# Alchemy Toys - Audit Report

## SUMMARY

Alchemy Toys is a new blockchain-based game where users own and collect unique cards, represented on-chain as NFTs, in order to create rare NFTs and win rewards.

For this audit, we reviewed the project's Game, Vault, Treasury, and Timer contracts. The code was reviewed at commit d2d32033ce9918c69c42d89aca07f712bf44025f and later at commit 5c9120ccf15f7554dceee3df3f351631cbb64641 on the project's private GitLab repo.

> *Notes on the Contracts:*
>
> - *The game is designed to be played over many periods of time divided into epochs, cycles, and turns. Users actions survive through these*

- *Each NFT has a a toy type and a level associated with it, ranging from 1-7. In addition, each NFT has an incremental serial number.*
- *Users can contribute platorm tokens via a worship function in order to generate 3 random NFTs. Probability leans towards each of these NFTs being less-rare.*
- *Users can melt two cards together to generate a higher level card.*
- *Users can also sacrifice any of their cards, burning the associated NFT but providing the user with an 'enlightenment' token.*
- *If a user holds an enlightenment token, they can burn that token to 'proclaim' an in return receive a 'goohood' token.*
- *Each of these actions has a cost associated with it denominated in the platform's tokens.*
- *Winners of the game will recieve most of proceeds from the Game Treasury which will also be split among other participants and reserved for future epochs.*
- *Ultimately, the goal of the game is to collect NFTs and sacrifice them in order to win.*
- *Once deployed, the team cannot change any variables related to the game.*
- *The randomness function, to an extent, relies on predictable environment variables. This is common, albiet not best practice; but the probability of miners maliciously changing these variables is extremley low.*
- *The team has worked with us to optimize these contracts for gas optimization and accuracy in calculations.*
- *Solidity 0.8.4 is used across all contracts to prevent overflows.*

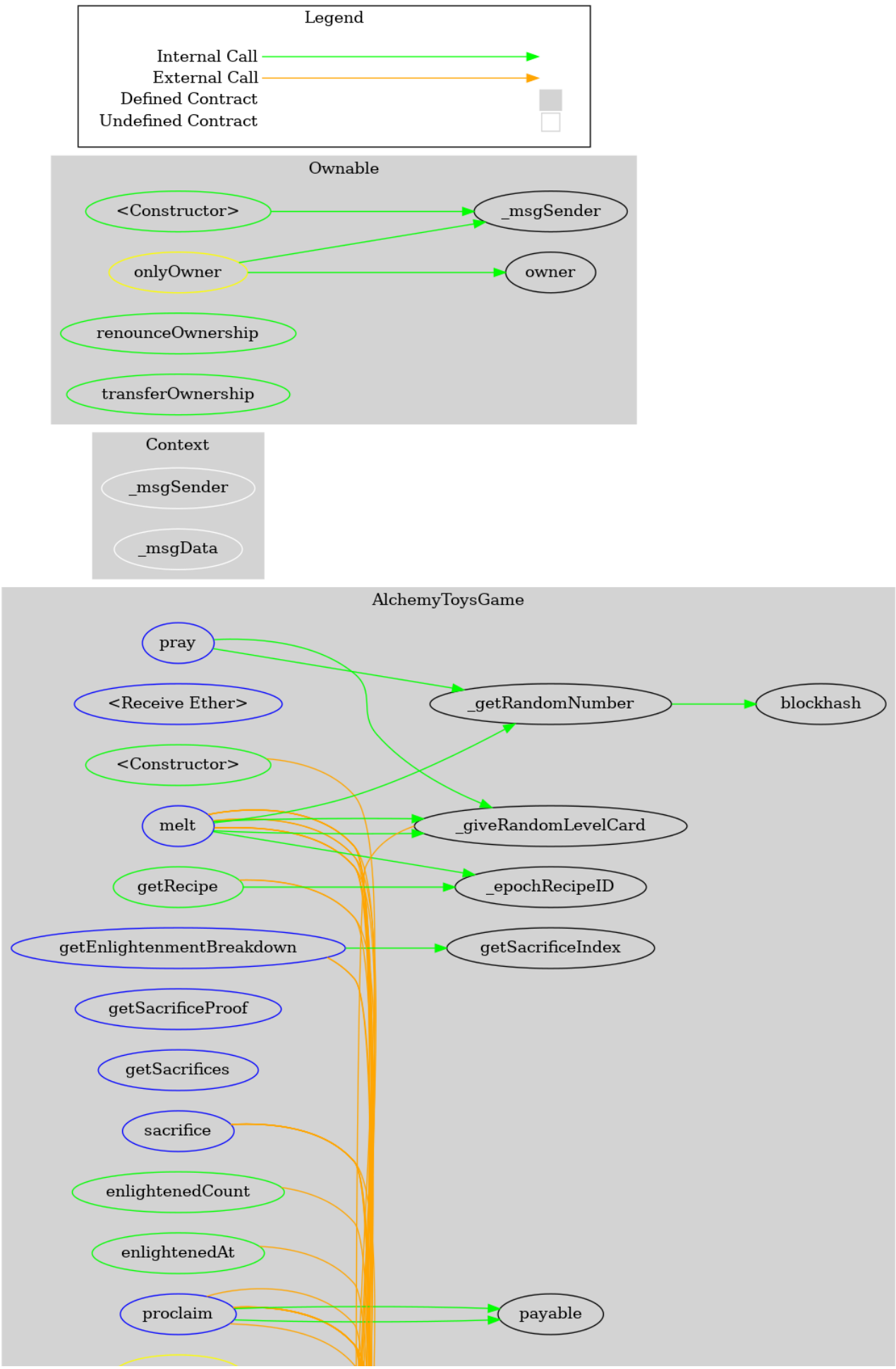
- *Date: April 30th, 2021*

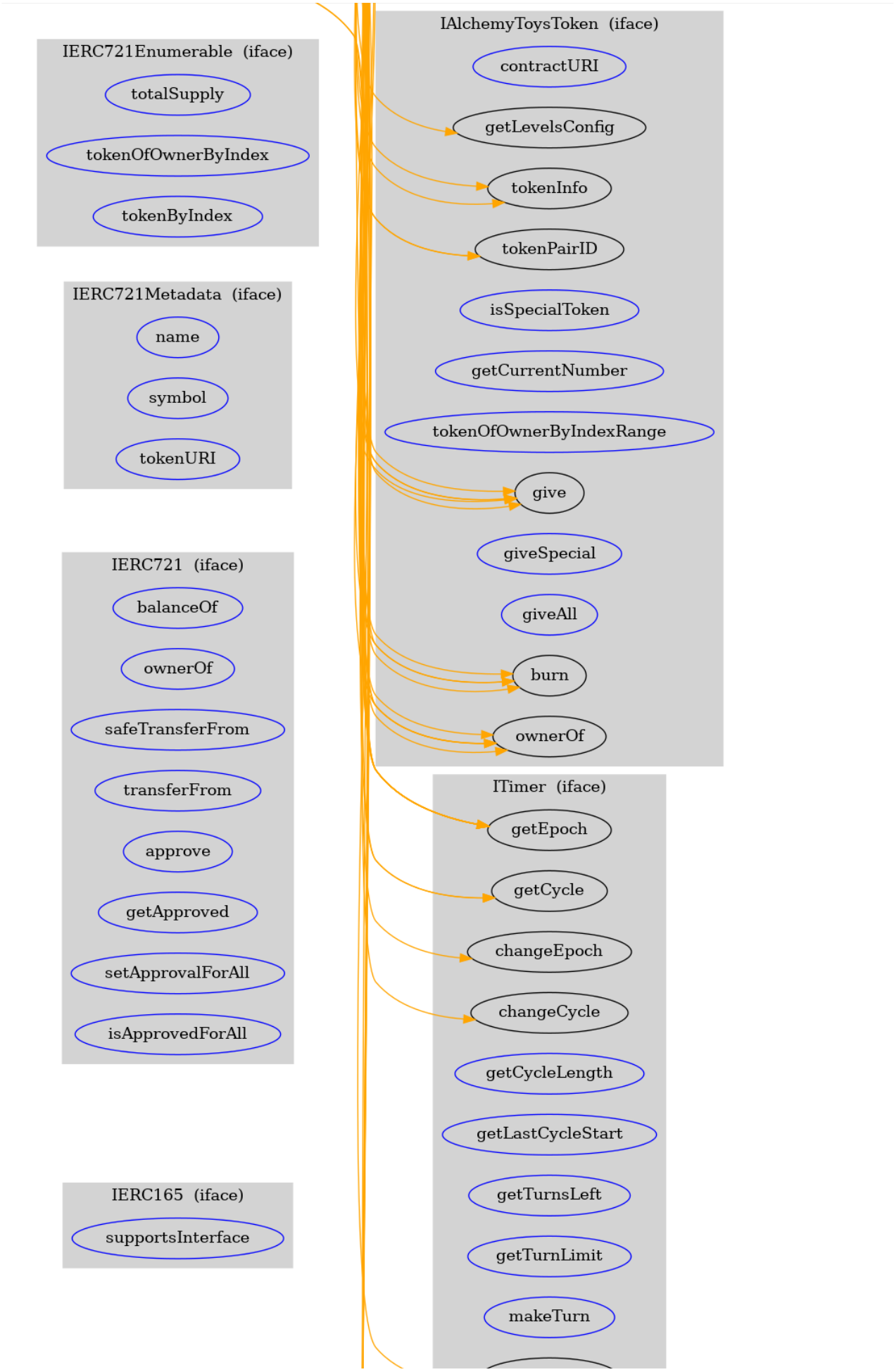
## EXTERNAL THREATS - AUDIT RESULTS

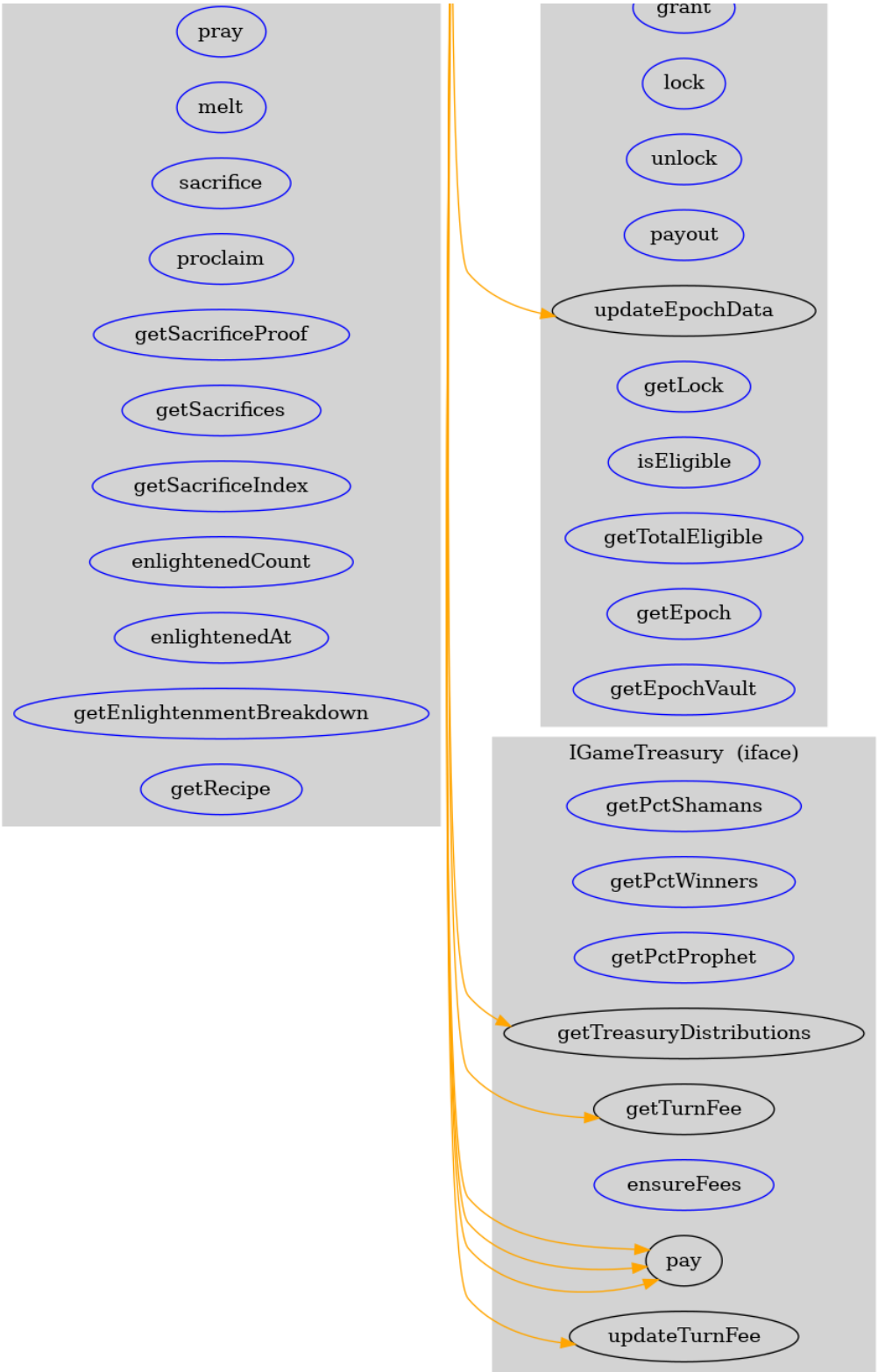
| Vulnerability Category | Notes | Result |
|---|---|---|
| Arbitrary Storage Write | N/A | PASS |
| Arbitrary Jump | N/A | PASS |
| Delegate Call to Untrusted Contract | N/A | PASS |
| Dependence on Predictable Variables | Randomness relies on a series of environmental variables. Probability of a negative impact is very low. | WARNING |
| Deprecated Opcodes | N/A | PASS |
| Ether Thief | N/A | PASS |
| Exceptions | N/A | PASS |
| External Calls | N/A | PASS |

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

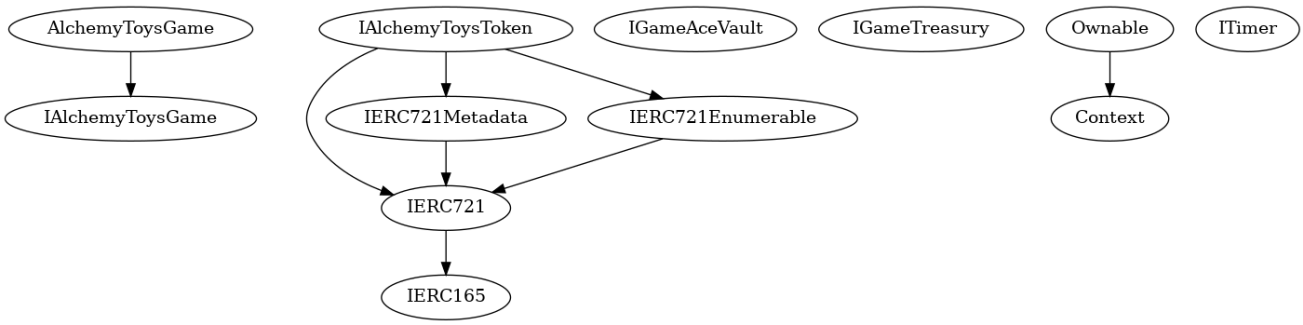
**DETAILS: ALCHEMYTOYSGAME.SOL**








## INHERITENCE CHART




## FUNCTIONS OVERVIEW

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

Int = Internal
Ext = External
Pub = Public

+ [Int] IAlchemyToysGame
   - [Ext] pray ($)
   - [Ext] melt ($)
   - [Ext] sacrifice #
   - [Ext] proclaim #
   - [Ext] getSacrificeProof
   - [Ext] getSacrifices
   - [Ext] getSacrificeIndex
   - [Ext] enlightenedCount
   - [Ext] enlightenedAt
   - [Ext] getEnlightenmentBreakdown
   - [Ext] getRecipe
```

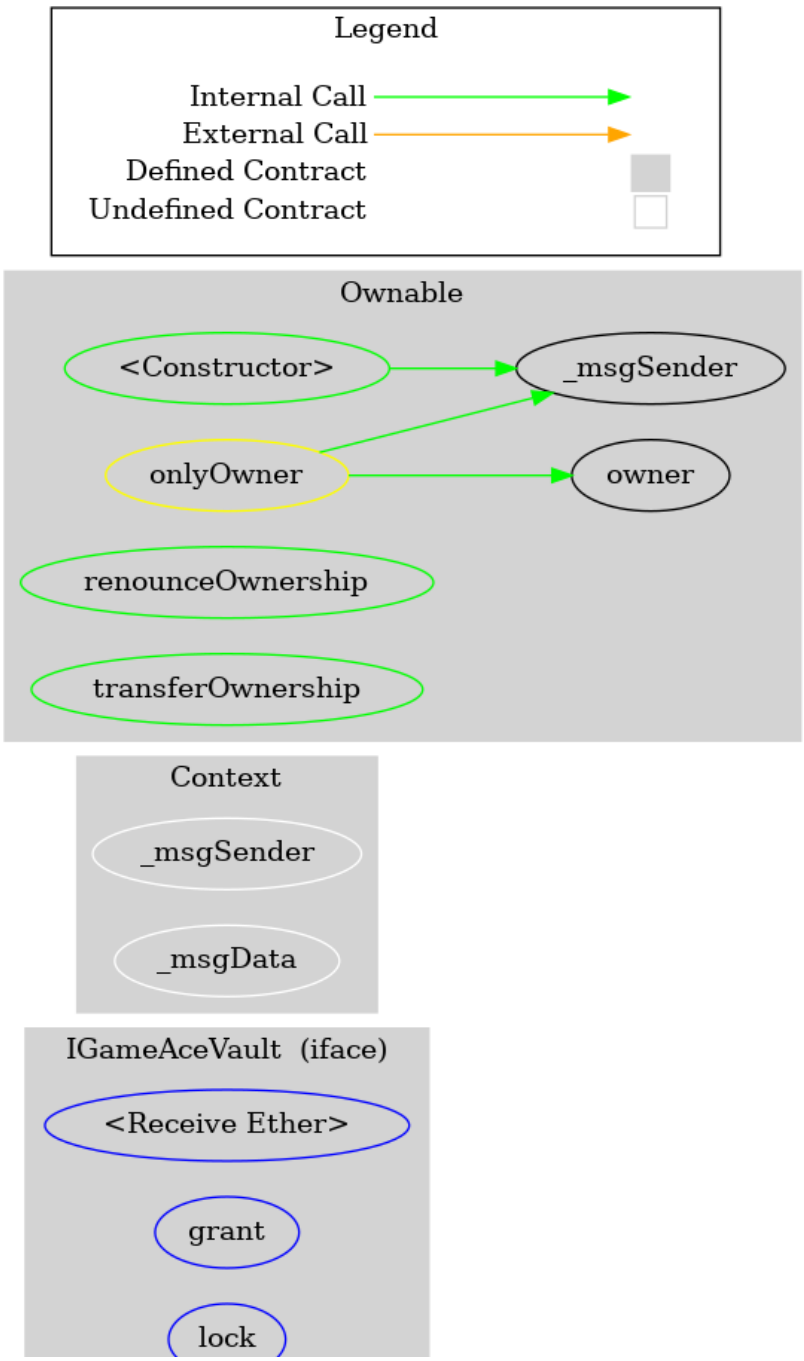
```
+ [Int] IERC721 (IERC165)
   - [Ext] balanceOf
   - [Ext] ownerOf
   - [Ext] safeTransferFrom #
   - [Ext] transferFrom #
   - [Ext] approve #
   - [Ext] getApproved
   - [Ext] setApprovalForAll #
   - [Ext] isApprovedForAll
   - [Ext] safeTransferFrom #

+ [Int] IERC721Metadata (IERC721)
   - [Ext] name
   - [Ext] symbol
   - [Ext] tokenURI

+ [Int] IERC721Enumerable (IERC721)
   - [Ext] totalSupply
   - [Ext] tokenOfOwnerByIndex
   - [Ext] tokenByIndex

+ [Int] IAlchemyToysToken (IERC721, IERC721Metadata, IERC7
   - [Ext] contractURI
   - [Ext] getLevelsConfig
   - [Ext] tokenInfo
   - [Ext] tokenPairID
   - [Ext] isSpecialToken
   - [Ext] getCurrentNumber
   - [Ext] tokenOfOwnerByIndexRange
   - [Ext] give #
   - [Ext] giveSpecial #
   - [Ext] giveAll #
```

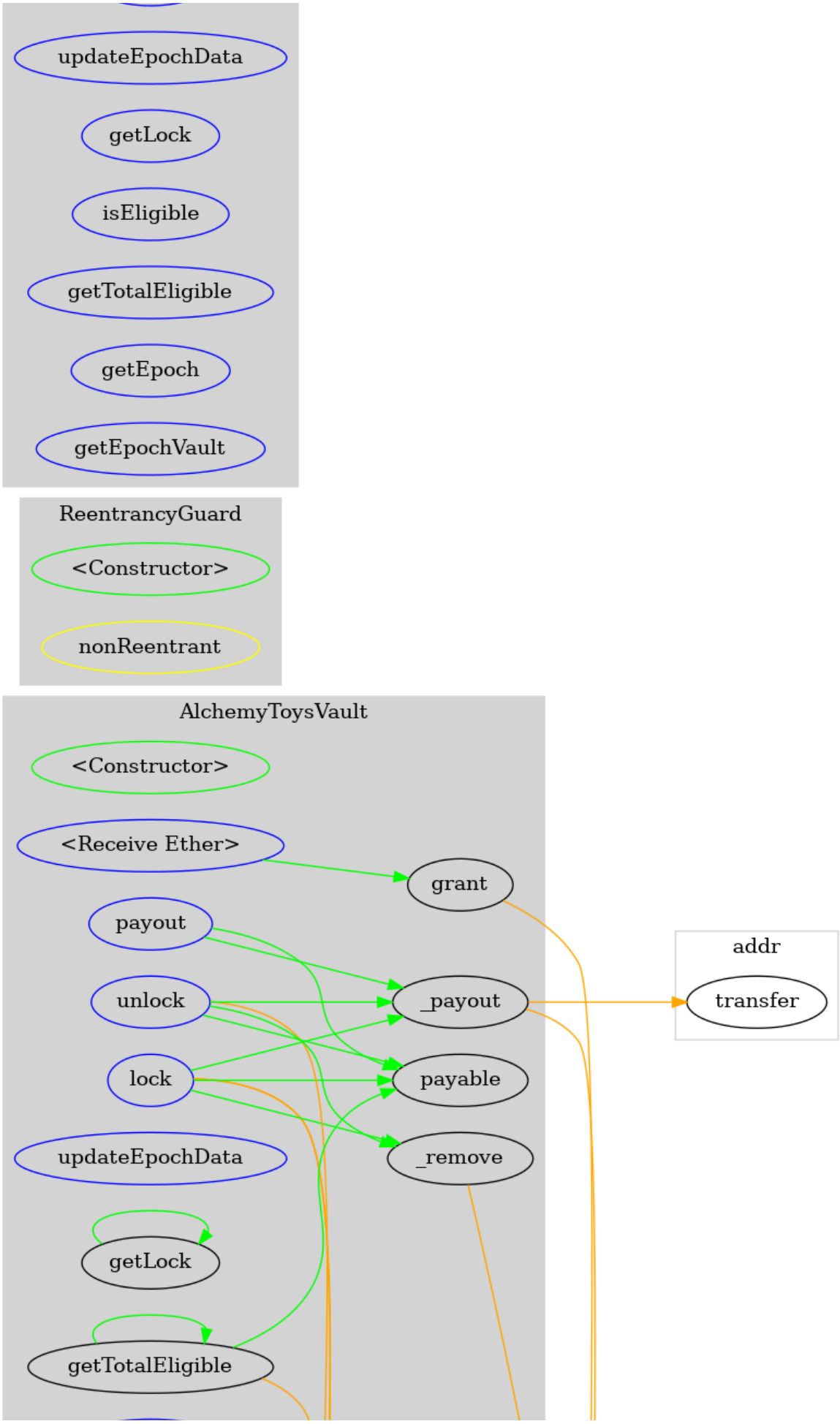
```
    - [Ext] grant ($)
    - [Ext] lock #
    - [Ext] unlock #
    - [Ext] payout #
    - [Ext] updateEpochData #
    - [Ext] getLock
    - [Ext] getLock
    - [Ext] isEligible
    - [Ext] isEligible
    - [Ext] getTotalEligible
    - [Ext] getTotalEligible
    - [Ext] getEpoch
    - [Ext] getEpochVault
    - [Ext] getEpochVault

+ [Int] IGameTreasury
    - [Ext] getPctShamans
    - [Ext] getPctWinners
    - [Ext] getPctProphet
    - [Ext] getTurnFee
    - [Ext] getTreasuryDistributions
    - [Ext] ensureFees ($)
    - [Ext] updateTurnFee #
    - [Ext] pay #

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

+  Ownable (Context)
    - [Pub]  #
    - [Pub] owner
```

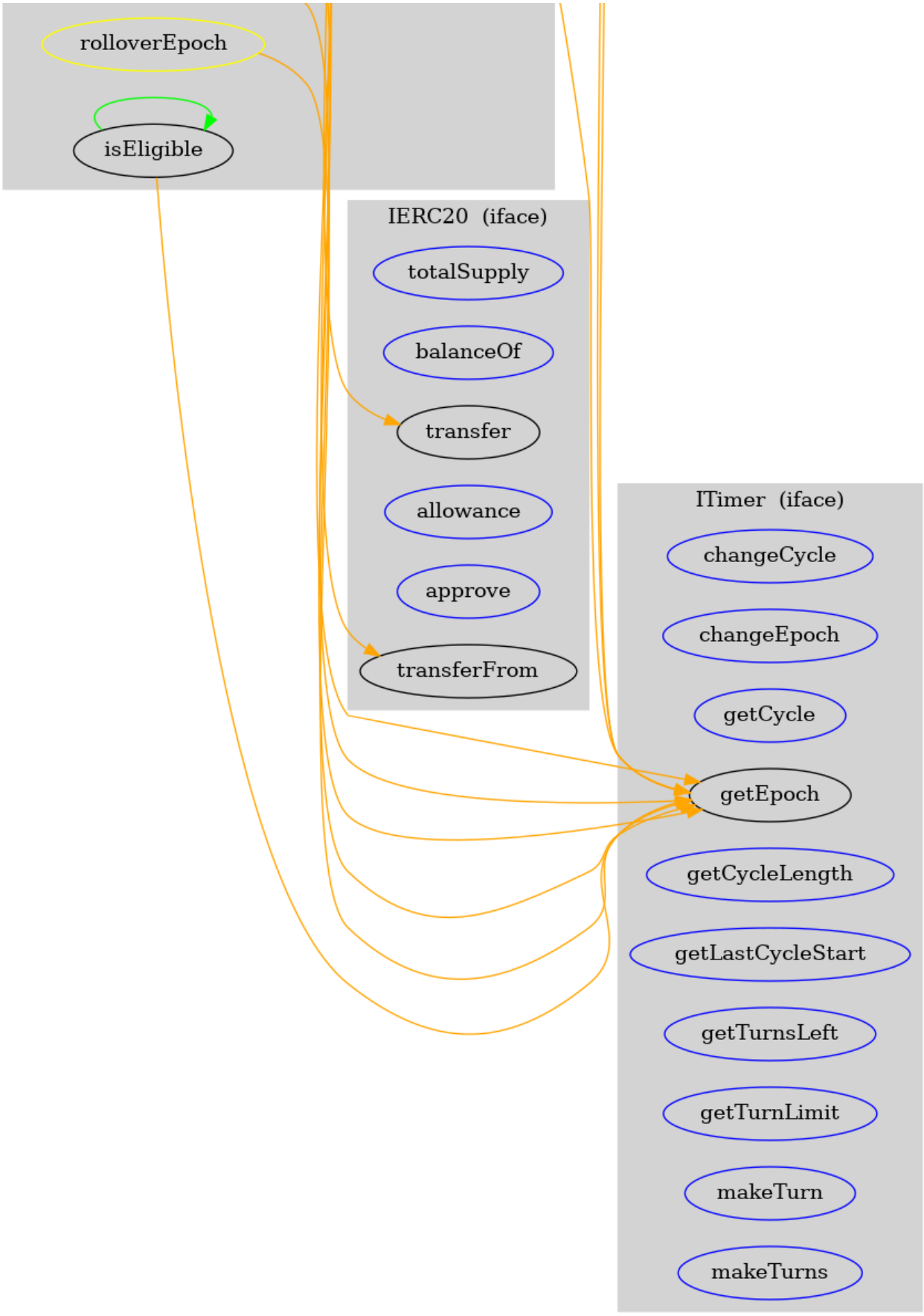
```
+ [Int] ITimer
   - [Ext] changeCycle #
   - [Ext] changeEpoch #
   - [Ext] getCycle
   - [Ext] getEpoch
   - [Ext] getCycleLength
   - [Ext] getLastCycleStart
   - [Ext] getTurnsLeft
   - [Ext] getTurnLimit
   - [Ext] makeTurn #
   - [Ext] makeTurns #

+  AlchemyToysGame (IAlchemyToysGame)
   - [Pub]  #
   - [Ext]  ($)
      - modifiers: ensureFee
   - [Ext] pray ($)
      - modifiers: ensureCycle,ensureFee,makeTurn
   - [Ext] melt ($)
      - modifiers: ensureCycle,ensureFee,makeTurn
   - [Ext] sacrifice #
      - modifiers: ensureCycle,makeTurn
   - [Ext] proclaim #
      - modifiers: ensureCycle
   - [Ext] getSacrificeProof
   - [Ext] getSacrifices
   - [Pub] getSacrificeIndex
   - [Pub] enlightenedCount
   - [Pub] enlightenedAt
   - [Ext] getEnlightenmentBreakdown
   - [Pub] getRecipe
```

## DETAILS: ALCHEMYTOYSVAULT.SOL

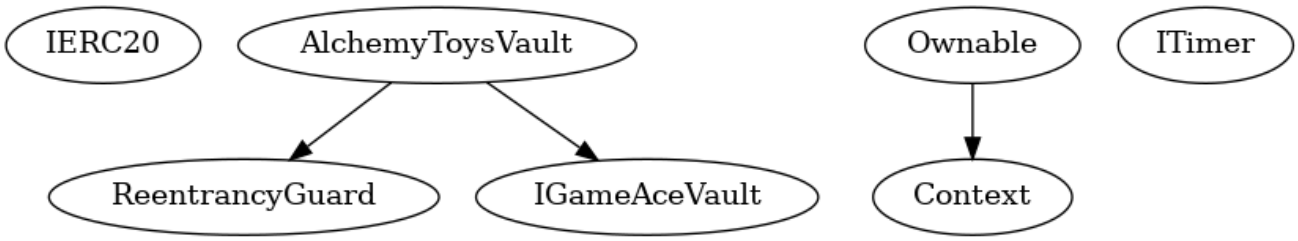
## FUNCTION GRAPH








## INHERITENCE CHART




## FUNCTIONS OVERVIEW

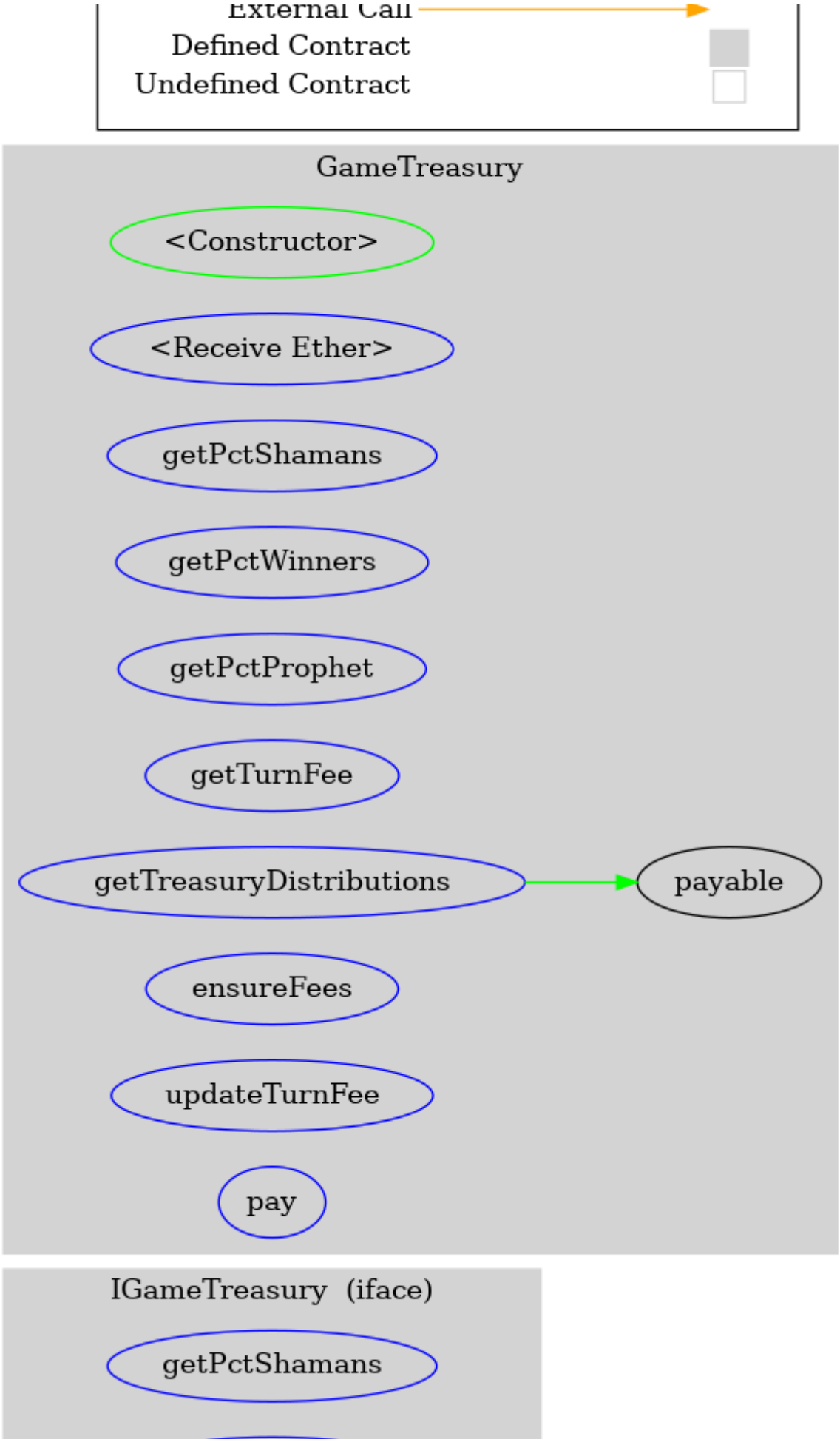
```
($) = payable function
# = non-constant function

Int = Internal
Ext = External
Pub = Public

+ [Int] IERC20
   - [Ext] totalSupply
   - [Ext] balanceOf
   - [Ext] transfer #
   - [Ext] allowance
   - [Ext] approve #
   - [Ext] transferFrom #

+  ReentrancyGuard
   - [Pub]  #

+ [Int] IGameAceVault
   - [Ext]  ($)
   - [Ext] grant ($)
```

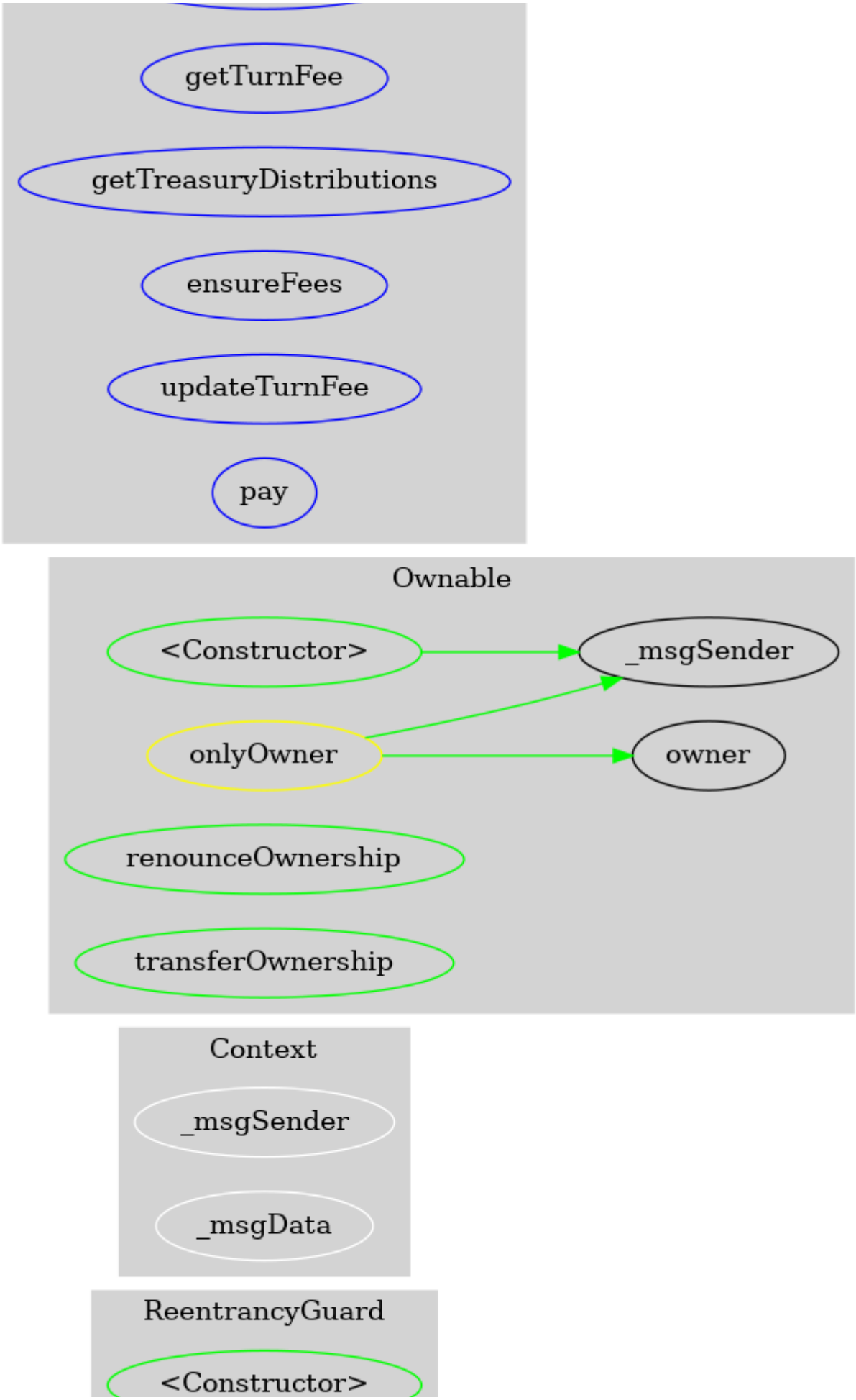
```
    - [Ext] updateEpochData #
    - [Ext] getLock
    - [Ext] getLock
    - [Ext] isEligible
    - [Ext] isEligible
    - [Ext] getTotalEligible
    - [Ext] getTotalEligible
    - [Ext] getEpoch
    - [Ext] getEpochVault
    - [Ext] getEpochVault

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

+   Ownable (Context)
    - [Pub]  #
    - [Pub] owner
    - [Pub] renounceOwnership #
       - modifiers: onlyOwner
    - [Pub] transferOwnership #
       - modifiers: onlyOwner

+ [Int] ITimer
    - [Ext] changeCycle #
    - [Ext] changeEpoch #
    - [Ext] getCycle
    - [Ext] getEpoch
    - [Ext] getCycleLength
    - [Ext] getLastCycleStart
    - [Ext] getTurnsLeft
    - [Ext] getTurnLimit
```

```
- [Pub]  #
- [Ext]  ($)
- [Pub] grant ($)
- [Ext] lock #
   - modifiers: rolloverEpoch
- [Ext] unlock #
   - modifiers: rolloverEpoch
- [Ext] payout #
   - modifiers: rolloverEpoch
- [Ext] updateEpochData #
   - modifiers: rolloverEpoch
- [Ext] getLock
- [Pub] getLock
- [Ext] isEligible
- [Pub] isEligible
- [Ext] getTotalEligible
- [Pub] getTotalEligible
- [Ext] getEpoch
- [Ext] getEpochVault
- [Pub] getEpochVault
- [Prv] _remove #
- [Prv] _payout #
   - modifiers: nonReentrant
```

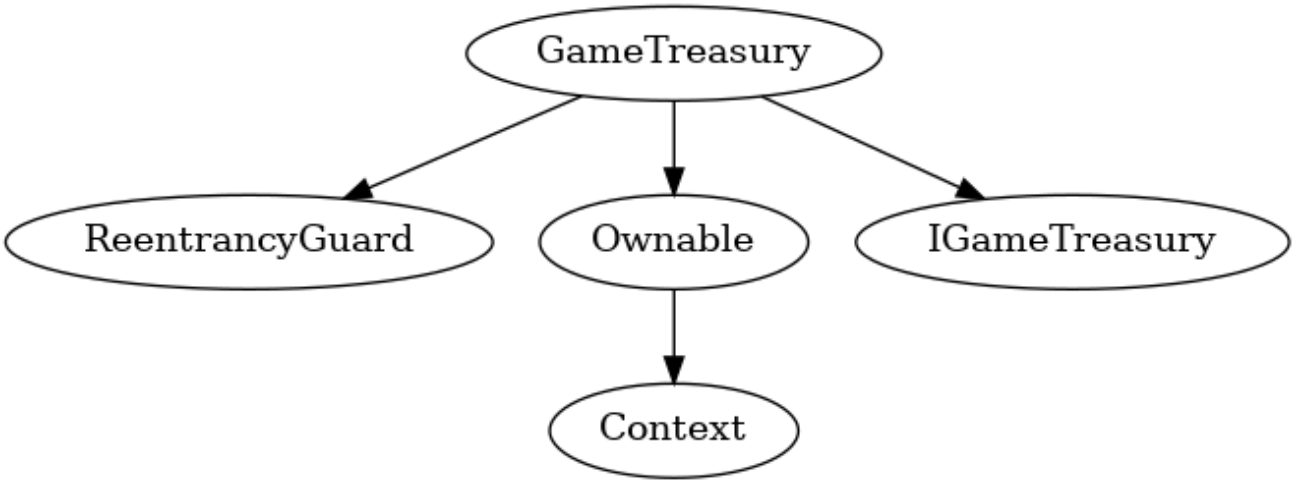
## DETAILS: GAMETREASURY.SOL

### FUNCTION GRAPH





## INHERITENCE CHART



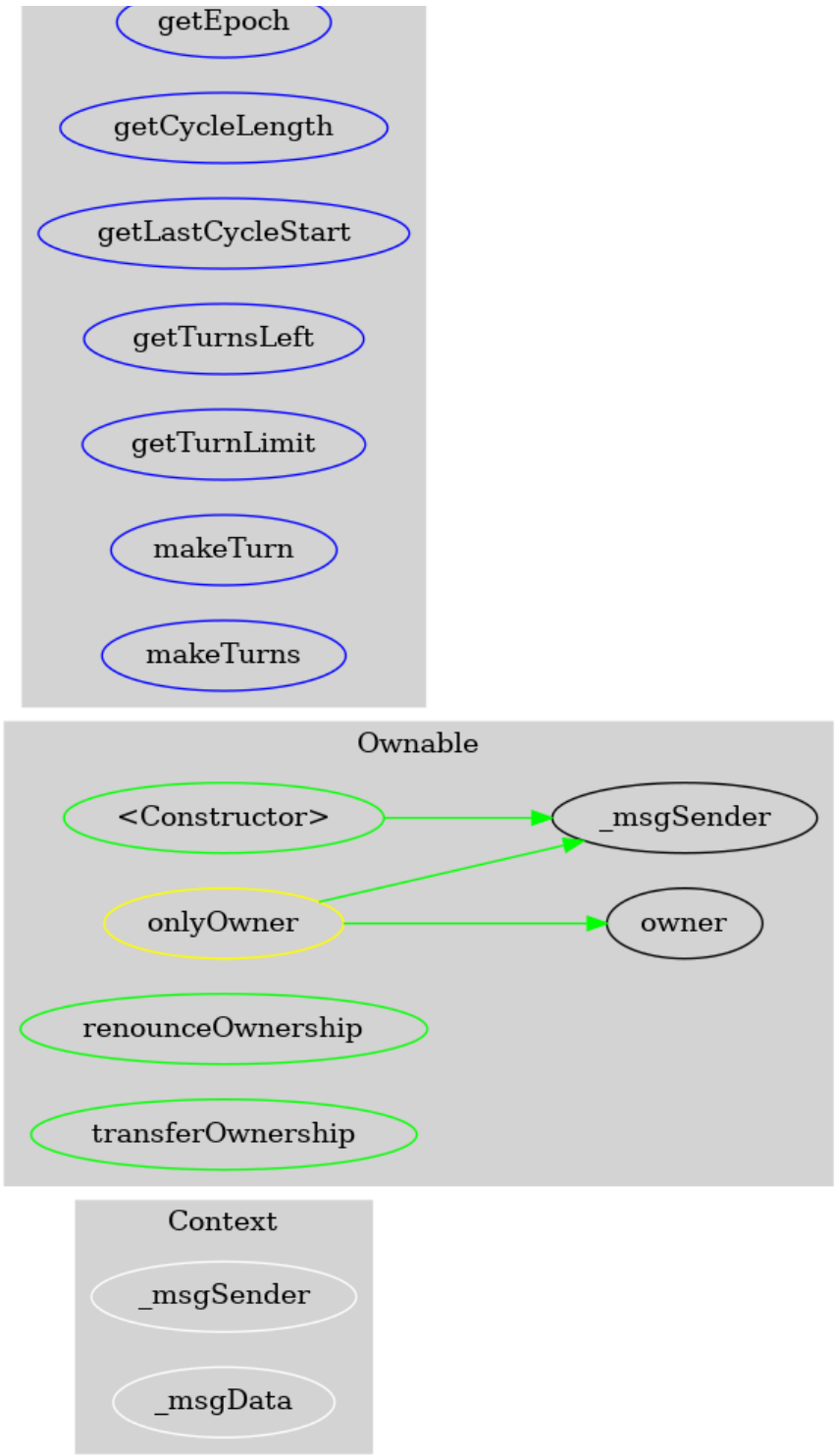

## FUNCTIONS OVERVIEW

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

Int = Internal
Ext = External
Pub = Public

+  ReentrancyGuard
   - [Pub]  #

+  Context
   - [Int] _msgSender
   - [Int] _msgData
```

```
    - [Pub] owner
    - [Pub] renounceOwnership #
       - modifiers: onlyOwner
    - [Pub] transferOwnership #
       - modifiers: onlyOwner

+ [Int] IGameTreasury
    - [Ext] getPctShamans
    - [Ext] getPctWinners
    - [Ext] getPctProphet
    - [Ext] getTurnFee
    - [Ext] getTreasuryDistributions
    - [Ext] ensureFees ($)
    - [Ext] updateTurnFee #
    - [Ext] pay #

+  GameTreasury (Ownable, IGameTreasury, ReentrancyGuard)
    - [Pub]  #
    - [Ext]  ($)
    - [Ext] getPctShamans
    - [Ext] getPctWinners
    - [Ext] getPctProphet
    - [Ext] getTurnFee
    - [Ext] getTreasuryDistributions
    - [Ext] ensureFees ($)
```

## DETAILS: TIMER.SOL

### FUNCTION GRAPH




## INHERITENCE CHART

# FUNCTIONS OVERVIEW

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

Int = Internal
Ext = External
Pub = Public

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

+  Ownable (Context)
   - [Pub]  #
   - [Pub] owner
   - [Pub] renounceOwnership #
      - modifiers: onlyOwner
   - [Pub] transferOwnership #
      - modifiers: onlyOwner

+ [Int] ITimer
   - [Ext] changeCycle #
   - [Ext] changeEpoch #
   - [Ext] getCycle
   - [Ext] getEpoch
   - [Ext] getCycleLength
   - [Ext] getLastCycleStart
   - [Ext] getTurnsLeft
```

```
+  MultiOwnable
   - [Pub]  #
   - [Pub] isOwner
   - [Pub] renounceOwnership #
      - modifiers: onlyOwners
   - [Pub] addOwnership #
      - modifiers: onlyOwners
   - [Pub] removeOwnership #
      - modifiers: onlyOwners

+  Timer (ITimer, MultiOwnable)
   - [Pub]  #
      - modifiers: MultiOwnable
   - [Ext] changeCycle #
   - [Ext] changeEpoch #
      - modifiers: onlyOwners
   - [Ext] getCycle
   - [Ext] getEpoch
   - [Ext] getCycleLength
   - [Ext] getLastCycleStart
   - [Pub] getTurnsLeft
   - [Ext] getTurnLimit
   - [Ext] makeTurn #
      - modifiers: onlyOwners
   - [Ext] makeTurns #
      - modifiers: onlyOwners
   - [Int] _makeTurns #
```

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