SOLIDITY.*FINANCE*

Predictz - Smart Contract Audit Report

SUMMARY

Predictz is a Defi token sale platform. Predictz provides a decentralized auction protocol with multilayered system of safeguards against project failure. Predictz seeks to maximise the capacity of decentralised finance by eliminating the middle men from financial transactions and pass on their earnings to the token holders in a sustainable, trust-less and decentralised manner

> *Notable features included in the contract:*
>
> - *List tokens through the contracts and allow users to buy/swap for tokens for a small set fee.*
> - *Ownership - Some functions are protected and can only be called by the contract owner. The deployer and future owners can transfer ownership to any address.*
> - *Owners have the ability to withdraw ether & ERC20s from the Dex contract.*
> - *Owners declare the results for predictions.*
> - *Utilization of SafeMath to prevent overflows.*
>
> *Audit Findings Summary*

- *The owner of the PredictzDex contract can withdraw the ether or any tokens sent to the contract.*
- *The owner of the FSTPrediction contract declares the results for markets. Ensure trust in the owner.*
- *No security issues from external attackers were identified.*
- *Date: November 13th, 2020.*

COMBINED AUDIT RESULTS

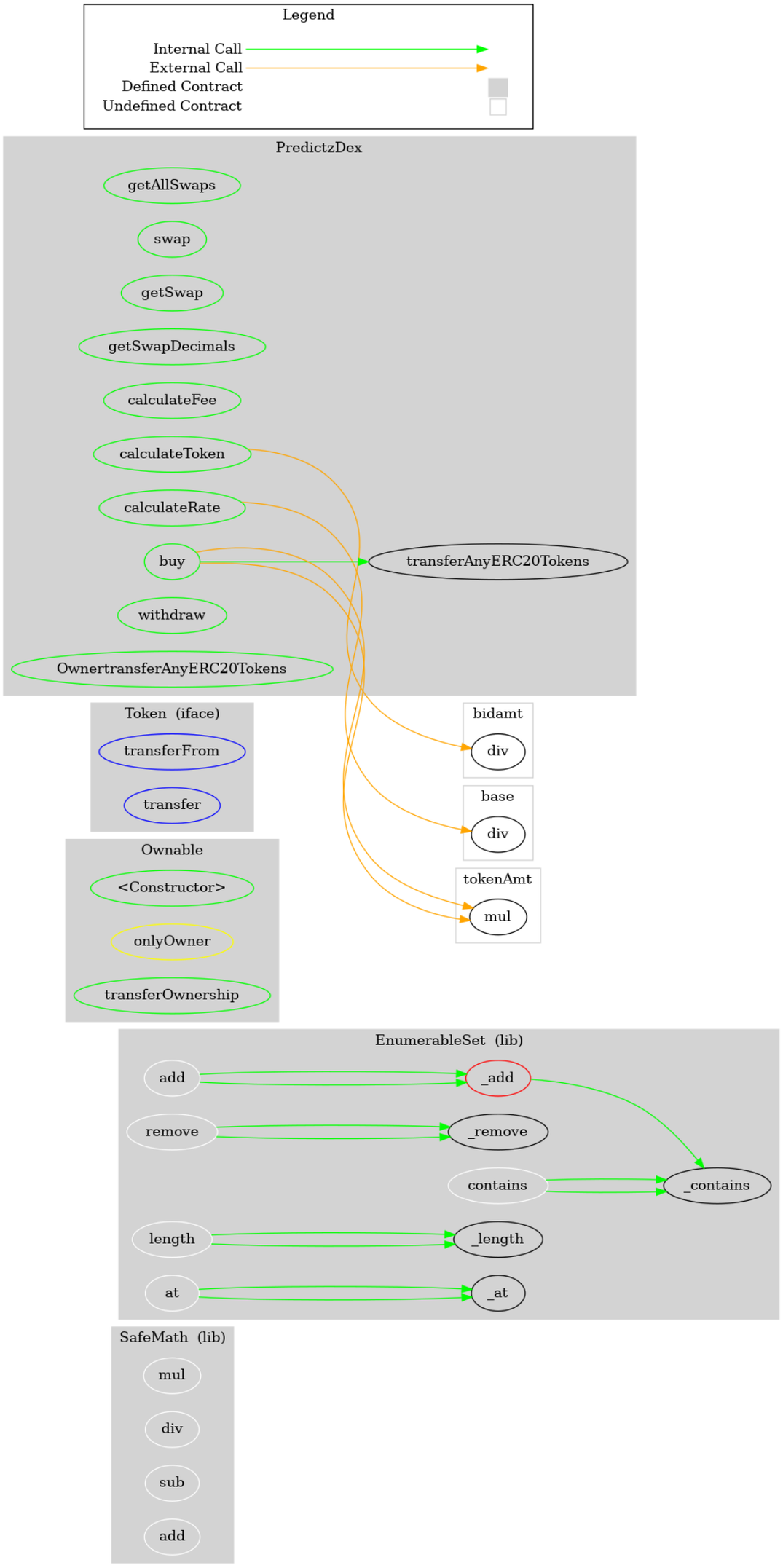
We ran over 400,000 transactions interacting with this suite of contracts on a test blockchain to determine these results.
Date: November 13th, 2020

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*
Integer Over/Underflow	*N/A*	*PASS*
Multiple Sends	*N/A*	*PASS*

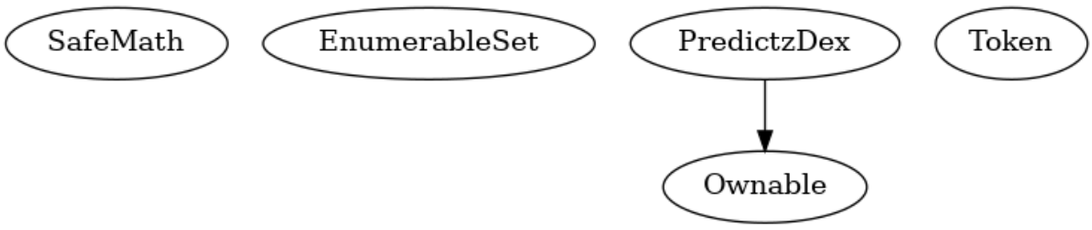
Vulnerability Category	Notes	Result
Suicide	*N/A*	*PASS*
State Change External Calls	*N/A*	*PASS*
Unchecked Retval	*N/A*	*PASS*

DETAILS: PREDICTZDEX

FUNCTION GRAPH


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
PredictzDex
getAllSwaps
swap
getSwap
getSwapDecimals
calculateFee
calculateToken
calculateRate
buy
withdraw
OwnertransferAnyERC20Tokens
transferAnyERC20Tokens
Token (iface)
transferFrom
transfer
Ownable
<Constructor>
onlyOwner
transferOwnership
bidamt
div
base
div
tokenAmt
mul
EnumerableSet (lib)
add
_add
remove
_remove
contains
_contains
length
_length
at
_at
SafeMath (lib)
mul
div
sub
add

INHERITENCE CHART



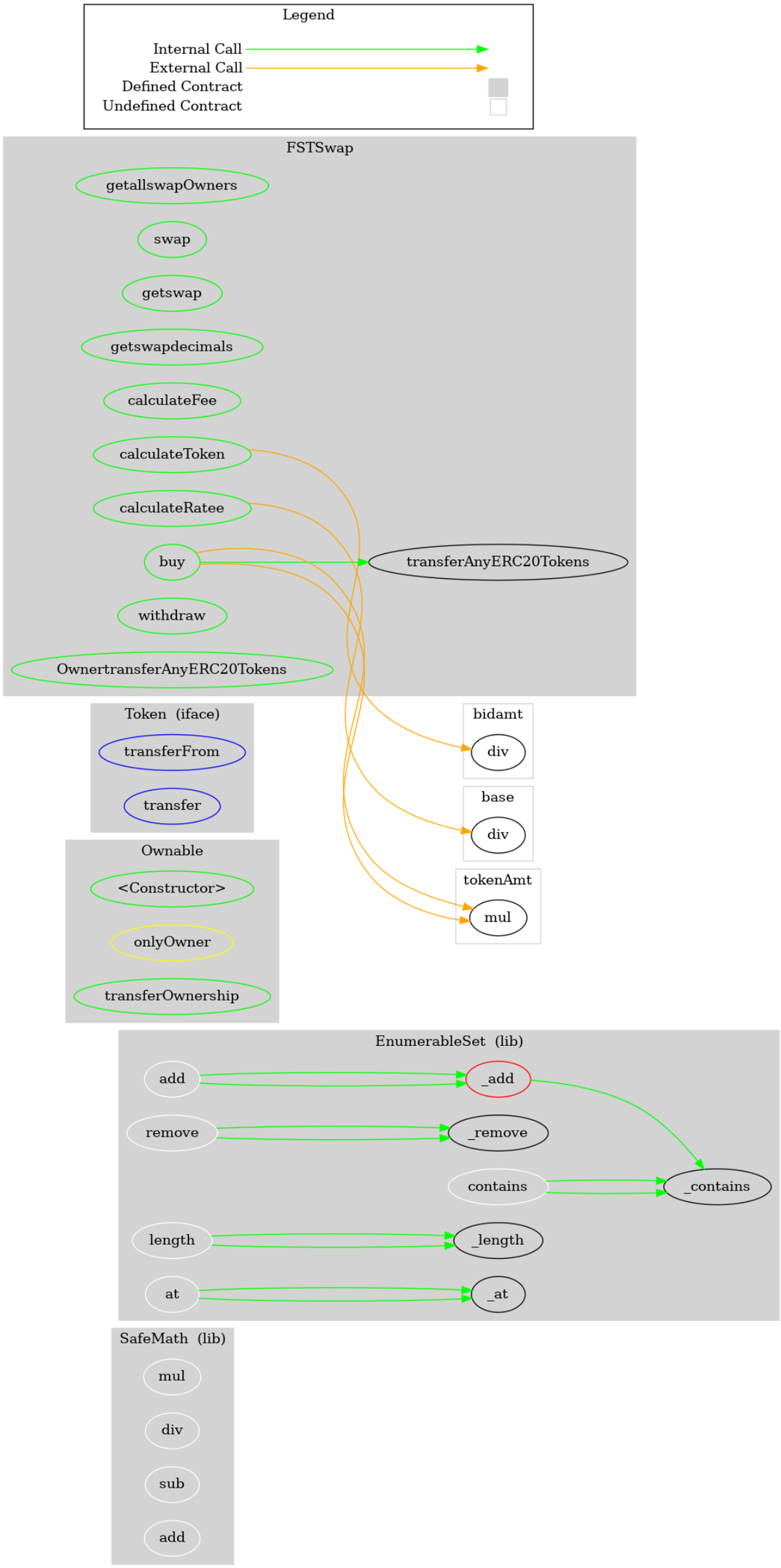
FUNCTIONS OVERVIEW

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

Int = Internal
Ext = External
Pub = Public

+ [Lib] SafeMath
   - [Int] mul
   - [Int] div
   - [Int] sub
   - [Int] add

+ [Lib] EnumerableSet
   - [Prv] _add #
   - [Prv] _remove #
   - [Prv] _contains
   - [Prv] _length
   - [Prv] _at
   - [Int] add #
   - [Int] remove #
   - [Int] contains
   - [Int] length
   - [Int] at
   - [Int] add #
   - [Int] remove #
   - [Int] contains
   - [Int] length
```

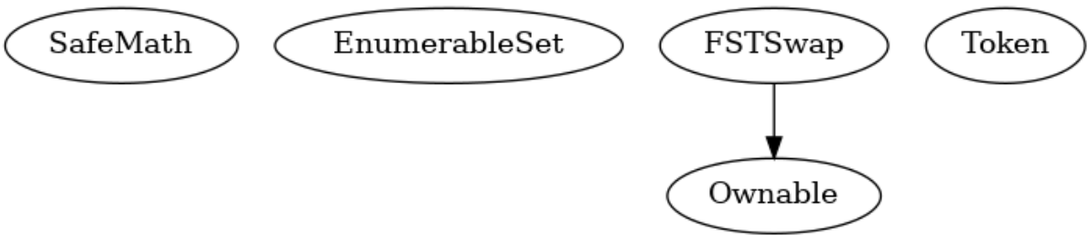
```
    - [Int] at

+  Ownable
    - [Pub]  #
    - [Pub] transferOwnership #
       - modifiers: onlyOwner

+ [Int] Token
    - [Ext] transferFrom #
    - [Ext] transfer #

+  PredictzDex (Ownable)
    - [Pub] getAllSwaps
    - [Pub] swap #
    - [Pub] getSwap
    - [Pub] getSwapDecimals
    - [Pub] calculateFee
    - [Pub] calculateToken
    - [Pub] calculateRate
    - [Pub] buy ($)
    - [Pub] withdraw #
       - modifiers: onlyOwner
    - [Prv] transferAnyERC20Tokens #
    - [Pub] OwnertransferAnyERC20Tokens #
       - modifiers: onlyOwner
```

DETAILS: FSTSWAP

FUNCTION GRAPH


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
FSTSwap
getallswapOwners
swap
getswap
getswapdecimals
calculateFee
calculateToken
calculateRatee
buy
withdraw
OwnertransferAnyERC20Tokens
transferAnyERC20Tokens
Token (iface)
transferFrom
transfer
Ownable
<Constructor>
onlyOwner
transferOwnership
bidamt
div
base
div
tokenAmt
mul
EnumerableSet (lib)
add
_add
remove
_remove
contains
_contains
length
_length
at
_at
SafeMath (lib)
mul
div
sub
add

INHERITENCE CHART



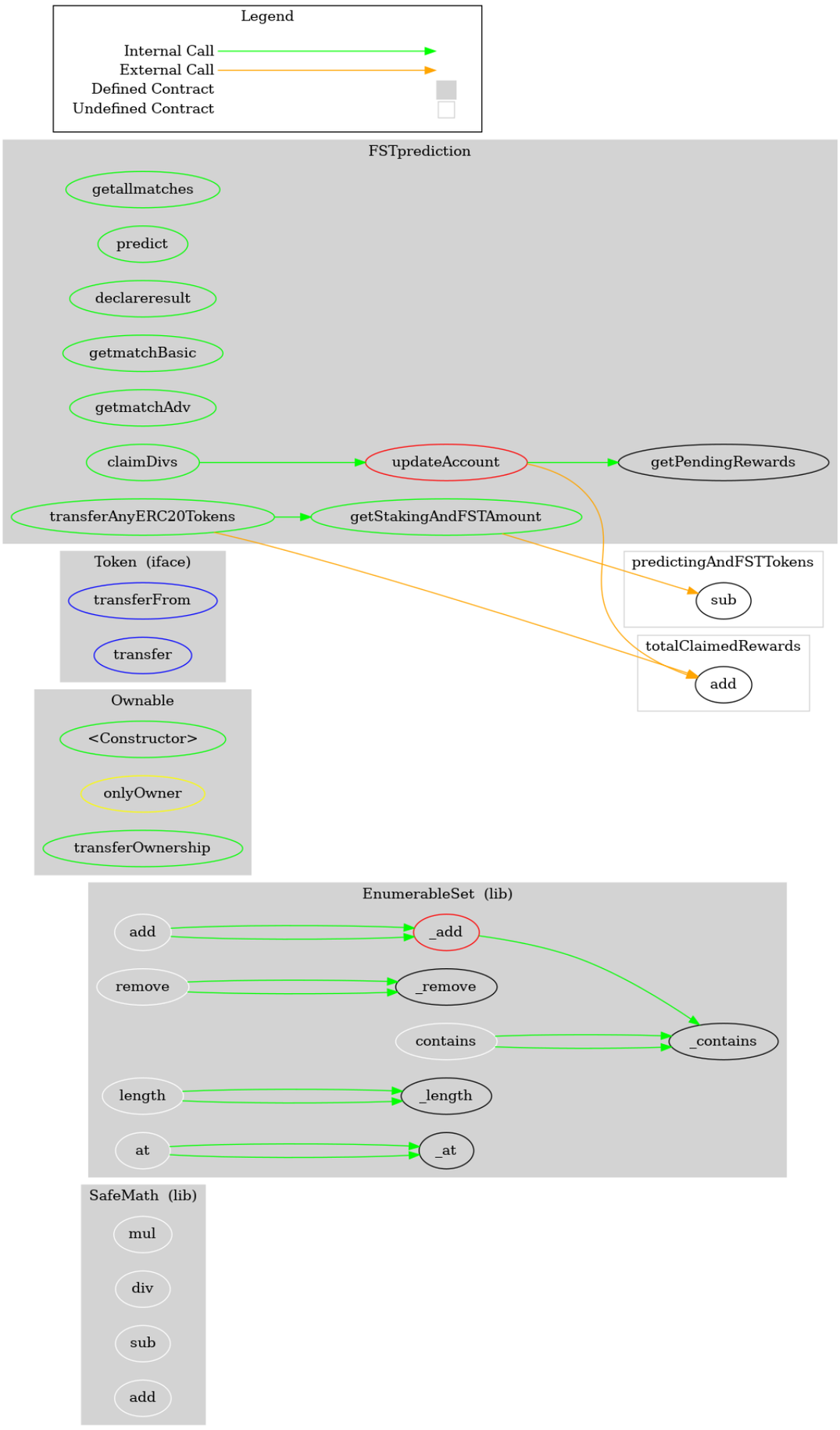
FUNCTIONS OVERVIEW

```
 + [Lib] SafeMath
    - [Int] mul
    - [Int] div
    - [Int] sub
    - [Int] add

 + [Lib] EnumerableSet
    - [Prv] _add #
    - [Prv] _remove #
    - [Prv] _contains
    - [Prv] _length
    - [Prv] _at
    - [Int] add #
    - [Int] remove #
    - [Int] contains
    - [Int] length
    - [Int] at
    - [Int] add #
    - [Int] remove #
    - [Int] contains
    - [Int] length
    - [Int] at

 +  Ownable
    - [Pub]  #
    - [Pub] transferOwnership #
       - modifiers: onlyOwner
```

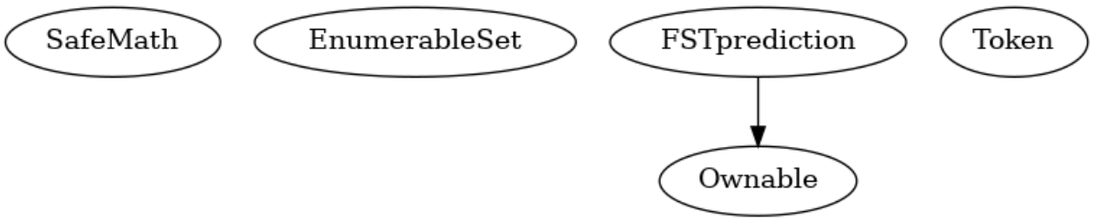
```
+ [Int] Token
   - [Ext] transferFrom #
   - [Ext] transfer #

+  FSTSwap (Ownable)
   - [Pub] getallswapOwners
   - [Pub] swap #
   - [Pub] getswap
   - [Pub] getswapdecimals
   - [Pub] calculateFee
   - [Pub] calculateToken
   - [Pub] calculateRatee
   - [Pub] buy ($)
   - [Pub] withdraw #
      - modifiers: onlyOwner
   - [Prv] transferAnyERC20Tokens #
   - [Pub] OwnertransferAnyERC20Tokens #
      - modifiers: onlyOwner
```

DETAILS: FSTPREDICTION

FUNCTION GRAPH



INHERITENCE CHART



FUNCTIONS OVERVIEW

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

Int = Internal
Ext = External
Pub = Public

+ [Lib] SafeMath
   - [Int] mul
   - [Int] div
   - [Int] sub
   - [Int] add

+ [Lib] EnumerableSet
   - [Prv] _add #
   - [Prv] _remove #
   - [Prv] _contains
   - [Prv] _length
   - [Prv] _at
   - [Int] add #
   - [Int] remove #
   - [Int] contains
   - [Int] length
   - [Int] at
   - [Int] add #
   - [Int] remove #
   - [Int] contains
   - [Int] length
   - [Int] at

+  Ownable
```

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

+ [Int] Token
    - [Ext] transferFrom #
    - [Ext] transfer #

+  FSTprediction (Ownable)
    - [Pub] getallmatches
    - [Pub] predict #
    - [Pub] declareresult #
       - modifiers: onlyOwner
    - [Pub] getmatchBasic
    - [Pub] getmatchAdv
    - [Pub] getPendingRewards
    - [Prv] updateAccount #
    - [Pub] claimDivs #
    - [Pub] getStakingAndFSTAmount
    - [Pub] transferAnyERC20Tokens #
       - modifiers: onlyOwner
```

PRINT EXPANDED SECTIONS

GO HOME

FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. WE DO NOT ENDORSE ANY OF THE PROJECTS LISTED. THE HOSTS OF THIS WEBSITE AND PRODUCERS OF THESE REPORTS DO NOT ENDORSE ANY OF THE PROJECTS LISTED. THIS IS NOT INVESTMENT ADVICE. BY USING THIS WEBSITE YOU AGREE TO THESE TERMS.