Auditoria Tokens

“Goal Stadium”

Miguel Ángel Mora Tudela
CIBINAR – CIBERSEGURIDAD E INTELIGENCIA ARITIFICAL

CONTRATO INTELIGENTE DE CRIPTOMONEDAS

INFORME DE ANÁLISIS DE CÓDIGO Y ANÁLISIS DE VULNERABILIDADES

Cliente: GoalStadium
Realizado en fecha: 17 de diciembre de 2021
Plataforma: GoalStadium and Smart Contract
Lenguaje: Solidity

ÍNDICE DE CONTENIDOS

1. Integridad de los contratos

Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol MD5

dd2a9892dd140e2dc2707d03994236dd

Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol SHA1

9916ba9b0a646609a59ae1313584b51c4d1970d6

Se incluye la huella MD5 y la huella SHA1 del fichero analizado para validar la integridad del mismo. Así mismo, si hubiera algún cambio en éste, las huellas se modificarían y el resultado de esta auditoría quedaría invalidado.

2. Resumen de auditoría y características

La auditoría de contrato inteligente es un proceso de estudio cuidadoso del código, es decir, se lleva a cabo el descubrimiento de errores, vulnerabilidades y riesgos antes de implementarlo y usarlo. De esta manera, el código no puede volver a modificarse una vez se ha publicado.

Para ello, se han utilizado las siguientes herramientas: Myth, Slither y RemixIDE. Más adelante, se presentarán y se comentarán las principales características.

Más adelante, se presentará y se comentará las principales características.

3. Presentación de las herramientas utilizadas

3.1 Presentación de las herramientas usadas en el contrato inteligente

Para verificar la seguridad del contrato usaremos Myth, Slither y RemixIDE. Los cuáles son frameworks con dependencias con el compilador de Solidity y tienen como finalidad proveer una serie de métricas para detectar diferentes tipos de vulnerabilidades. Las principales funcionalidades de estas tres herramientas son:

Myth	**Slither**
- Detecta vulnerabilidades de seguridad en contratos para Ethereum, Hedera, Quorum, Vechain, Roostock y Tron - Utiliza ejecución simbólica, resolución SMT y análisis de contaminación - Se utiliza en combinación con otras herramientas y técnicas en MythX	- Detecta los falsos positivos - Localiza de manera precisa los errores del código - Cubre el 99,9 % del código de Solidity - La media de ejecución es rápida

RemixIDE
- Proporciona una manera fácil de leer el AST de contrato inteligente escrito en Solidity - Cuenta con un conjunto de bibliotecas que pueden ser usadas en distintos módulos con el objetivo de llevar a cabo el análisis - Proporciona la posibilidad de importar un contrato inteligente desde distintoa repositortios

4. Vulnerabilidades encontradas en el contrato inteligente

El alcance del contrato inteligente es el análisis de la calidad del código, que permite descubrir posibles errores, vulnerabilidades y riesgos. Este alcance está definido en las siguientes categorías: Security, Gas & Economy, ERC y Miscellaneous.

RemixIDE

Security

Potential violation of Checks-Effects-Interaction pattern in Address._functionCallWithValues(address,bytes,uint256.string): Could potentially lead to re-entrancy vulnerability.

Note: Modifiers are currently not considered by this static analysis.

```
 function _functionCallWithValue(address target, bytes memory data, uint256
weiValue, string memory errorMessage) private returns (bytes memory) {
        require(isContract(target), "Address: call to non-contract");
        // solhint-disable-next-line avoid-low-level-calls
        (bool success, bytes memory returndata) = target.call{ value:
weiValue }(data);
        if (success) {
            return returndata;
        } else {
            // Look for revert reason and bubble it up if present
            if (returndata.length > 0) {
                // The easiest way to bubble the revert reason is using memory via
assembly
                // solhint-disable-next-line no-inline-assembly
                assembly {
                    let returndata_size := mload(returndata)
                    revert(add(32, returndata), returndata_size)
                }
            } else {
                revert(errorMessage);
            }
        }
    }
}
```

Potential violation of Checks-Effects-Interaction pattern in GOALSTADIUM.(): Could potentially lead to re-entrancy vulnerability.

Note: Modifiers are currently not considered by this static analysis.

```
 function name() public view returns (string memory) {
    return _name;
  }
  function symbol() public view returns (string memory) {
    return _symbol;
  }
  function decimals() public view returns (uint8) {
    return _decimals;
  }
  function totalSupply() public view override returns (uint256) {
    return _tTotal;
  }
  function balanceOf(address account) public view override returns (uint256) {
    if (_isExcludedRewards[account]) return _tOwned[account];
    return tokenFromReflection(_rOwned[account]);
  }
  function transfer(address recipient, uint256 amount) public override returns
(bool) {
    _transfer(_msgSender(), recipient, amount);
    return true;
  }
  function allowance(address owner, address spender) public view override
returns (uint256) {
    return _allowances[owner][spender];
  }
  function approve(address spender, uint256 amount) public override returns
(bool) {
    _approve(_msgSender(), spender, amount);
    return true;
  }
```

Potential violation of Checks-Effects-Interaction pattern in GOALSTADIUM.projectFundingSwap(uint 256): Could potentially lead to re-entrancy vulnerability.

Note: Modifiers are currently not considered by this static analysis.

```
 path[1] = uniswapV2Router.WETH();
    _approve(address(this), address(uniswapV2Router), tokenAmount);
```

```
        // make the swap
 uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
            tokenAmount,
            0, // accept any amount of ETH
            path,
            address(this),
            block.timestamp
        );
    }

    function addLiquidity(uint256 tokenAmount, uint256 ethAmount) private {
        // approve token transfer to cover all possible scenarios
        _approve(address(this), address(uniswapV2Router), tokenAmount);
        // add the liquidity
        uniswapV2Router.addLiquidityETH{value: ethAmount}(
            address(this),
            tokenAmount,
            0, // slippage is unavoidable
            0, // slippage is unavoidable
            owner(),
            block.timestamp
        );
    }
```

Potential violation of Checks-Effects-Interaction pattern in GOALSTADIUM.swapTokensForBNB(uint 256): Could potentially lead to re-entrancy vulnerability.

Note: Modifiers are currently not considered by this static analysis

```
            owner(),
            block.timestamp
        );
    }

    // this method is responsible for taking all fee, if takeAllFees is true
    function _tokenTransfer(address sender, address recipient, uint256 amount,bool
takeAllFees) private {
        if(!takeAllFees)
            removeAllFees();
        if (_isExcludedRewards[sender] && !_isExcludedRewards[recipient]) {
            _transferFromExcluded(sender, recipient, amount);
        } else if (!_isExcludedRewards[sender] && _isExcludedRewards[recipient]) {
            _transferToExcluded(sender, recipient, amount);
        } else if (!_isExcludedRewards[sender] && !_isExcludedRewards[recipient]) {
```

```
        _transferStandard(sender, recipient, amount);
    } else if (_isExcludedRewards[sender] && _isExcludedRewards[recipient]) {
        _transferBothExcluded(sender, recipient, amount);
    } else {
        _transferStandard(sender, recipient, amount);
    }
```

The Contract uses inline assembly, this is only advised in rare cases.

Additionally static analysis modules do not parse inline Assembly, this can lead to wrong analysis results.

```
function isContract(address account) internal view returns (bool) {
    // According to EIP-1052, 0x0 is the value returned for not-yet created accounts
    // and 0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470 is returned
    // for accounts without code, i.e. `keccak256('')`
    bytes32 codehash;
    bytes32 accountHash = 0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470;
    // solhint-disable-next-line no-inline-assembly
    assembly { codehash := extcodehash(account) }
    return (codehash != accountHash && codehash != 0x0);
}
```

The Contract uses inline assembly, this is only advised in rare cases.

Additionally static analysis modules do not parse inline Assembly, this can lead to wrong analysis results.

```
else {
        // Look for revert reason and bubble it up if present
        if (returndata.length > 0) {
            // The easiest way to bubble the revert reason is using memory via

            // solhint-disable-next-line no-inline-assembly
            assembly {
                let returndata_size := mload(returndata)
                revert(add(32, returndata), returndata_size)
            }
        } else {
            revert(errorMessage);
```

```
        }
```

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree.

That means that a miner can "choose" the block.timestamp to a certain degree to change the outcome of a transaction in the mined block.

```
        if (from != uniswapV2Pair && to != uniswapV2Pair) {
            isTrade = false;

            if (BridgeOrExchange[from]) {
                projectFee = BridgeOrExchange_ProjectFee[from];
                reflectionsFee = BridgeOrExchange_ReflectionsFee[from];
            }
            else if (BridgeOrExchange[to]) {
                projectFee = BridgeOrExchange_ProjectFee[to];
                reflectionsFee = BridgeOrExchange_ReflectionsFee[to];
            }
            else {
                projectFee = transfer_ProjectFee;
                reflectionsFee = transfer_ReflectionsFee;

                if (antiDump_SellWait_Enabled) {
                // To prevent evading the sell waiting time by sending to
                // another wallet and then selling from it we set a sell
                // waiting time also for the transfer recipient wallet
                sell_AllowedTime[to] = block.timestamp +
antiDump_SellWait_Duration_Seconds;
                }
            }
        }
    }
```

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree.

That means that a miner can "choose" the block.timestamp to a certain degree to change the outcome of a transaction in the mined block.

```
function swapTokensForBNB(uint256 tokenAmount) private {
        address[] memory path = new address[](2);
        path[0] = address(this);
        path[1] = uniswapV2Router.WETH();

        _approve(address(this), address(uniswapV2Router), tokenAmount);

        // make the swap
        uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
            tokenAmount,
            0, // accept any amount of ETH
            path,
            address(this),
            block.timestamp
        );
    }
```

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree.

That means that a miner can "choose" the block.timestamp to a certain degree to change the outcome of a transaction in the mined block.

```
// this method is responsible for taking all fee, if takeAllFees is true
    function _tokenTransfer(address sender, address recipient, uint256 amount,bool
takeAllFees) private {
        if(!takeAllFees)
            removeAllFees();

        if (_isExcludedRewards[sender] && !_isExcludedRewards[recipient]) {
            _transferFromExcluded(sender, recipient, amount);
        } else if (!_isExcludedRewards[sender] && _isExcludedRewards[recipient]) {
            _transferToExcluded(sender, recipient, amount);
        } else if (!_isExcludedRewards[sender] && !_isExcludedRewards[recipient]) {
            _transferStandard(sender, recipient, amount);
        } else if (_isExcludedRewards[sender] && _isExcludedRewards[recipient]) {
            _transferBothExcluded(sender, recipient, amount);
        } else {
            _transferStandard(sender, recipient, amount);
        }

        if(!takeAllFees)
            restoreAllFees();
    }
```

Use of “block.timestamp”: “block.timestamp” can be influenced by miners to a certain degree.

That means that a miner can “choose” the block.timestamp to a certain degree to change the outcome of a transaction in the mined block.

```
function _transferStandard(address sender, address recipient, uint256 tAmount) private {
    (uint256 rAmount, uint256 rTransferAmount, uint256 rFee, uint256 tTransferAmount, uint256 tFee, uint256 tLiquidity) = _getValues(tAmount);
    _rOwned[sender] = _rOwned[sender].sub(rAmount);
    _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount);
    _takeProjectFee(tLiquidity);
    _reflectFee(rFee, tFee);
    emit Transfer(sender, recipient, tTransferAmount);
  }
```

Use of “call”:should be avoided whenever possible.
It can lead to unexpected behavior if return value is not handled properly.

Please use Direct Calls via specifying the called contract interface.

```
  function sendValue(address payable recipient, uint256 amount) internal {
    require(address(this).balance >= amount, "Address: insufficient balance");

    // solhint-disable-next-line avoid-low-level-calls, avoid-call-value
    (bool success, ) = recipient.call{ value: amount }("");
    require(success, "Address: unable to send value, recipient may have reverted");
  }
```

Use of “call”: should be avoided whenever possible.
It can lead to unexpected behavior if return value is not handled properly.

Please use Direct Calls via specifying the called contract interface.

```
function _functionCallWithValue(address target, bytes memory data, uint256 weiValue, string memory errorMessage) private returns (bytes memory) {
    require(isContract(target), "Address: call to non-contract");

    // solhint-disable-next-line avoid-low-level-calls
    (bool success, bytes memory returndata) = target.call{ value: weiValue }(data);
    if (success) {
      return returndata;
```

```
        } else {
            // Look for revert reason and bubble it up if present
            if (returndata.length > 0) {
                // The easiest way to bubble the revert reason is using memory via
assembly

                // solhint-disable-next-line no-inline-assembly
                assembly {
                    let returndata_size := mload(returndata)
                    revert(add(32, returndata), returndata_size)
                }
            } else {
                revert(errorMessage);
            }
        }
    }
```

Gas costs:

Gas requirement of function GOALSTADIUM.uniswapV2Router is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

IUniswapV2Router02 public immutable uniswapV2Router;
address public immutable uniswapV2Pair;

Gas requirement of function GOALSTADIUM.uniswapV2Pair is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

IUniswapV2Router02 public immutable uniswapV2Router;
address public immutable uniswapV2Pair;

Gas requirement of function GOALSTADIUM.name is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
   function approve(address spender, uint256 amount) public override returns (bool)
{
      _approve(_msgSender(), spender, amount);
      return true;
   }
   function transferFrom(address sender, address recipient, uint256 amount) public
override returns (bool) {
      _transfer(sender, recipient, amount);
      _approve(sender, _msgSender(),
_allowances[sender][_msgSender()].sub(amount, "Transfer amount exceeds
allowance"));
      return true;
   }
```

Gas requirement of function GOALSTADIUM.symbol is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
   function transferFrom(address sender, address recipient, uint256 amount) public
override returns (bool) {
      _transfer(sender, recipient, amount);
      _approve(sender, _msgSender(),
_allowances[sender][_msgSender()].sub(amount, "Transfer amount exceeds
allowance"));
      return true;
   }
```

Gas requirement of function GOALSTADIUM.balanceOf is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
 function decreaseAllowance(address spender, uint256 subtractedValue) public virtual returns (bool) {
        _approve(_msgSender(), spender, _allowances[_msgSender()][spender].sub(subtractedValue, "Decreased allowance below zero"));
        return true;
    }
```

Gas requirement of function GOALSTADIUM.transfer is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
function totalFees() public view returns (uint256) {
        return _tFeeTotal;
    }
    function reflectionFromToken(uint256 tAmount, bool deductTransferFee) public view returns(uint256) {
        require(tAmount <= _tTotal, "Amount must be less than supply");
        if (!deductTransferFee) {
            (uint256 rAmount,,,,,) = _getValues(tAmount);
            return rAmount;
        } else {
            (,uint256 rTransferAmount,,,,) = _getValues(tAmount);
            return rTransferAmount;
        }
    }
```

Gas requirement of function GOALSTADIUM.allowance is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
function reflectionFromToken(uint256 tAmount, bool deductTransferFee) public view returns(uint256) {
        require(tAmount <= _tTotal, "Amount must be less than supply");
        if (!deductTransferFee) {
            (uint256 rAmount,,,,,) = _getValues(tAmount);
            return rAmount;
        } else {
            (,uint256 rTransferAmount,,,,) = _getValues(tAmount);
            return rTransferAmount;
        }
    }
    function tokenFromReflection(uint256 rAmount) public view returns(uint256) {
        require(rAmount <= _rTotal, "Amount must be less than total reflections");
        uint256 currentRate =  _getRate();
        return rAmount.div(currentRate);
    }
```

Gas requirement of function GOALSTADIUM.approve is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
function reflectionFromToken(uint256 tAmount, bool deductTransferFee) public view returns(uint256) {
        require(tAmount <= _tTotal, "Amount must be less than supply");
        if (!deductTransferFee) {
            (uint256 rAmount,,,,,) = _getValues(tAmount);
            return rAmount;
        } else {
            (,uint256 rTransferAmount,,,,) = _getValues(tAmount);
            return rTransferAmount;
        }
    }
```

Gas requirement of function GOALSTADIUM.transferFrom is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
function tokenFromReflection(uint256 rAmount) public view returns(uint256) {
    require(rAmount <= _rTotal, "Amount must be less than total reflections");
    uint256 currentRate =  _getRate();
    return rAmount.div(currentRate);
}
function _approve(address owner, address spender, uint256 amount) private {
    require(owner != address(0), "Approve from the zero address is not allowed");
    require(spender != address(0), "Approve to the zero address is not allowed");

    _allowances[owner][spender] = amount;
    emit Approval(owner, spender, amount);
}
```

Gas requirement of function GOALSTADIUM.increaseALlowance is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
function _approve(address owner, address spender, uint256 amount) private {
    require(owner != address(0), "Approve from the zero address is not allowed");
    require(spender != address(0), "Approve to the zero address is not allowed");

    _allowances[owner][spender] = amount;
    emit Approval(owner, spender, amount);
}
```

Gas requirement of function GOALSTADIUM.decreaseALlowance is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
function _approve(address owner, address spender, uint256 amount) private {
    require(owner != address(0), "Approve from the zero address is not allowed");
    require(spender != address(0), "Approve to the zero address is not allowed");

    _allowances[owner][spender] = amount;
    emit Approval(owner, spender, amount);
}
```

Gas requirement of function GOALSTADIUM.reflectionFromToken is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
function _transfer(
    address from,
    address to,
    uint256 amount
) private {
    require(from != address(0), "Transfer from the zero address is not allowed");
    require(to != address(0), "Transfer to the zero address is not allowed");
    require(amount > 0, "Transfer amount must be greater than zero");
    require(!isBlacklisted[from], "Sender address is blacklisted");
            require(!isBlacklisted[to], "Recipient address is blacklisted");
    require(Public_Trading_Enabled || _isExcludedFromFee[from] || _isExcludedF
```

Gas requirement of function GOALSTADIUM.tokenFromReflection is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
if (from != owner() && to != owner() && !_isExcludedFromFee[from] && !_isExcludedFromFee[to]) {

        if (from == uniswapV2Pair && to != address(uniswapV2Router)) {
            isTrade = true;
            projectFee = buy_ProjectFee;
            reflectionsFee = buy_ReflectionsFee;
        }
```

Gas requirement of function GOALSTADIUM.B1_check_sell_AllowedTime is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
// Trading, price impacts tiers and fees

   function C01_enable_Public_Trading() external onlyOwner {
      Public_Trading_Enabled = true;
   }
   function C02_disable_Public_Trading() external onlyOwner {
      Public_Trading_Enabled = false;
   }
```

Gas requirement of function GOALSTADIUM.C25_enable_receive_Reftections is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

```
   // Project fee further split to wallets
   function D1_set_FondoBNB_wallet(address account) external onlyOwner {
      FondoBNB_wallet = account;
   }
   function D2_set_ReservaTokens_wallet(address account) external onlyOwner {
      ReservaTokens_wallet = account;
   }
   function D3_set_BlockchainSupport_wallet(address account) external
onlyBlockchainDev {
      BlockchainSupport_wallet = account;
   }

   // Blockchain Support Team members

   function E1_add_BlockchainSupportDev(address account) external
onlyBlockchainDev {
      require(!BlockchainSupportDevs[account],"Blockchain Support Dev already
added");
      BlockchainSupportDevs[account] = true;
      emit Added_BlockchainSupportDev(account);
   }
   function E2_remove_BlockchainSupportDev(address account) external
onlyBlockchainDev {
      require(BlockchainSupportDevs[account],"Unable to remove. The account is
not in the BlockchainSupportDevs list");
      BlockchainSupportDevs[account] = false;
      emit Removed_BlockchainSupportDev(account);
   }
```

GOALSTADIUM.C26_exclude_fromReceiving_Reflections is infinite: If the gas requirement of a function is higher than the block gas limit it cannot be executed.

Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage).

// Blockchain Support Team members

```
  function E1_add_BlockchainSupportDev(address account) external onlyBlockchainDev {
      require(!BlockchainSupportDevs[account],"Blockchain Support Dev already added");
      BlockchainSupportDevs[account] = true;
      emit Added_BlockchainSupportDev(account);
  }
  function E2_remove_BlockchainSupportDev(address account) external onlyBlockchainDev {
      require(BlockchainSupportDevs[account],"Unable to remove. The account is not in the BlockchainSupportDevs list");
      BlockchainSupportDevs[account] = false;
      emit Removed_BlockchainSupportDev(account);
  }
```

Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas. The number of iterations in a loop can grow beyond the block gas limit which can cause the complete contract to be stalled at a certain point. Additionally, using unbounded loops incurs in a lot of avoidable gas costs.

Carefully test how many items at maximum you can pass to such functions to make it successful.

```
  function calculateReflectionsFee(uint256 _amount) private view returns (uint256) {
      return _amount.mul(reflectionsFee).div(100);
  }
  function calculateProjectFee(uint256 _amount) private view returns (uint256) {
      return _amount.mul(projectFee).div(100);
  }
```

Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas. The number of iterations in a loop can grow beyond the block gas limit which can cause the complete contract to be stalled at a certain point. Additionally, using unbounded loops incurs in a lot of avoidable gas costs.
Carefully test how many items at maximum you can pass to such functions to make it successful.

```
  function D2_set_ReservaTokens_wallet(address account) external onlyOwner {
      ReservaTokens_wallet = account;
  }
  function D3_set_BlockchainSupport_wallet(address account) external
onlyBlockchainDev {
      BlockchainSupport_wallet = account;
  }
```

ERC:

ERC20 contract's "decimals" function should have "uint8" as return type.

```
interface IUniswapV2Pair {
    event Approval(address indexed owner, address indexed spender, uint value);
    event Transfer(address indexed from, address indexed to, uint value);

    function name() external pure returns (string memory);
    function symbol() external pure returns (string memory);
    function decimals() external pure returns (uint8);
    function totalSupply() external view returns (uint);
    function balanceOf(address owner) external view returns (uint);
    function allowance(address owner, address spender) external view returns (uint);

    function approve(address spender, uint value) external returns (bool);
    function transfer(address to, uint value) external returns (bool);
    function transferFrom(address from, address to, uint value) external returns (bool);

    function DOMAIN_SEPARATOR() external view returns (bytes32);
    function PERMIT_TYPEHASH() external pure returns (bytes32);
    function nonces(address owner) external view returns (uint);
```

Miscellaneous - Constant/View/Pure functions:

IERC20.transfer(address,uint256): Potentially should be constant/view/pure but is not. Node: Modifiers are currently not considered by this static analysis.

interface IERC20 {

function totalSupply() external view returns (uint256);
function balanceOf(address account) external view returns (uint256);
function transfer(address recipient, uint256 amount) external returns (bool);
function allowance(address owner, address spender) external view returns (uint256);
function approve(address spender, uint256 amount) external returns (bool);
function transferFrom(address sender, address recipient, uint256 amount) external returns (bool);

event Transfer(address indexed from, address indexed to, uint256 value);
event Approval(address indexed owner, address indexed spender, uint256 value);
}

SafeMath.sub(uint256,uint256): Is constant but potentially should not be.

NOTE:Modifiers are currently not considered by this static analysis.

```
function sub(uint256 a, uint256 b) internal pure returns (uint256) {
    return sub(a, b, "SafeMath: subtraction overflow");
}
```

SafeMath.div(uint256,uint256): Is constant but potentially should not be.

NOTE:Modifiers are currently not considered by this static analysis.

```
function div(uint256 a, uint256 b) internal pure returns (uint256) {
    return div(a, b, "SafeMath: division by zero");
}
```

SafeMath.mod(uint256,uint256): Is constant but potentially should not be.

NOTE:Modifiers are currently not considered by this static analysis.

```
function mod(uint256 a, uint256 b) internal pure returns (uint256) {
    return mod(a, b, "SafeMath: modulo by zero");
}
```

Address.isContract(address): Is constant but potentially should not be.

NOTE:Modifiers are currently not considered by this static analysis.

```
library Address {

    function isContract(address account) internal view returns (bool) {
        // According to EIP-1052, 0x0 is the value returned for not-yet created accounts
        // and 0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470 is returned
        // for accounts without code, i.e. `keccak256('')`
        bytes32 codehash;
        bytes32 accountHash = 0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470;
        // solhint-disable-next-line no-inline-assembly
        assembly { codehash := extcodehash(account) }
        return (codehash != accountHash && codehash != 0x0);
    }
```

IUNiswapV2Factory.createPair(address,address): Potentially should be constant/view/pure but is not.

NOTE: Modifiers are currently not considered by this static analysis.

```
interface IUniswapV2Factory {
    event PairCreated(address indexed token0, address indexed token1, address pair, uint);

    function feeTo() external view returns (address);
    function feeToSetter() external view returns (address);

    function getPair(address tokenA, address tokenB) external view returns (address pair);
    function allPairs(uint) external view returns (address pair);
    function allPairsLength() external view returns (uint);
```

function createPair(address tokenA, address tokenB) external returns (address pair);

f**unction setFeeTo(address) external;**
function setFeeToSetter(address) external;
}

IUNiswapV2Pair.approve(address,uint256): Potentially should be constant/view/pure but is not.

NOTE: Modifiers are currently not considered by this static analysis.

interface IUniswapV2Pair {
event Approval(address indexed owner, address indexed spender, uint value);
event Transfer(address indexed from, address indexed to, uint value);

function name() external pure returns (string memory);
function symbol() external pure returns (string memory);
function decimals() external pure returns (uint8);
function totalSupply() external view returns (uint);
function balanceOf(address owner) external view returns (uint);
function allowance(address owner, address spender) external view returns (uint);

f**unction approve(address spender, uint value) external returns (bool);**
function transfer(address to, uint value) external returns (bool);
function transferFrom(address from, address to, uint value) external returns (bool);
function permit(address owner, address spender, uint value, uint deadline, uint8 v, bytes32 r, bytes32 s) external;

IUniswapV2Pair.mint(address): Potentially should be constant/view/pure but is not.

NOTE: Modifiers are currently not considered by this static analysis.

function mint(address to) external returns (uint liquidity);
function burn(address to) external returns (uint amount0, uint amount1);
function swap(uint amount0Out, uint amount1Out, address to, bytes calldata data) external;
function skim(address to) external;
function sync() external;
function initialize(address, address) external;

IUNiswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256): Potentially should be constant/view/pure but is not.

NOTE: Modifiers are currently not considered by this static analysis.

```
interface IUniswapV2Router01 {
    function factory() external pure returns (address);
    function WETH() external pure returns (address);
    function addLiquidity(
        address tokenA,
        address tokenB,
        uint amountADesired,
        uint amountBDesired,
        uint amountAMin,
        uint amountBMin,
        address to,
        uint deadline
    ) external returns (uint amountA, uint amountB, uint liquidity);
```

IUNiswapV2Router01.removeLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256): Potentially should be constant/view/pure but is not.

NOTE: Modifiers are currently not considered by this static analysis.

```
function removeLiquidity(
        address tokenA,
        address tokenB,
        uint liquidity,
        uint amountAMin,
        uint amountBMin,
        address to,
        uint deadline
    ) external returns (uint amountA, uint amountB);
```

THE SAME RULE APPLIES TO THE REST OF THE SIMILAR WARNINGS

Similar variable names:

GOALSTADIUM.(): Variables have very similar names "_rOwned" and "_tOwned".

Note: Modifiers are currently not considered by this static analysis.

```
 function name() public view returns (string memory) {
        return _name;
    }
    function symbol() public view returns (string memory) {
        return _symbol;
    }
    function decimals() public view returns (uint8) {
        return _decimals;
    }
    function totalSupply() public view override returns (uint256) {
        return _tTotal;
    }
    function balanceOf(address account) public view override returns (uint256) {
        if (_isExcludedRewards[account]) return _tOwned[account];
        return tokenFromReflection(_rOwned[account]);
    }
    function transfer(address recipient, uint256 amount) public override returns (bool)
{
        _transfer(_msgSender(), recipient, amount);
        return true;
    }
    function allowance(address owner, address spender) public view override returns
(uint256) {
        return _allowances[owner][spender];
```

THE SAME RULE APPLIES TO THE REST OF THE SIMILAR WARNINGS

No return:

IERC20.totalSupply(): Defines a return type but never explicitly returns a value.

Sin retorno:

interface IERC20 {

function totalSupply() external view returns (uint256);
function balanceOf(address account) external view returns (uint256);
function transfer(address recipient, uint256 amount) external returns (bool);
function allowance(address owner, address spender) external view returns (uint256);
function approve(address spender, uint256 amount) external returns (bool);
function transferFrom(address sender, address recipient, uint256 amount) external returns (bool);

event Transfer(address indexed from, address indexed to, uint256 value);
event Approval(address indexed owner, address indexed spender, uint256 value);
}

THE SAME RULE APPLIES TO THE REST OF THE SIMILAR WARNINGS

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

```
function add(uint256 a, uint256 b) internal pure returns (uint256) {
    uint256 c = a + b;
    require(c >= a, "SafeMath: addition overflow");

    return c;
}
```

THE SAME RULE APPLIES TO THE REST OF THE SIMILAR WARNINGS

Delete from dynamic array:

Using “delete” on an array leaves a grap. The lenght of the array remains the same. If you want to remove the empty position you need to shift items manually and update the “length” property.

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.

```
function mul(uint256 a, uint256 b) internal pure returns (uint256) {
    // Gas optimization: this is cheaper than requiring 'a' not being zero, but the
    // benefit is lost if 'b' is also tested.
    // See: https://github.com/OpenZeppelin/openzeppelin-contracts/pull/522
    if (a == 0) {
        return 0;
    }
    uint256 c = a * b;
    require(c / a == b, "SafeMath: multiplication overflow");
    return c;
}
```

Slither

A continuación, se adjunta parte del código del contrato inteligente y se describen los fallos destacables.

GOALSTADIUM.B4_set_AntiDump_SellWait_Duration(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#884-888) should emit an event for:
-antiDump_SellWait_Duration_Seconds = wait_seconds (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#887)
GOALSTADIUM.B5_set_MinTokens_ForProjectFundingSwap(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#889-892) should emit an event for:
- minTokensForProjectFundingSwap = minTokenAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#891)
GOALSTADIUM.C05_set_Sell_Price_Impact1(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#910-914) should emit an event for:
- price_impact1 = impact1 (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#913)
GOALSTADIUM.C06_set_Sell_Price_Impact2(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#915-921) should emit an event for:
- price_impact2 = impact2 (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#917)
GOALSTADIUM.C07_set_ProjectFundingFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#922-927) should emit an event for:
- projectFee = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#924)
GOALSTADIUM.C08_set_FondoBNB_Fee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#928-933) should emit an event for:
- FondoBNB_Fee = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#932)
GOALSTADIUM.C10_set_Buy_ProjectFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#945-947) should emit an event for:
- buy_ProjectFee = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#946)
GOALSTADIUM.C11_set_Buy_ReflectionsFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#948-950) should emit an event for:
- buy_ReflectionsFee = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#949)

GOALSTADIUM.C12_set_Default_ReflectionsFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#951-954) should emit an event for:
- reflectionsFee = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#953)
GOALSTADIUM.C13_set_Transfer_ProjectFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#955-958) should emit an event for:
- transfer_ProjectFee = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#957)
GOALSTADIUM.C14_set_Transfer_ReflectionsFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#959-962) should emit an event for:
- transfer_ReflectionsFee = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#961)
GOALSTADIUM.C15_set_sell_ProjectFee_A(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#963-966) should emit an event for:
- sell_ProjectFee_A = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#965)
GOALSTADIUM.C16_set_sell_ProjectFee_B(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#967-970) should emit an event for:
- sell_ProjectFee_B = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#969)
GOALSTADIUM.C17_set_sell_ProjectFee_C(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#971-976) should emit an event for:
- sell_ProjectFee_C = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#975)
GOALSTADIUM.C18_set_sell_ReflectionsFee_A(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#977-980) should emit an event for:
- sell_ReflectionsFee_A = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#979)
GOALSTADIUM.C19_set_sell_ReflectionsFee_B(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#981-984) should emit an event for:
- sell_ReflectionsFee_B = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#983)
GOALSTADIUM.C20_set_sell_ReflectionsFee_C(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#985-988) should emit an event for:
- sell_ReflectionsFee_C = fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#987)

GOALSTADIUM.D1_set_FondoBNB_wallet(address).account (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1035) lacks a zero-check on :
- FondoBNB_wallet = account (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1036)
GOALSTADIUM.D2_set_ReservaTokens_wallet(address).account (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1038) lacks a zero-check on :
- ReservaTokens_wallet = account (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1039)
GOALSTADIUM.D3_set_BlockchainSupport_wallet(address).account (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1041) lacks a zero-check on :
- BlockchainSupport_wallet = account (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1042)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation

Reentrancy in GOALSTADIUM._transfer(address,address,uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#569-661):
External calls:
*projectFundingSwap(contractTokenBalance) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#647)

*uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#692-698)

External calls sending eth:
*projectFundingSwap(contractTokenBalance) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#647)

*address(BlockchainSupport_wallet).transfer(blockchainSupportBNB) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#677)
*address(FondoBNB_wallet).transfer(fondoBNB) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#680)

State variables written after the call(s):
*_tokenTransfer(from,to,amount,takeAllFees) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*_tFeeTotal = _tFeeTotal.add(tFee) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#771)
*_tokenTransfer(from,to,amount,takeAllFees) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*previousProjectFee = projectFee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#832)

*_tokenTransfer(from,to,amount,takeAllFees) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*previousReflectionsFee = reflectionsFee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#831)
*_tokenTransfer(from,to,amount,takeAllFees) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*projectFee = previousProjectFee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#839)
*projectFee = 0 (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#835)
*_tokenTransfer(from,to,amount,takeAllFees) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*reflectionsFee = previousReflectionsFee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#838)
*reflectionsFee = 0 (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#834)
Reentrancy in GOALSTADIUM.constructor() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#478-503):

External calls:
*uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this),_uniswapV2Router.WETH()) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#485-486)

State variables written after the call(s):
*BlockchainSupportDevs[msg.sender] = true (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#499)
*BlockchainSupport_wallet = msg.sender (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#496)
*FondoBNB_wallet = msg.sender (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#495)
*ReservaTokens_wallet = msg.sender (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#497)
*_isExcludedFromFee[owner()] = true (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#492)
*_isExcludedFromFee[address(this)] = true (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#493)
*uniswapV2Router = _uniswapV2Router (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#489)

Reentrancy in GOALSTADIUM.transferFrom(address,address,uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#531-535):

External calls:
*_transfer(sender,recipient,amount) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#532)

*uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#692-698)

External calls sending eth:
*_transfer(sender,recipient,amount) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#532)
*address(BlockchainSupport_wallet).transfer(blockchainSupportBNB) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#677)
*address(FondoBNB_wallet).transfer(fondoBNB) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#680)
State variables written after the call(s):
*_approve(sender,_msgSender(),_allowances[sender][_msgSender()].sub(amount,Transfer amount exceeds allowance)) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#533)
*_allowances[owner][spender] = amount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#566)

Reentrancy in GOALSTADIUM._transfer(address,address,uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#569-661):

External calls:
*projectFundingSwap(contractTokenBalance) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#647)

*uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#692-698)

External calls sending eth:
*projectFundingSwap(contractTokenBalance) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#647)
*address(BlockchainSupport_wallet).transfer(blockchainSupportBNB) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#677)
*address(FondoBNB_wallet).transfer(fondoBNB) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#680)
Event emitted after the call(s):
*TokensSentToReservaWallet(ReservaTokens_wallet,rLiquidity) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#815)

*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*TokensSentToReservaWallet(ReservaTokens_wallet,tLiquidity)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#819)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*Transfer(sender,recipient,tTransferAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#739)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*Transfer(sender,recipient,tTransferAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#748)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*Transfer(sender,recipient,tTransferAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#757)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*Transfer(sender,recipient,tTransferAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#767)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)

Reentrancy in GOALSTADIUM.constructor()
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#478-503):

External calls:
*uniswapV2Pair=IUniswapV2Factory(_uniswapV2Router.factory()).createPair(
address(this),_uniswapV2Router.WETH())
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#485-486)

Event emitted after the call(s):
*Transfer(address(0),_msgSender(),_tTotal)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#502)

Reentrancy in GOALSTADIUM.projectFundingSwap(uint256)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#662-683):
External calls:
*swapTokensForBNB(tokensbeforeSwap)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#668)

*uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(t
okenAmount,0,path,address(this),block.timestamp)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#692-698)

External calls sending eth:
*address(BlockchainSupport_wallet).transfer(blockchainSupportBNB)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#677)
*address(FondoBNB_wallet).transfer(fondoBNB)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#680)

Event emitted after the call(s):
*ProjectFundingDone(tokensbeforeSwap,FondoBNB_wallet,fondoBNB,BlockchainSupport_wallet,blockchainSupportBNB)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#682)

Reentrancy in GOALSTADIUM.transferFrom(address,address,uint256)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#531-535):

External calls:
*_transfer(sender,recipient,amount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#532)
*uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#692-698)

External calls sending eth:
*_transfer(sender,recipient,amount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#532)
*address(BlockchainSupport_wallet).transfer(blockchainSupportBNB)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#677)
*address(FondoBNB_wallet).transfer(fondoBNB)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#680)
Event emitted after the call(s):
*Approval(owner,spender,amount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#567)
*_approve(sender,_msgSender(),_allowances[sender][_msgSender()].sub(amount,Transfer amount exceeds allowance))
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#533)

GOALSTADIUM._transfer(address,address,uint256)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#569-661) uses timestamp for comparisons

Dangerous comparisons:
*require(bool)(block.timestamp > sell_AllowedTime[from]) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#593)

Address.isContract(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#73-82) uses assembly
- INLINE ASM (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#80)
Address._functionCallWithValue(address,bytes,uint256,string) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#103-124) uses assembly
- INLINE ASM (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#116-119)

Address._functionCallWithValue(address,bytes,uint256,string) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#103-124) is never used and should be removed
Address.functionCall(address,bytes) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#90-92) is never used and should be removed
Address.functionCall(address,bytes,string) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#93-95) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#96-98) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#99-102) is never used and should be removed
Address.isContract(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#73-82) is never used and should be removed
Address.sendValue(address,uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#83-89) is never used and should be removed
Context._msgData() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#10-13) is never used and should be removed
GOALSTADIUM.addLiquidity(uint256,uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#700-712) is never used and should be removed
SafeMath.mod(uint256,uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#63-65) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#66-69) is never used and should be removed

GOALSTADIUM._tTotal (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#381) is set pre-construction with a non-constant function or state variable:
- 500000000 * 10 ** _decimals
GOALSTADIUM._rTotal (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#382) is set pre-construction with a non-constant function or state variable:
- (MAX - (MAX % _tTotal))
GOALSTADIUM.minTokensForProjectFundingSwap (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#451) is set pre-construction with a non-constant function or state variable:
- 50000 * 10 ** _decimals

Pragma version^0.8.8 (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6 solc-0.8.9 is not recommended for deployment

Low level call in Address.sendValue(address,uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#83-89):
- (success) = recipient.call{value: amount}() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#87)

Low level call in Address._functionCallWithValue(address,bytes,uint256,string) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#103-124):
- (success,returndata) = target.call{value: weiValue}(data) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#107)

Event OwnableOwnership_Transferred(address,address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#131) is not in CapWords
Function Ownable.Z_transfer_Ownership(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#146-155) is not in mixedCase
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#193) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#194) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#211) is not in mixedCase
Function IUniswapV2Router01.WETH() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#233) is not in mixedCase
Event GOALSTADIUMAdded_BlockchainSupportDev(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#464) is not in CapWords
Event GOALSTADIUMRemoved_BlockchainSupportDev(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#465) is not in CapWords
Parameter GOALSTADIUM.calculateReflectionsFee(uint256)._amount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#822) is not in mixedCase

Parameter GOALSTADIUM.calculateProjectFee(uint256)._amount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#825) is not in mixedCase
Function GOALSTADIUM.A1_Blacklist_BadActor(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#844-853) is not in mixedCase
Function GOALSTADIUM.A2_removeFromBlacklist(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#854-858) is not in mixedCase
Function GOALSTADIUM.A3_checkif_Blacklisted(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#859-863) is not in mixedCase
Function GOALSTADIUM.B1_check_sell_AllowedTime(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#867-875) is not in mixedCase
Function GOALSTADIUM.B2_enable_AntiDump_sellWait() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#876-879) is not in mixedCase
Function GOALSTADIUM.B3_disable_AntiDump_sellWait() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#880-883) is not in mixedCase
Function GOALSTADIUM.B4_set_AntiDump_SellWait_Duration(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#884-888) is not in mixedCase
Parameter GOALSTADIUM.B4_set_AntiDump_SellWait_Duration(uint256).wait_seconds (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#884) is not in mixedCase
Function GOALSTADIUM.B5_set_MinTokens_ForProjectFundingSwap(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#889-892) is not in mixedCase
Function GOALSTADIUM.C01_enable_Public_Trading() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#896-898) is not in mixedCase
Function GOALSTADIUM.C02_disable_Public_Trading() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#899-901) is not in mixedCase
Function GOALSTADIUM.C03_enable_All_Fees() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#902-905) is not in mixedCase
Function GOALSTADIUM.C04_disable_All_Fees() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#906-909) is not in mixedCase
Function GOALSTADIUM.C05_set_Sell_Price_Impact1(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#910-914) is not in mixedCase

Function GOALSTADIUM.C06_set_Sell_Price_Impact2(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#915-921) is not in mixedCase
Function GOALSTADIUM.C07_set_ProjectFundingFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#922-927) is not in mixedCase
Parameter GOALSTADIUM.C07_set_ProjectFundingFee(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#922) is not in mixedCase
Function GOALSTADIUM.C08_set_FondoBNB_Fee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#928-933) is not in mixedCase
Parameter GOALSTADIUM.C08_set_FondoBNB_Fee(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#928) is not in mixedCase
Function GOALSTADIUM.C10_set_Buy_ProjectFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#945-947) is not in mixedCase
Parameter GOALSTADIUM.C10_set_Buy_ProjectFee(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#945) is not in mixedCase
Function GOALSTADIUM.C11_set_Buy_ReflectionsFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#948-950) is not in mixedCase
Parameter GOALSTADIUM.C11_set_Buy_ReflectionsFee(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#948) is not in mixedCase
Function GOALSTADIUM.C12_set_Default_ReflectionsFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#951-954) is not in mixedCase
Parameter GOALSTADIUM.C12_set_Default_ReflectionsFee(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#951) is not in mixedCase
Function GOALSTADIUM.C13_set_Transfer_ProjectFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#955-958) is not in mixedCase
Parameter GOALSTADIUM.C13_set_Transfer_ProjectFee(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#955) is not in mixedCase
Function GOALSTADIUM.C14_set_Transfer_ReflectionsFee(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#959-962) is not in mixedCase
Parameter GOALSTADIUM.C14_set_Transfer_ReflectionsFee(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#959) is not in mixedCase
Function GOALSTADIUM.C15_set_sell_ProjectFee_A(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#963-966) is not in mixedCase
Parameter GOALSTADIUM.C15_set_sell_ProjectFee_A(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#963) is not in mixedCase
Function GOALSTADIUM.C16_set_sell_ProjectFee_B(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#967-970) is not in mixedCase

Parameter GOALSTADIUM.C16_set_sell_ProjectFee_B(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#967) is not in mixedCase
Function GOALSTADIUM.C17_set_sell_ProjectFee_C(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#971-976) is not in mixedCase
Parameter GOALSTADIUM.C17_set_sell_ProjectFee_C(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#971) is not in mixedCase
Function GOALSTADIUM.C18_set_sell_ReflectionsFee_A(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#977-980) is not in mixedCase
Parameter GOALSTADIUM.C18_set_sell_ReflectionsFee_A(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#977) is not in mixedCase
Function GOALSTADIUM.C19_set_sell_ReflectionsFee_B(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#981-984) is not in mixedCase
Parameter GOALSTADIUM.C19_set_sell_ReflectionsFee_B(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#981) is not in mixedCase
Function GOALSTADIUM.C20_set_sell_ReflectionsFee_C(uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#985-988) is not in mixedCase
Parameter GOALSTADIUM.C20_set_sell_ReflectionsFee_C(uint256).fee_percent (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#985) is not in mixedCase
Function GOALSTADIUM.C21_enable_mustPayFees(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#989-993) is not in mixedCase
Function GOALSTADIUM.C22_exclude_fromPayingFees(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#994-998) is not in mixedCase
Function GOALSTADIUM.C23_checkif_ExcludedFromPayingFees(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#999-1005) is not in mixedCase
Function GOALSTADIUM.C24_checkif_excluded_fromReceiving_Reflections(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1006-1010) is not in mixedCase
Function GOALSTADIUM.C25_enable_receive_Reflections(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1011-1022) is not in mixedCase
Function GOALSTADIUM.C26_exclude_fromReceiving_Reflections(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1023-1031) is not in mixedCase
Function GOALSTADIUM.D1_set_FondoBNB_wallet(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1035-1037) is not in mixedCase

Function GOALSTADIUM.D2_set_ReservaTokens_wallet(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1038-1040) is not in mixedCase
Function GOALSTADIUM.D3_set_BlockchainSupport_wallet(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1041-1043) is not in mixedCase
Function GOALSTADIUM.E1_add_BlockchainSupportDev(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1047-1051) is not in mixedCase
Function GOALSTADIUM.E2_remove_BlockchainSupportDev(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1052-1056) is not in mixedCase
Function GOALSTADIUM.E3_check_BlockchainSupportDev(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1057-1059) is not in mixedCase
Function GOALSTADIUM.F1_add_BridgeOrExchange(address,uint256,uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1063-1067) is not in mixedCase
Parameter GOALSTADIUM.F1_add_BridgeOrExchange(address,uint256,uint256).proj_fee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1063) is not in mixedCase
Parameter GOALSTADIUM.F1_add_BridgeOrExchange(address,uint256,uint256).reflections_fee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1063) is not in mixedCase
Function GOALSTADIUM.F2_remove_BridgeOrExchange(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1068-1072) is not in mixedCase
Function GOALSTADIUM.F3_check_BridgeOrExchange(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1073-1075) is not in mixedCase
Function GOALSTADIUM.F4_get_BridgeOrExchange_ProjectFee(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1076-1078) is not in mixedCase
Function GOALSTADIUM.F5_get_BridgeOrExchange_ReflectionsFee(address) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#1079-1081) is not in mixedCase
Variable GOALSTADIUM.FondoBNB_wallet (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#388) is not in mixedCase
Variable GOALSTADIUM.ReservaTokens_wallet (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#389) is not in mixedCase
Variable GOALSTADIUM.BlockchainSupport_wallet (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#391) is not in mixedCase
Variable GOALSTADIUM.price_impact1 (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#393) is not in mixedCase

Variable GOALSTADIUM.price_impact2 (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#394) is not in mixedCase
Variable GOALSTADIUM.FondoBNB_Fee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#406) is not in mixedCase
Variable GOALSTADIUM.BlockchainSupport_Fee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#407) is not in mixedCase
Variable GOALSTADIUM.transfer_ProjectFee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#414) is not in mixedCase
Variable GOALSTADIUM.transfer_ReflectionsFee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#415) is not in mixedCase
Variable GOALSTADIUM.buy_ProjectFee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#417) is not in mixedCase
Variable GOALSTADIUM.buy_ReflectionsFee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#418) is not in mixedCase
Variable GOALSTADIUM.sell_ProjectFee_A (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#420) is not in mixedCase
Variable GOALSTADIUM.sell_ProjectFee_B (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#421) is not in mixedCase
Variable GOALSTADIUM.sell_ProjectFee_C (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#422) is not in mixedCase
Variable GOALSTADIUM.sell_ReflectionsFee_A (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#424) is not in mixedCase
Variable GOALSTADIUM.sell_ReflectionsFee_B (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#425) is not in mixedCase
Variable GOALSTADIUM.sell_ReflectionsFee_C (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#426) is not in mixedCase
Variable GOALSTADIUM.BridgeOrExchange (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#429) is not in mixedCase
Variable GOALSTADIUM.BridgeOrExchange_ProjectFee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#430) is not in mixedCase
Variable GOALSTADIUM.BridgeOrExchange_ReflectionsFee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#431) is not in mixedCase
Variable GOALSTADIUM.BlockchainSupportDevs (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#436) is not in mixedCase
Variable GOALSTADIUM.sell_AllowedTime (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#438) is not in mixedCase
Variable GOALSTADIUM.antiDump_SellWait_Duration_Seconds (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#439) is not in mixedCase
Variable GOALSTADIUM.antiDump_SellWait_Enabled (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#440) is not in mixedCase
Variable GOALSTADIUM.AllFeesEnabled (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#445) is not in mixedCase
Variable GOALSTADIUM.ProjectFundingSwapMode (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#448) is not in mixedCase
Variable GOALSTADIUM.Public_Trading_Enabled (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#449) is not in mixedCase

Redundant expression "this (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#11)" inContext (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#5-14)

Redundant expression "restoreAllFees (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#656)" inGOALSTADIUM (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#366-1084)

Reentrancy in GOALSTADIUM._transfer(address,address,uint256) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#569-661):

External calls:
*projectFundingSwap(contractTokenBalance) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#647)
*address(BlockchainSupport_wallet).transfer(blockchainSupportBNB) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#677)
*address(FondoBNB_wallet).transfer(fondoBNB) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#680)
State variables written after the call(s):
*_tokenTransfer(from,to,amount,takeAllFees) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*_rOwned[address(this)] = _rOwned[address(this)].add(rLiquidity) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#810)
*_rOwned[sender] = _rOwned[sender].sub(rAmount) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#735)
*_rOwned[address(ReservaTokens_wallet)] = _rOwned[address(ReservaTokens_wallet)].add(rLiquidity) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#814)
*_rOwned[sender] = _rOwned[sender].sub(rAmount) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#743)
*_rOwned[sender] = _rOwned[sender].sub(rAmount) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#762)
*_rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#736)
*_rOwned[sender] = _rOwned[sender].sub(rAmount) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#753)
*_rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#754)
*_rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#745)
*_rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#764)
*_tokenTransfer(from,to,amount,takeAllFees) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*_rTotal = _rTotal.sub(rFee) (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#770)

*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*_tFeeTotal = _tFeeTotal.add(tFee)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#771)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*_tOwned[address(this)] = _tOwned[address(this)].add(tLiquidity)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#812)
*_tOwned[sender] = _tOwned[sender].sub(tAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#761)
*_tOwned[sender] = _tOwned[sender].sub(tAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#752)
*_tOwned[recipient] = _tOwned[recipient].add(tTransferAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#744)
*_tOwned[recipient] = _tOwned[recipient].add(tTransferAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#763)
*_tOwned[address(ReservaTokens_wallet)] =
_tOwned[address(ReservaTokens_wallet)].add(tLiquidity)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#818)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*previousProjectFee = projectFee
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#832)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*previousReflectionsFee = reflectionsFee
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#831)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*projectFee = previousProjectFee
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#839)
*projectFee = 0
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#835)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*reflectionsFee = previousReflectionsFee
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#838)
*reflectionsFee = 0
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#834)
*sell_AllowedTime[from] = block.timestamp +
antiDump_SellWait_Duration_Seconds
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#659)
Event emitted after the call(s):
*TokensSentToReservaWallet(ReservaTokens_wallet,rLiquidity)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#815)

*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*TokensSentToReservaWallet(ReservaTokens_wallet,tLiquidity)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#819)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*Transfer(sender,recipient,tTransferAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#739)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*Transfer(sender,recipient,tTransferAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#748)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*Transfer(sender,recipient,tTransferAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#757)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)
*Transfer(sender,recipient,tTransferAmount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#767)
*_tokenTransfer(from,to,amount,takeAllFees)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#655)

Reentrancy in GOALSTADIUM.projectFundingSwap(uint256)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#662-683):

External calls:
*address(BlockchainSupport_wallet).transfer(blockchainSupportBNB)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#677)
*address(FondoBNB_wallet).transfer(fondoBNB)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#680)

Event emitted after the call(s):
*ProjectFundingDone(tokensbeforeSwap,FondoBNB_wallet,fondoBNB,BlockchainSupport_wallet,blockchainSupportBNB)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#682)

Reentrancy in GOALSTADIUM.transferFrom(address,address,uint256)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#531-535):

External calls:
*_transfer(sender,recipient,amount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#532)
*address(BlockchainSupport_wallet).transfer(blockchainSupportBNB)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#677)

*address(FondoBNB_wallet).transfer(fondoBNB)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#680)

State variables written after the call(s):
*_approve(sender,_msgSender(),_allowances[sender][_msgSender()].sub(amount,Transfer amount exceeds allowance))
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#533)
*_allowances[owner][spender] = amount
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#566)

Event emitted after the call(s):
*Approval(owner,spender,amount)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#567)

*_approve(sender,_msgSender(),_allowances[sender][_msgSender()].sub(amount,Transfer amount exceeds allowance))
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#533)

Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#237) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#238)

Variable GOALSTADIUM.price_impact1
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#393) is too similar to GOALSTADIUM.price_impact2
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#394)

Variable GOALSTADIUM._transferBothExcluded(address,address,uint256).rTransferAmount
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760) is too similar to GOALSTADIUM._transferStandard(address,address,uint256).tTransferAmount
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734)

Variable GOALSTADIUM.reflectionFromToken(uint256,bool).rTransferAmount
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#553) is too similar to GOALSTADIUM._getValues(uint256).tTransferAmount
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#774)

Variable GOALSTADIUM._getValues(uint256).rTransferAmount
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#775) is too similar to GOALSTADIUM._transferBothExcluded(address,address,uint256).tTransferAmount
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760)

Variable GOALSTADIUM._getValues(uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#775) is too similar to GOALSTADIUM._transferToExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742)

Variable GOALSTADIUM._getValues(uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#775) is too similar to GOALSTADIUM._transferFromExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751)

Variable GOALSTADIUM._getValues(uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#775) is too similar to GOALSTADIUM._getValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#774)

Variable GOALSTADIUM._getValues(uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#775) is too similar to GOALSTADIUM._getTValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#781)

Variable GOALSTADIUM._transferBothExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760) is too similar to GOALSTADIUM._getTValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#781)

Variable GOALSTADIUM._transferStandard(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734) is too similar to GOALSTADIUM._getValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#774)

Variable GOALSTADIUM._transferBothExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760) is too similar to GOALSTADIUM._transferFromExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751)

Variable GOALSTADIUM._transferToExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742) is too similar to GOALSTADIUM._transferToExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742)

Variable GOALSTADIUM._transferFromExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751) is too similar to GOALSTADIUM._getValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#774)

Variable GOALSTADIUM._transferFromExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751) is too similar to GOALSTADIUM._transferFromExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751)

Variable GOALSTADIUM._getValues(uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#775) is too similar to GOALSTADIUM._transferStandard(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734)

Variable GOALSTADIUM._transferBothExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760) is too similar to GOALSTADIUM._getValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#774)

Variable GOALSTADIUM._transferToExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742) is too similar to GOALSTADIUM._getValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#774)

Variable GOALSTADIUM._transferStandard(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734) is too similar to GOALSTADIUM._transferFromExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751)

Variable GOALSTADIUM._transferBothExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760) is too similar to GOALSTADIUM._transferToExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742)

Variable GOALSTADIUM._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#788) is too similar to GOALSTADIUM._transferFromExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751)

Variable GOALSTADIUM._transferStandard(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734) is too similar to GOALSTADIUM._transferToExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742)

Variable GOALSTADIUM._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#788) is too similar to GOALSTADIUM._getValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#774)

Variable GOALSTADIUM._transferBothExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760) is too similar to GOALSTADIUM._transferBothExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760)

Variable GOALSTADIUM._transferToExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742) is too similar to GOALSTADIUM._transferFromExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751)

Variable GOALSTADIUM._transferStandard(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734) is too similar to GOALSTADIUM._transferStandard(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734)

Variable GOALSTADIUM.sell_ProjectFee_A (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#420) is too similar to GOALSTADIUM.sell_ProjectFee_B (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#421)

Variable GOALSTADIUM.sell_ProjectFee_A (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#420) is too similar to GOALSTADIUM.sell_ProjectFee_C (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#422)

Variable GOALSTADIUM.sell_ProjectFee_B (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#421) is too similar to GOALSTADIUM.sell_ProjectFee_C (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#422)

Variable GOALSTADIUM.sell_ReflectionsFee_A (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#424) is too similar to GOALSTADIUM.sell_ReflectionsFee_B (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#425)

Variable GOALSTADIUM.sell_ReflectionsFee_A (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#424) is too similar to GOALSTADIUM.sell_ReflectionsFee_C (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#426)

Variable GOALSTADIUM.sell_ReflectionsFee_B (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#425) is too similar to GOALSTADIUM.sell_ReflectionsFee_C (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#426)

Variable GOALSTADIUM._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#788) is too similar to GOALSTADIUM._getTValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#781)

Variable GOALSTADIUM._transferFromExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751) is too similar to GOALSTADIUM._transferBothExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760)

Variable GOALSTADIUM._transferFromExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751) is too similar to GOALSTADIUM._transferToExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742)

Variable GOALSTADIUM._transferStandard(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734) is too similar to GOALSTADIUM._getTValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#781)

Variable GOALSTADIUM.reflectionFromToken(uint256,bool).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#553) is too similar to GOALSTADIUM._transferStandard(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734)

Variable GOALSTADIUM._transferStandard(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734) is too similar to GOALSTADIUM._transferBothExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760)

Variable GOALSTADIUM._transferToExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742) is too similar to GOALSTADIUM._transferBothExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760)

Variable GOALSTADIUM.reflectionFromToken(uint256,bool).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#553) is too similar to GOALSTADIUM._transferToExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742)

Variable GOALSTADIUM._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#788) is too similar to GOALSTADIUM._transferBothExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760)

Variable GOALSTADIUM._transferFromExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751) is too similar to GOALSTADIUM._transferStandard(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734)

Variable GOALSTADIUM._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#788) is too similar to GOALSTADIUM._transferToExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742)

Variable GOALSTADIUM.reflectionFromToken(uint256,bool).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#553) is too similar to GOALSTADIUM._transferFromExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751)

Variable GOALSTADIUM.reflectionFromToken(uint256,bool).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#553) is too similar to GOALSTADIUM._transferBothExcluded(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#760)

Variable GOALSTADIUM._transferToExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742) is too similar to GOALSTADIUM._getTValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#781)

Variable GOALSTADIUM.reflectionFromToken(uint256,bool).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#553) is too similar to GOALSTADIUM._getTValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#781)

Variable GOALSTADIUM._transferToExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#742) is too similar to GOALSTADIUM._transferStandard(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734)

Variable GOALSTADIUM._transferFromExcluded(address,address,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#751) is too similar to GOALSTADIUM._getTValues(uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#781)

Variable GOALSTADIUM._getRValues(uint256,uint256,uint256,uint256).rTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#788) is too similar to GOALSTADIUM._transferStandard(address,address,uint256).tTransferAmount (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#734)

GOALSTADIUM.slitherConstructorVariables() (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#366-1084) uses literals with too many digits:
- _tTotal = 500000000 * 10 ** _decimals (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#381)

GOALSTADIUM.BlockchainSupport_Fee (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#407) should be constant
GOALSTADIUM._decimals (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#378) should be constant
GOALSTADIUM._name (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#385) should be constant
GOALSTADIUM._symbol (Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#386) should be constant

Z_transfer_Ownership(address) should be declared external:
	*Ownable.Z_transfer_Ownership(address)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#146-155)
name() should be declared external:
	*GOALSTADIUM.name()
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#504-506)
symbol() should be declared external:
	*GOALSTADIUM.symbol()
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#507-509)
decimals() should be declared external:
	*GOALSTADIUM.decimals()
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#510-512)
totalSupply() should be declared external:
	*GOALSTADIUM.totalSupply()
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#513-515)
transfer(address,uint256) should be declared external:
	*GOALSTADIUM.transfer(address,uint256)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#520-523)
allowance(address,address) should be declared external:
	*GOALSTADIUM.allowance(address,address)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#524-526)
approve(address,uint256) should be declared external:
	*GOALSTADIUM.approve(address,uint256)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#527-530)
transferFrom(address,address,uint256) should be declared external:
	*GOALSTADIUM.transferFrom(address,address,uint256)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#531-535)
increaseAllowance(address,uint256) should be declared external:
	*GOALSTADIUM.increaseAllowance(address,uint256)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#536-539)
decreaseAllowance(address,uint256) should be declared external:
	*GOALSTADIUM.decreaseAllowance(address,uint256)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#540-543)
totalFees() should be declared external:
	*GOALSTADIUM.totalFees()
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#544-546)
reflectionFromToken(uint256,bool) should be declared external:
	*GOALSTADIUM.reflectionFromToken(uint256,bool)
(Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol#547-556)

Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol analyzed (10 contracts with 75 detectors), 228 result(s) found

Myth

Mediante esta herramienta se ha ejecutado un comando que analiza vulnerabilidades en el código del contrato inteligente. Los resultados arrojan que no se han encontrado fallas en el código.

 # analyze Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol
The analysis was completed successfully. No issues were detected.

Por otro lado, con otro comando se ha analizado el estado de seguridad de las funciones del contrato inteligente y los resultados muestran que las funciones se consideran seguras.

#safe-functions Goal_Stadium_Contrato_de_HyperchainX_15Dic2021.sol

Contract GOALSTADIUM:

86 functions are deemed safe in this contract: projectFee(), C05_set_Sell_Price_Impact1(uint256), sell_ProjectFee_B(), FondoBNB_wallet(), E2_remove_BlockchainSupportDev(address), C14_set_Transfer_ReflectionsFee(uint256), reflectionsFee(), B5_set_MinTokens_ForProjectFundingSwap(uint256), E1_add_BlockchainSupportDev(address), ReservaTokens_wallet(), E3_check_BlockchainSupportDev(address), transfer(address,uint256), B2_enable_AntiDump_sellWait(), C10_set_Buy_ProjectFee(uint256), C13_set_Transfer_ProjectFee(uint256), C03_enable_All_Fees(), C07_set_ProjectFundingFee(uint256), totalFees(), F4_get_BridgeOrExchange_ProjectFee(address), totalSupply(), C24_checkif_excluded_fromReceiving_Reflections(address), BlockchainSupport_Fee(), sell_ReflectionsFee_C(), minTokensForProjectFundingSwap(), BlockchainSupport_wallet(), C17_set_sell_ProjectFee_C(uint256), allowance(address,address), transferFrom(address,address,uint256), C22_exclude_fromPayingFees(address), reflectionFromToken(uint256,bool), sell_ProjectFee_C(), A2_removeFromBlacklist(address), C23_checkif_ExcludedFromPayingFees(address), F2_remove_BridgeOrExchange(address), buy_ProjectFee(), F5_get_BridgeOrExchange_ReflectionsFee(address), F3_check_BridgeOrExchange(address), C20_set_sell_ReflectionsFee_C(uint256), D3_set_BlockchainSupport_wallet(address), uniswapV2Router(), transfer_ReflectionsFee(), C11_set_Buy_ReflectionsFee(uint256), D2_set_ReservaTokens_wallet(address), decimals(), A3_checkif_Blacklisted(address), C02_disable_Public_Trading(), uniswapV2Pair(), approve(address,uint256), C25_enable_receive_Reflections(address), AllFeesEnabled(), sell_ReflectionsFee_A(), Public_Trading_Enabled(),

price_impact1(), antiDump_SellWait_Enabled(), sell_ProjectFee_A(), A1_Blacklist_BadActor(address), C19_set_sell_ReflectionsFee_B(uint256), C26_exclude_fromReceiving_Reflections(address), transfer_ProjectFee(), sell_ReflectionsFee_B(), F1_add_BridgeOrExchange(address,uint256,uint256), balanceOf(address), buy_ReflectionsFee(), C06_set_Sell_Price_Impact2(uint256), decreaseAllowance(address,uint256), increaseAllowance(address,uint256), C16_set_sell_ProjectFee_B(uint256), tokenFromReflection(uint256), C15_set_sell_ProjectFee_A(uint256), C21_enable_mustPayFees(address), name(), Z_transfer_Ownership(address), C08_set_FondoBNB_Fee(uint256), antiDump_SellWait_Duration_Seconds(), C01_enable_Public_Trading(), C18_set_sell_ReflectionsFee_A(uint256), C04_disable_All_Fees(), D1_set_FondoBNB_wallet(address), B4_set_AntiDump_SellWait_Duration(uint256), FondoBNB_Fee(), C12_set_Default_ReflectionsFee(uint256), B1_check_sell_AllowedTime(address), symbol(), owner(), B3_disable_AntiDump_sellWait(), price_impact2()

Contract Ownable:

2 functions are deemed safe in this contract: Z_transfer_Ownership(address), owner()

5. Resultados

Por un lado, el contrato inteligente tiene un archivo de 1084 líneas de código. Todos los comentarios de función y variable de estado siguen el formato de descripción estándar para escribir lo que puede ayudarnos a comprender rápidamente cómo funciona el programa.

Se ha realizado un correcto uso de la librería ERC20 y esto hace que el código generado sea pequeño, conciso y sencillo de seguir.

En cuanto a la calidad del código no se ha encontrado ninguna mejora a realizar para el objetivo del contrato inteligente. Sólo se han informado de posibles mejoras en el código que no tienen ningún impacto en la usabilidad del contrato.

Por tanto, no se han encontrado vulnerabilidades de ningún tipo de gravedad y las recomendaciones de reparación deben ser examinadas por los desarrolladores y el éxito de la misma es un proceso continuo antes de hacerse público.

6. Descargo de responsabilidad

La auditoría realizada garantiza que no se han encontrado vulnerabilidades conocidas en la totalidad del código, pero no exime de que posteriormente puedan aparecer algunas de estas. Por ello, desde Ciberseguridad e Inteligencia Artificial se recomienda hacer un seguimiento continuo del proyecto desarrollado mediante auditorías de token. A lo largo de estas auditorías se puede analizar y evaluar el estado de este código pudiendo realizar comparaciones con las auditorías anteriores.

El seguimiento continuo es imprescindible para asegurar que no se produzcan posibles fugas de información o activos tanto de la empresa como de los usuarios, evitando así fallos de seguridad que afecten al software.

El presente documento se basa en proveer seguridad en el código asumiendo que la empresa desarrolladora ha tenido en cuenta la normativa vigente. Es decir, el objetivo es más bien realizar un análisis exhaustivo sobre el código para intentar encontrar vulnerabilidades o minimizar el riesgo de fallos de seguridad en el proyecto. Sin embargo, no es un documento legalmente vinculante de la seguridad del código, la aplicabilidad del modelo comercial, el sistema regulatorio del modelo comercial o cualquier otra declaración de un estado libre de errores.