SOLIDITY.*FINANCE*

Axion - Audit Report

SUMMARY

AXION

Axion is an ethical, community-driven cryptocurrency that rewards long-term investing with high-yield interest rates and weekly dividends.

We initially reviewed Axion's Auction and Staking contracts at commit 3e6e1a83b440b0e6629dc455667ecb71567455c3 on GitHub. We later updated our findings after the implementation of a series of recommendations, based on commit ae162c056db394a91b89b097b5314e2e705a34f7. The mainnet addresses as of the date of this report are listed below. Please note we have not reviewed other parts of the Axion suite of smart contracts.

- Auction (Current Implementation): 0x8cf5f583d6d35488220f91b9b388e53ba38bbd9d
- Staking (Upgradable Proxy): 0x1920d646574E097c2c487F69F40814F95d45bf8C
- Staking (Current Implementation): 0xf6b44397c8756ed95ff138554e5d6349c62bf885

> *Notes on the Staking Contract:*
>
> - *Token holders can elect to time-lock their Axion tokens into the staking contract in exchange for 'shares', representing a certificate of deposit and a right to future rewards.*
> - *Users select the lockup period for their tokens when depositing their stake, with a maximum duration of slightly over 15 years.*
> - *The amount of shares and rewards a user recieves for their stake depends upon the staker's staked amount of AXN, the total amount staked by all users, the start date of the stake, and the end date of the stake. The base minimum rate of return is 8% APY.*
> - *This calculation also features a share factor that multiplies the amount of shares by a certain value depending on the stake duration: 0-5 years: share factor = 1x; 5-10 years: share factor = 2x; 10-15 years: share factor = 3x. This implies that a user's stake will double after 5 years, triple after 10 years, and*

- *Users also have the ability to utilize their existing Axion V1 stakes (if applicable) to earn rewards in the new staking contract.*
- *Penalties may be incurred by stakers who unstake earlier than their commitment, or who fail to claim their rewards in a timely manner. Penalties have been temporarily suppressed for the launch of the platform.*

Notes on the Auction Contract:

- *Outside of traditional DEXs, Axion Token can be acquired by participating in one of the "Daily Auctions" and spending ETH as a bid for a portion of the Auction pool.*
- *The price of the tokens to be sold at auction are dynamically determined by the amount of tokens for sale and the total amount of ETH that has be deposited for the auction on that paticular day.*
- *A price floor exists for tokens sold in the pool. The minimum price is determined by calculating the time-weighted average price (TWAP) of the token on Uniswap; which is flash loan resistant.*
- *Auction winnings are automatically staked into the staking contract for a minimum of 60 days. Any early unstaking penalties would be sent back to auction.*
- *The Auction has two different modes - Normal and VCA (Venture Capital).*

- *In the normal auction, users contribute ETH which is swapped into Axion (a buyback), which increases the price. The Axion tokens bought are sent to the staking contract to provide rewards to stakers.*
- *The Axion tokens sold in the Daily Auction are sourced from penalties users incur for unstaking early, or not claiming rewards in a timely manner.*
- *When the manager sets the token(s) of the day, they also set percentage(s) of each token along with it and this proportion is used in calculating prices when bidding in the VCA.*

General Notes:

- *The project's GitHub contain a series of passing test cases related to the contracts in scope for this review.*
- *Axion lead developer/maintainer has worked extensively with our team to properly implement our security recommendations.*
- *We have worked with the team to check the addresses assigned to each role on the live contracts to ensure only the proper addresses have control.*
- *Proper structuring of logic to prevent re-entrancy attacks.*
- *Utilization of SafeMath to prevent overflows.*

Audit Findings Summary:

> *and focus on admin control makes us belive they are trustworthy.*
> - *Date: March 10th, 2021*

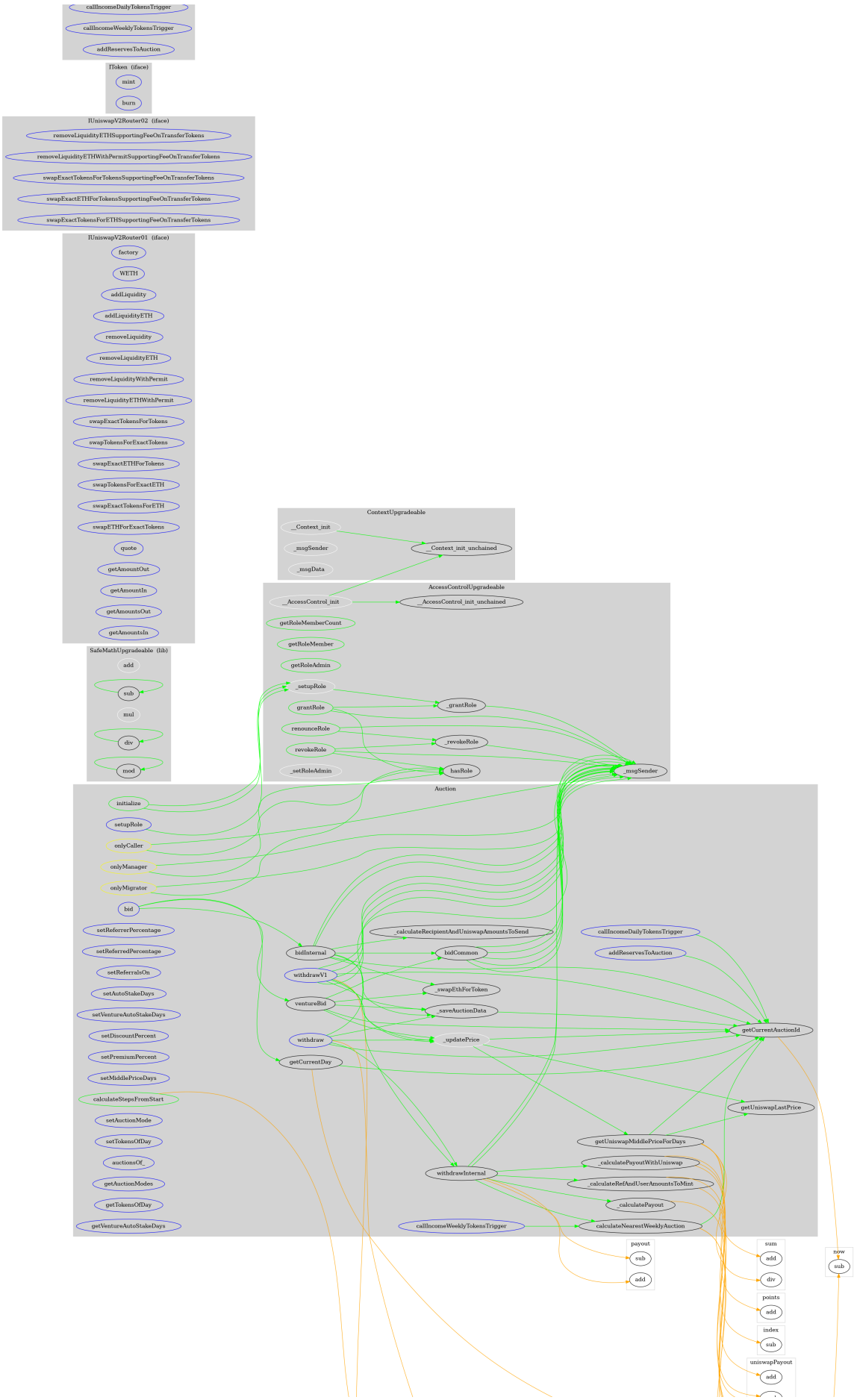
EXTERNAL THREATS - AUDIT RESULTS

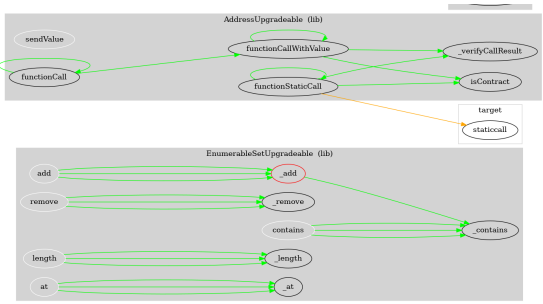
Vulnerability Category	Notes	Result
Arbitrary Storage Write	N/A	PASS
Arbitrary Jump	N/A	PASS
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Deprecated Opcodes	N/A	PASS
Ether Thief	N/A	PASS
Exceptions	N/A	PASS
External Calls	N/A	PASS

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

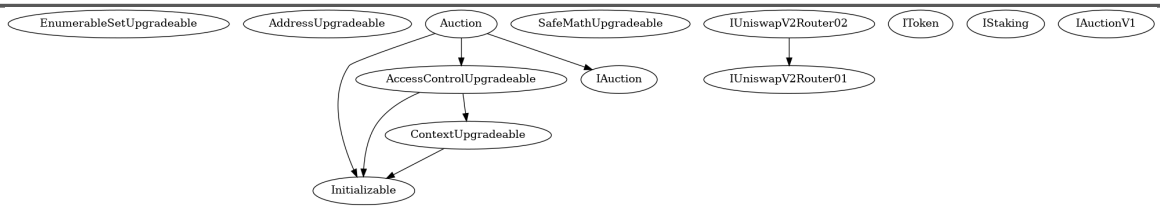
Auction Contract

FUNCTION GRAPH





INHERITENCE CHART



FUNCTIONS OVERVIEW

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

Int = Internal
Ext = External
Pub = Public

+ [Lib] EnumerableSetUpgradeable
   - [Prv] _add #
   - [Prv] _remove #
   - [Prv] _contains
   - [Prv] _length
   - [Prv] _at
   - [Int] add #
```

```
    - [Int] at
    - [Int] add #
    - [Int] remove #
    - [Int] contains
    - [Int] length
    - [Int] at
    - [Int] add #
    - [Int] remove #
    - [Int] contains
    - [Int] length
    - [Int] at

+ [Lib] AddressUpgradeable
    - [Int] isContract
    - [Int] sendValue #
    - [Int] functionCall #
    - [Int] functionCall #
    - [Int] functionCallWithValue #
    - [Int] functionCallWithValue #
    - [Int] functionStaticCall
    - [Int] functionStaticCall
    - [Prv] _verifyCallResult

+  Initializable
    - [Prv] _isConstructor

+  ContextUpgradeable (Initializable)
    - [Int] __Context_init #
       - modifiers: initializer
    - [Int] __Context_init_unchained #
       - modifiers: initializer
```

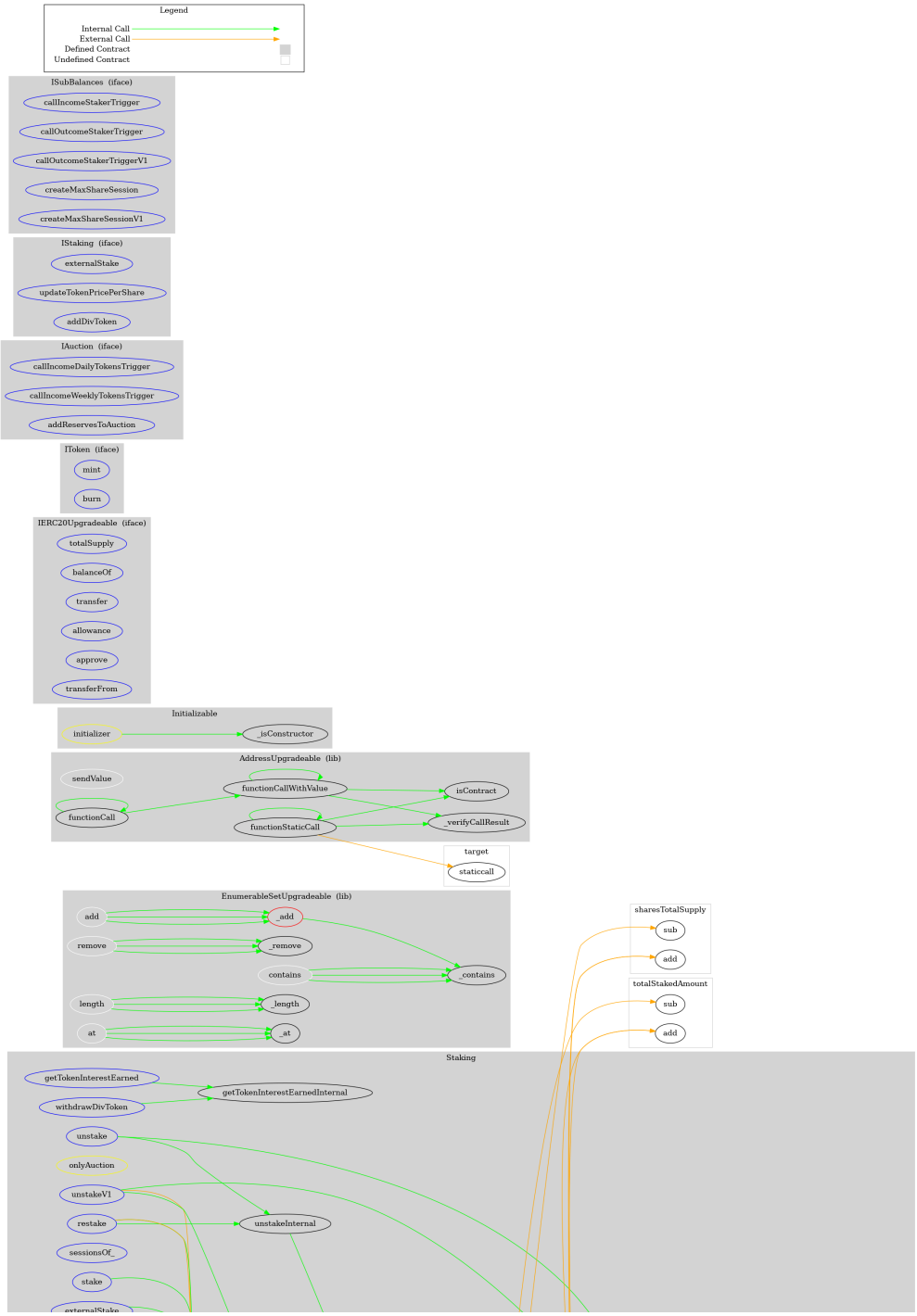
```
+  AccessControlUpgradeable (Initializable, Context
   - [Int] __AccessControl_init #
      - modifiers: initializer
   - [Int] __AccessControl_init_unchained #
      - modifiers: initializer
   - [Pub] hasRole
   - [Pub] getRoleMemberCount
   - [Pub] getRoleMember
   - [Pub] getRoleAdmin
   - [Pub] grantRole #
   - [Pub] revokeRole #
   - [Pub] renounceRole #
   - [Int] _setupRole #
   - [Int] _setRoleAdmin #
   - [Prv] _grantRole #
   - [Prv] _revokeRole #

+ [Lib] SafeMathUpgradeable
   - [Int] add
   - [Int] sub
   - [Int] sub
   - [Int] mul
   - [Int] div
   - [Int] div
   - [Int] mod
   - [Int] mod

+ [Int] IUniswapV2Router01
   - [Ext] factory
   - [Ext] WETH
   - [Ext] addLiquidity #
```

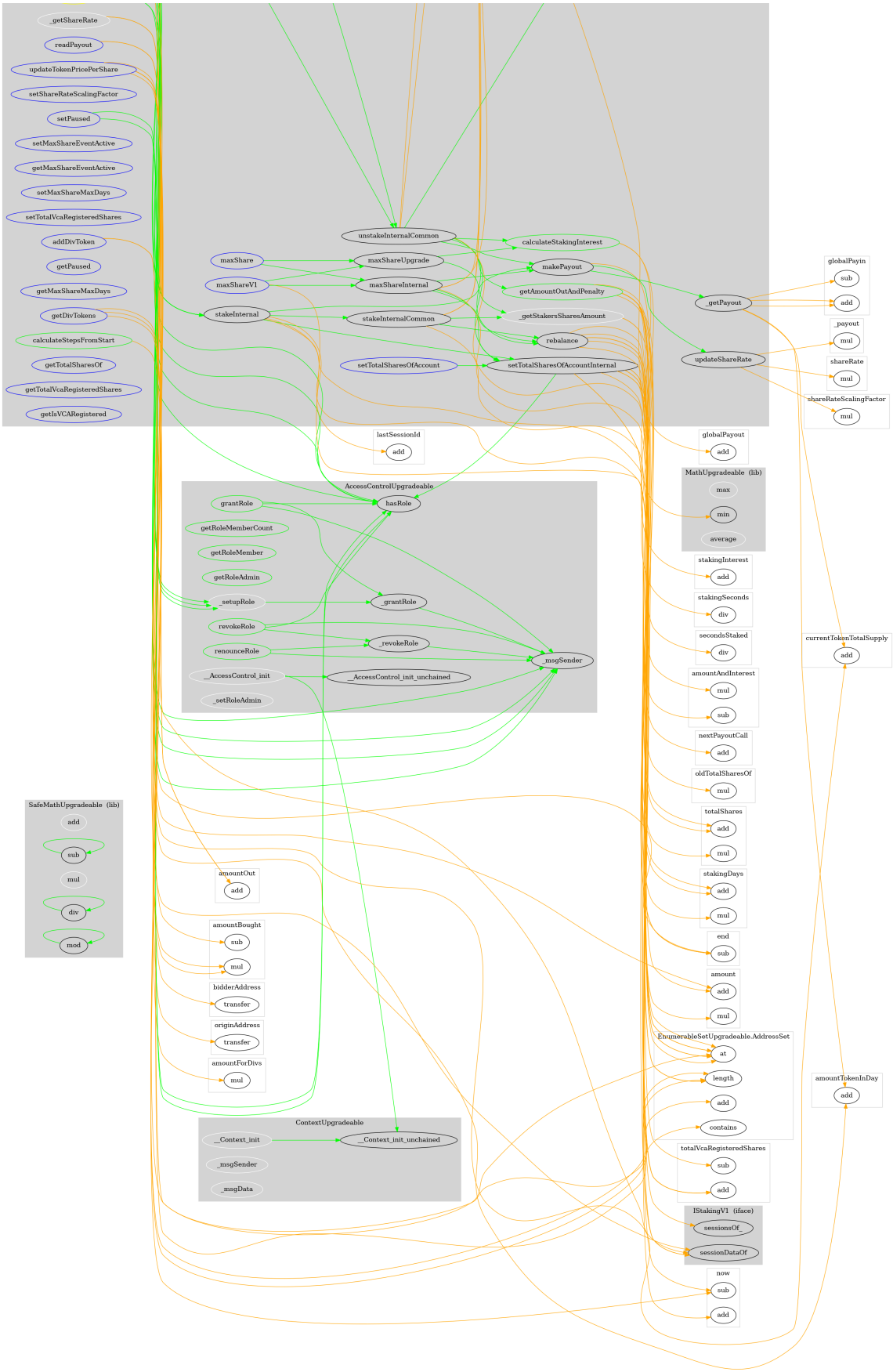
```
    - [Ext] removeLiquidityWithPermit #
    - [Ext] removeLiquidityETHWithPermit #
    - [Ext] swapExactTokensForTokens #
    - [Ext] swapTokensForExactTokens #
    - [Ext] swapExactETHForTokens ($)
    - [Ext] swapTokensForExactETH #
    - [Ext] swapExactTokensForETH #
    - [Ext] swapETHForExactTokens ($)
    - [Ext] quote
    - [Ext] getAmountOut
    - [Ext] getAmountIn
    - [Ext] getAmountsOut
    - [Ext] getAmountsIn

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
    - [Ext] removeLiquidityETHSupportingFeeOnTransfe
    - [Ext] removeLiquidityETHWithPermitSupportingFe
    - [Ext] swapExactTokensForTokensSupportingFeeOnT
    - [Ext] swapExactETHForTokensSupportingFeeOnTran
    - [Ext] swapExactTokensForETHSupportingFeeOnTran

+ [Int] IToken
    - [Ext] mint #
    - [Ext] burn #

+ [Int] IAuction
    - [Ext] callIncomeDailyTokensTrigger #
    - [Ext] callIncomeWeeklyTokensTrigger #
    - [Ext] addReservesToAuction #

+ [Int] IStaking
```

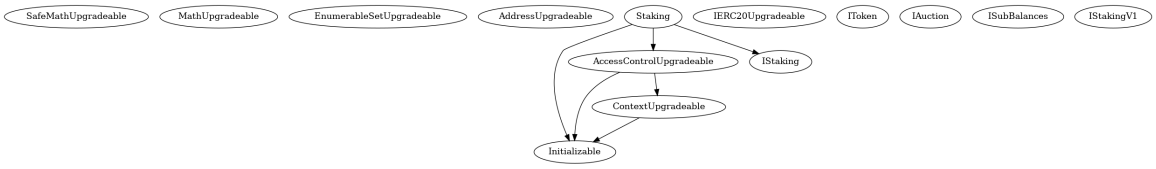
```
+ [Int] IAuctionV1
   - [Ext] auctionBetOf #

+  Auction (IAuction, Initializable, AccessControlU
   - [Int] _updatePrice #
   - [Prv] _swapEthForToken #
   - [Ext] bid ($)
   - [Int] bidInternal #
   - [Int] ventureBid #
   - [Int] bidCommon #
   - [Int] getUniswapLastPrice
   - [Int] getUniswapMiddlePriceForDays
   - [Ext] withdraw #
   - [Ext] withdrawV1 #
   - [Int] withdrawInternal #
   - [Ext] callIncomeDailyTokensTrigger #
      - modifiers: onlyCaller
   - [Ext] addReservesToAuction #
      - modifiers: onlyCaller
   - [Ext] callIncomeWeeklyTokensTrigger #
      - modifiers: onlyCaller
   - [Pub] calculateNearestWeeklyAuction
   - [Int] getCurrentDay
   - [Pub] getCurrentAuctionId
   - [Pub] calculateStepsFromStart
   - [Int] _calculatePayoutWithUniswap
   - [Int] _calculatePayout
   - [Prv] _calculateRecipientAndUniswapAmountsToSe
   - [Prv] _calculateRefAndUserAmountsToMint
   - [Int] _saveAuctionData #
```

Staking Contract

FUNCTION GRAPH







FUNCTIONS OVERVIEW

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

Int = Internal
Ext = External
Pub = Public

+ [Lib] SafeMathUpgradeable
   - [Int] add
   - [Int] sub
   - [Int] sub
   - [Int] mul
   - [Int] div
   - [Int] div
   - [Int] mod
   - [Int] mod

+ [Lib] MathUpgradeable
   - [Int] max
   - [Int] min
   - [Int] average

+ [Lib] EnumerableSetUpgradeable
```

```
    - [Prv] _at
    - [Int] add #
    - [Int] remove #
    - [Int] contains
    - [Int] length
    - [Int] at
    - [Int] add #
    - [Int] remove #
    - [Int] contains
    - [Int] length
    - [Int] at
    - [Int] add #
    - [Int] remove #
    - [Int] contains
    - [Int] length
    - [Int] at

+ [Lib] AddressUpgradeable
    - [Int] isContract
    - [Int] sendValue #
    - [Int] functionCall #
    - [Int] functionCall #
    - [Int] functionCallWithValue #
    - [Int] functionCallWithValue #
    - [Int] functionStaticCall
    - [Int] functionStaticCall
    - [Prv] _verifyCallResult

+  Initializable
    - [Prv] _isConstructor
```

```
    - [Int] __Context_init_unchained #
       - modifiers: initializer
    - [Int] _msgSender
    - [Int] _msgData

+  AccessControlUpgradeable (Initializable, Context
    - [Int] __AccessControl_init #
       - modifiers: initializer
    - [Int] __AccessControl_init_unchained #
       - modifiers: initializer
    - [Pub] hasRole
    - [Pub] getRoleMemberCount
    - [Pub] getRoleMember
    - [Pub] getRoleAdmin
    - [Pub] grantRole #
    - [Pub] revokeRole #
    - [Pub] renounceRole #
    - [Int] _setupRole #
    - [Int] _setRoleAdmin #
    - [Prv] _grantRole #
    - [Prv] _revokeRole #

+ [Int] IERC20Upgradeable
    - [Ext] totalSupply
    - [Ext] balanceOf
    - [Ext] transfer #
    - [Ext] allowance
    - [Ext] approve #
    - [Ext] transferFrom #

+ [Int] IToken
```

```
+ [Int] IAuction
   - [Ext] callIncomeDailyTokensTrigger #
   - [Ext] callIncomeWeeklyTokensTrigger #
   - [Ext] addReservesToAuction #

+ [Int] IStaking
   - [Ext] externalStake #
   - [Ext] updateTokenPricePerShare ($)
   - [Ext] addDivToken #

+ [Int] ISubBalances
   - [Ext] callIncomeStakerTrigger #
   - [Ext] callOutcomeStakerTrigger #
   - [Ext] callOutcomeStakerTriggerV1 #
   - [Ext] createMaxShareSession #
   - [Ext] createMaxShareSessionV1 #

+ [Int] IStakingV1
   - [Ext] sessionDataOf
   - [Ext] sessionsOf_

+  Staking (IStaking, Initializable, AccessControlU
   - [Pub] initialize #
      - modifiers: initializer
   - [Ext] sessionsOf_
   - [Ext] stake #
      - modifiers: pausable
   - [Ext] externalStake #
      - modifiers: onlyExternalStaker,pausable
   - [Int] stakeInternal #
   - [Int] _initPayout #
```

```
- [Ext] unstakeV1 #
   - modifiers: pausable
- [Pub] getAmountOutAndPenalty
- [Pub] makePayout #
- [Ext] readPayout
- [Int] _getPayout #
- [Int] _getStakersSharesAmount
- [Int] _getShareRate
- [Ext] restake #
   - modifiers: pausable
- [Ext] restakeV1 #
   - modifiers: pausable
- [Int] unstakeInternal #
- [Int] unstakeV1Internal #
- [Int] unstakeInternalCommon #
- [Int] stakeInternalCommon #
- [Ext] withdrawDivToken #
- [Ext] getTokenInterestEarned
- [Int] getTokenInterestEarnedInternal
- [Int] rebalance #
- [Int] setTotalSharesOfAccountInternal #
   - modifiers: pausable
- [Ext] setTotalSharesOfAccount #
- [Ext] updateTokenPricePerShare ($)
   - modifiers: onlyAuction
- [Ext] addDivToken #
   - modifiers: onlyAuction
- [Int] updateShareRate #
- [Ext] setShareRateScalingFactor #
```

- Declaration of variables as constant and functions external to save gas.

Staking Contract:

- Rearrange logic in function stakeInternal() to save gas.
- Rearrange logic in function withdrawDivToken(tokenAddress) to prevent potential reentrancy attacks.