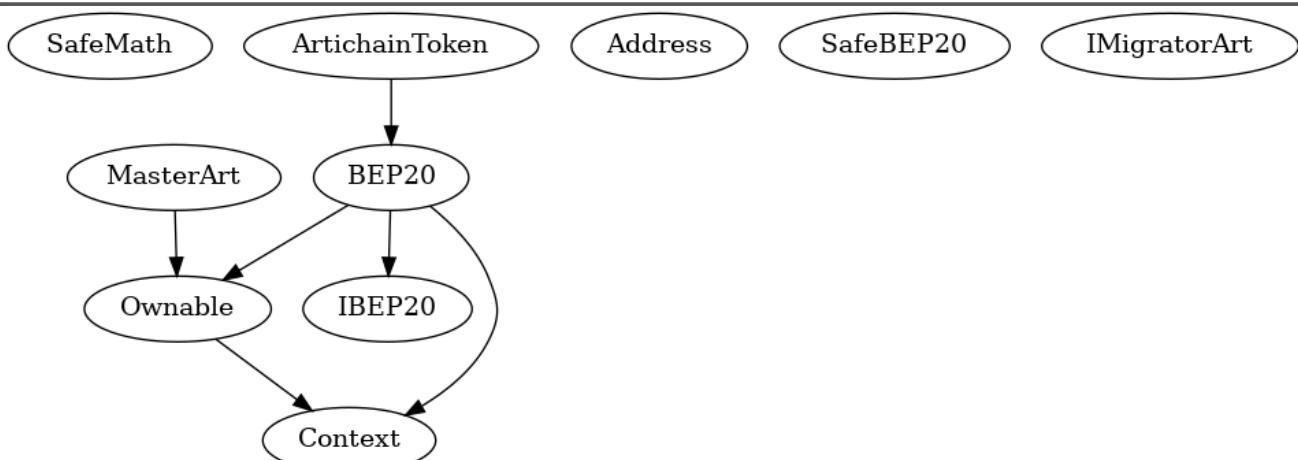


Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.



## INHERITENCE CHART



Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

## FUNCTIONS OVERVIEW

`(\$)` = payable function  
`#` = non-constant function

`Int` = Internal

`Ext` = External

`Pub` = Public

- + [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod
  - [Int] min
  - [Int] sqrt
- + [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

```
- [Int] isContract  
- [Int] sendValue #  
- [Int] functionCall #  
- [Int] functionCall #  
- [Int] functionCallWithValue #  
- [Int] functionCallWithValue #  
- [Prv] _functionCallWithValue #  
  
+ [Lib] SafeBEP20  
- [Int] safeTransfer #  
- [Int] safeTransferFrom #  
- [Int] safeApprove #  
- [Int] safeIncreaseAllowance #  
- [Int] safeDecreaseAllowance #  
- [Prv] _callOptionalReturn #  
  
+ Context  
- [Int] #  
- [Int] _msgSender  
- [Int] _msgData  
  
+ Ownable (Context)  
- [Int] #  
- [Pub] owner  
- [Pub] renounceOwnership #  
  - modifiers: onlyOwner  
- [Pub] transferOwnership #  
  - modifiers: onlyOwner  
- [Int] _transferOwnership #  
  
+ BEP20 (Context, IBEP20, Ownable)  
- [Pub] #
```

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

```
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] mint #
  - modifiers: onlyOwner
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve #
- [Int] _burnFrom #
```

```
+ ArtichainToken (BEP20)
- [Pub] mint #
  - modifiers: onlyOwner
- [Pub] #
- [Ext] delegates
- [Ext] delegate #
- [Ext] delegateBySig #
- [Ext] getCurrentVotes
- [Ext] getPriorVotes
- [Int] _delegate #
- [Int] _moveDelegates #
- [Int] _writeCheckpoint #
- [Int] safe32
- [Int] getChainId
```

```
+ [Int] IMigratorArt
```

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

By using this site, you explicitly agree to these terms.

- [Ext] updateMultiplier #
  - modifiers: onlyOwner
- [Ext] poolLength
- [Ext] add #
  - modifiers: onlyOwner
- [Ext] set #
  - modifiers: onlyOwner
- [Int] updateStakingPool #
  - modifiers: onlyOwner

## G O H O M E

Copyright 2021 © Solidity Finance LLC. All rights reserved. Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#).

Please review our Terms & Conditions, Privacy Policy, and other legal information [here](#). By using this site, you explicitly agree to these terms.