BlockSAFU

ADVANCE MANUAL
SMART CONTRACT AUDIT

Project: Tripin

Website: https://tripins.io/

BlockSAFU Score:

82

Contract Address:

0xe27B49606c61C6eD7Fc7d90f41b9FeBe9868d84e

Disclamer: BlockSAFU is not responsible for any financial losses.
Nothing in this contract audit is financial advice, please do your own reasearch.

DISCLAMER

BlockSAFU has completed this report to provide a summary of the Smart Contract functions, and any security, dependency, or cybersecurity vulnerabilities. This is often a constrained report on our discoveries based on our investigation and understanding of the current programming versions as of this report's date. To understand the full scope of our analysis, it is vital for you to at the date of this report. To understand the full scope of our analysis, you need to review the complete report. Although we have done our best in conducting our investigation and creating this report, it is vital to note that you should not depend on this report and cannot make any claim against BlockSAFU or its Subsidiaries and Team members on the premise of what has or has not been included in the report. Please remember to conduct your independent examinations before making any investment choices. We do not provide investment advice or in any way claim to determine if the project will be successful or not.

By perusing this report or any portion of it, you concur to the terms of this disclaimer. In the unlikely situation where you do not concur to the terms, you should immediately terminate reading this report, and erase and discard any duplicates of this report downloaded and/or printed by you. This report is given for data purposes as it were and on a non-reliance premise and does not constitute speculation counsel. No one should have any right to depend on the report or its substance, and BlockSAFU and its members (including holding companies, shareholders, backups, representatives, chiefs, officers, and other agents) BlockSAFU and its subsidiaries owe no obligation of care towards you or any other person, nor does BlockSAFU make any guarantee or representation to any individual on the precision or completeness of the report.

ABOUT THE AUDITOR:

BlockSAFU (BSAFU) is an Anti-Scam Token Utility that reviews Smart Contracts and Token information to Identify Rug Pull and Honey Pot scamming activity. BlockSAFUs Development Team consists of several Smart Contract creators, Auditors Developers, and Blockchain experts. BlockSAFU provides solutions, prevents, and hunts down scammers. BSAFU is a utility token with features Audit, KYC, Token Generators, and Bounty Scammers. It will enrich the crypto ecosystem.

OVERVIEW

BlockSAFU was commissioned by Tripin to complete a Smart Contract audit. The objective of the Audit is to achieve the following:

- Review the Project and experience and Development team
- Ensure that the Smart Contract functions are necessary and operate as intended.
- Identify any vulnerabilities in the Smart Contract code.

DISCLAIMER: This Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or provide financial advice in any way, all investments are made at your own risk. (https://blocksafu.com/)

SMART CONTRACT REVIEW

Token Name	**Tripin**
Token Symbol	**TRIP**
Token Decimal	9
Total Supply	1,000,000,000,000,000 **TRIP**
Contract Address	0xe27B49606c61C6eD7Fc7d90f41b9FeBe9868d84e
Deployer Address	0x2A688caA962181C4db4B0c503aB43313ABaa95CC
Owner Address	0x2a688caa962181c4db4b0c503ab43313abaa95cc
Tax Fees Buy	3%
Tax Fees Sell	3%
Gas Used for Buy	*will be updated after the DEX listing*
Gas Used for Sell	*will be updated after the DEX listing*
Contract Created	Aug-27-2022 08:36:35 PM +UTC
Initial Liquidity	*will be updated after the DEX listing*
Liquidity Status	Locked
Unlocked Date	*will be updated after the DEX listing*
Verified CA	Yes
Compiler	v0.8.4+commit.c7e474f2
Optimization	Yes with 200 runs
Sol License	MIT License
Top 5 Holders	*will be updated after the DEX listing*
Other	default evmVersion

TAX

BUY	3%	**SELL**	3%
charity Fee	0%	charity Fee	0%
liquidity Fee	2%	liquidity Fee	2%
tax Fee	1%	tax Fee	1%

OVERVIEW

Mint Function

- No mint functions.

Fees

- Buy 3% (owner can’t set fees over 25%).
- Sell 3% (owner can’t set fees over 25%).

Tx Amount

- Owner cannot set max tx amount.

Transfer Pausable

- Owner cannot pause.

Blacklist

- Owner cannot blacklist.

Ownership

- Owner cannot take back ownership.

Proxy

- This contract has no proxy.

Anti Whale

- Owner cannot limit the number of wallet holdings.

Trading Cooldown

- Owner cannot set the selling time interval.

Token Metrics

Rank	Address	Quantity	Percentage	Analytics
1	Pinksale: PinkLock V2	500,000,000,000,000	50.0000%	
2	0x2a688caa962181c4db4b0c503ab43313abaa95cc	500,000,000,000,000	50.0000%	

[Download CSV Export]

Team Review

The Tripin team has a nice website, their website is professionally built and the Smart contract is well developed, their social media is growing with over 2 people in their telegram group (count in audit date).

Official Website And Social Media

Website: https://tripins.io/

Telegram Group: https://t.me/tripin_en

Twitter: https://twitter.com/tripintoken

MANUAL CODE REVIEW

Minor-risk

1 minor-risk code issue found

Could be fixed, and will not bring problems.

1. The return value of an external transfer/transferFrom return value is checked. Recommendation: use SafeERC20, or ensure that the transfer/transferFrom return value is checked

```
function transferFrom(
      address sender,
      address recipient,
      uint256 amount
   ) external returns (bool);
```

Medium-risk

0 medium-risk code issues found

Should be fixed, could bring problems.

High-Risk

0 high-risk code issues found

Must be fixed, and will bring problem.

Critical-Risk

0 critical-risk code issues found

Must be fixed, and will bring problem.

EXTRA NOTES SMART CONTRACT

1. IERC20

```
interface IERC20 {
    /**
     * @dev Returns the number of tokens in existence.
     */
    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);

    /**
     * @dev Emitted when `value` tokens are moved from one account (`from`) to
     * another (`to`).
     *
     * Note that `value` may be zero.
     */
    event Transfer(address indexed from, address indexed to, uint256 value);
…
}
```

IERC20 Normal Base Template

2. SafeMath Contract

```
library SafeMath {
...
    function add(uint256 a, uint256 b) internal pure returns
(uint256) {
        uint256 c = a + b;
        require(c >= a, "SafeMath: addition overflow");
        return c;
    }
...
    function sub(uint256 a, uint256 b, string memory errorMessage)
internal pure returns (uint256) {
        require(b <= a, errorMessage);
        uint256 c = a - b;

        return c;
    }
    /**
     * @dev Returns the multiplication of two unsigned integers,
reverting on
     * overflow.
     *
     * Counterpart to Solidity's `*` operator.
     *
     * Requirements:
     *
     * - Multiplication cannot overflow.
     */
  ...
    function mod(
        uint256 a,
        uint256 b,
        string memory errorMessage
    ) internal pure returns (uint256) {
        unchecked {
            require(b > 0, errorMessage);
            return a % b;
        }
    }
}
```

Standard Safemath contract

3. Tripin Contract

```
contract AntiBotLiquidityGeneratorToken is IERC20, Ownable,
BaseToken {
    using SafeMath for uint256;
    using Address for address;

    uint256 public constant VERSION = 1;

    mapping(address => uint256) private _rOwned;
    mapping(address => uint256) private _tOwned;
    mapping(address => mapping(address => uint256)) private
_allowances;

    mapping(address => bool) private _isExcludedFromFee;
    mapping(address => bool) private _isExcluded;
    address[] private _excluded;

    uint256 private constant MAX = ~uint256(0);
    uint256 private _tTotal;
    uint256 private _rTotal;
    uint256 private _tFeeTotal;

    string private _name;
    string private _symbol;
    uint8 private _decimals;

    uint256 public _taxFee;
    uint256 private _previousTaxFee = _taxFee;

    uint256 public _liquidityFee;
    uint256 private _previousLiquidityFee = _liquidityFee;

    uint256 public _charityFee;
    uint256 private _previousCharityFee = _charityFee;

    IUniswapV2Router02 public uniswapV2Router;
    address public uniswapV2Pair;
    address public _charityAddress;

    bool inSwapAndLiquify;
    bool public swapAndLiquifyEnabled;
```

```
    uint256 private numTokensSellToAddToLiquidity;

    IPinkAntiBot public pinkAntiBot;
    bool public enableAntiBot;

    event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);
    event SwapAndLiquifyEnabledUpdated(bool enabled);
    event SwapAndLiquify(
        uint256 tokensSwapped,
        uint256 ethReceived,
        uint256 tokensIntoLiqudity
    );

    modifier lockTheSwap() {
        inSwapAndLiquify = true;
        _;
        inSwapAndLiquify = false;
    }

    constructor(
        string memory name_,
        string memory symbol_,
        uint256 totalSupply_,
        address router_,
        address charityAddress_,
        uint16 taxFeeBps_,
        uint16 liquidityFeeBps_,
        uint16 charityFeeBps_,
        address pinkAntiBot_,
        address serviceFeeReceiver_,
        uint256 serviceFee_
    ) payable {
        require(taxFeeBps_ >= 0, "Invalid tax fee");
        require(liquidityFeeBps_ >= 0, "Invalid liquidity fee");
        require(charityFeeBps_ >= 0, "Invalid charity fee");
        if (charityAddress_ == address(0)) {
            require(
                charityFeeBps_ == 0,
                "Cant set both charity address to address 0 and
charity percent more than 0"
            );
        }
```

```
        require(
            taxFeeBps_ + liquidityFeeBps_ + charityFeeBps_ <=
10**4 / 4,
            "Total fee is over 25%"
        );

        pinkAntiBot = IPinkAntiBot(pinkAntiBot_);
        pinkAntiBot.setTokenOwner(owner());
        enableAntiBot = true;

        _name = name_;
        _symbol = symbol_;
        _decimals = 9;

        _tTotal = totalSupply_;
        _rTotal = (MAX - (MAX % _tTotal));

        _taxFee = taxFeeBps_;
        _previousTaxFee = _taxFee;

        _liquidityFee = liquidityFeeBps_;
        _previousLiquidityFee = _liquidityFee;

        _charityAddress = charityAddress_;
        _charityFee = charityFeeBps_;
        _previousCharityFee = _charityFee;

        numTokensSellToAddToLiquidity =
totalSupply_.mul(5).div(10**4); // 0.05%

        swapAndLiquifyEnabled = true;

        _rOwned[owner()] = _rTotal;

        IUniswapV2Router02 _uniswapV2Router =
IUniswapV2Router02(router_);
        // Create a uniswap pair for this new token
        uniswapV2Pair =
IUniswapV2Factory(_uniswapV2Router.factory())
            .createPair(address(this), _uniswapV2Router.WETH());

        // set the rest of the contract variables
```

```
        uniswapV2Router = _uniswapV2Router;

        // exclude owner and this contract from fee
        _isExcludedFromFee[owner()] = true;
        _isExcludedFromFee[address(this)] = true;

        emit Transfer(address(0), owner(), _tTotal);

        emit TokenCreated(
            owner(),
            address(this),
            TokenType.antiBotLiquidityGenerator,
            VERSION
        );

        payable(serviceFeeReceiver_).transfer(serviceFee_);
    }

    function setEnableAntiBot(bool _enable) external onlyOwner {
        enableAntiBot = _enable;
    }

    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 (_isExcluded[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;
    }

    function transferFrom(
        address sender,
        address recipient,
        uint256 amount
    ) public override returns (bool) {
        _transfer(sender, recipient, amount);
        _approve(
            sender,
            _msgSender(),
            _allowances[sender][_msgSender()].sub(
                amount,
                "ERC20: transfer amount exceeds allowance"
```

```
            )
        );
        return true;
    }

    function increaseAllowance(address spender, uint256
addedValue)
        public
        virtual
        returns (bool)
    {
        _approve(
            _msgSender(),
            spender,
            _allowances[_msgSender()][spender].add(addedValue)
        );
        return true;
    }

    function decreaseAllowance(address spender, uint256
subtractedValue)
        public
        virtual
        returns (bool)
    {
        _approve(
            _msgSender(),
            spender,
            _allowances[_msgSender()][spender].sub(
                subtractedValue,
                "ERC20: decreased allowance below zero"
            )
        );
        return true;
    }

    function isExcludedFromReward(address account) public view
returns (bool) {
        return _isExcluded[account];
    }

    function totalFees() public view returns (uint256) {
```

```
        return _tFeeTotal;
    }

    function deliver(uint256 tAmount) public {
        address sender = _msgSender();
        require(
            !_isExcluded[sender],
            "Excluded addresses cannot call this function"
        );
        (uint256 rAmount, , , , , , ) = _getValues(tAmount);
        _rOwned[sender] = _rOwned[sender].sub(rAmount);
        _rTotal = _rTotal.sub(rAmount);
        _tFeeTotal = _tFeeTotal.add(tAmount);
    }

    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);
    }

    function excludeFromReward(address account) public onlyOwner {
        // require(account !=
0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D, 'We can not exclude
Uniswap router.');
        require(!_isExcluded[account], "Account is already
excluded");
        if (_rOwned[account] > 0) {
            _tOwned[account] =
tokenFromReflection(_rOwned[account]);
        }
        _isExcluded[account] = true;
        _excluded.push(account);
    }

    function includeInReward(address account) external onlyOwner {
        require(_isExcluded[account], "Account is already
excluded");
        for (uint256 i = 0; i < _excluded.length; i++) {
            if (_excluded[i] == account) {
                _excluded[i] = _excluded[_excluded.length - 1];
                _tOwned[account] = 0;
                _isExcluded[account] = false;
                _excluded.pop();
                break;
            }
        }
    }

    function _transferBothExcluded(
        address sender,
        address recipient,
        uint256 tAmount
    ) private {
        (
            uint256 rAmount,
            uint256 rTransferAmount,
            uint256 rFee,
            uint256 tTransferAmount,
```

```
            uint256 tFee,
            uint256 tLiquidity,
            uint256 tCharity
        ) = _getValues(tAmount);
        _tOwned[sender] = _tOwned[sender].sub(tAmount);
        _rOwned[sender] = _rOwned[sender].sub(rAmount);
        _tOwned[recipient] =
_tOwned[recipient].add(tTransferAmount);
        _rOwned[recipient] =
_rOwned[recipient].add(rTransferAmount);
        _takeLiquidity(tLiquidity);
        _takeCharityFee(tCharity);
        _reflectFee(rFee, tFee);
        emit Transfer(sender, recipient, tTransferAmount);
    }

    function excludeFromFee(address account) public onlyOwner {
        _isExcludedFromFee[account] = true;
    }

    function includeInFee(address account) public onlyOwner {
        _isExcludedFromFee[account] = false;
    }

    function setTaxFeePercent(uint256 taxFeeBps) external
onlyOwner {
        _taxFee = taxFeeBps;
        require(
            _taxFee + _liquidityFee + _charityFee <= 10**4 / 4,
            "Total fee is over 25%"
        );
    }

    function setLiquidityFeePercent(uint256 liquidityFeeBps)
        external
        onlyOwner
    {
        _liquidityFee = liquidityFeeBps;
        require(
            _taxFee + _liquidityFee + _charityFee <= 10**4 / 4,
            "Total fee is over 25%"
        );
```

```
    }

    function setSwapAndLiquifyEnabled(bool _enabled) public
onlyOwner {
        swapAndLiquifyEnabled = _enabled;
        emit SwapAndLiquifyEnabledUpdated(_enabled);
    }

    //to recieve ETH from uniswapV2Router when swaping
    receive() external payable {}

    function _reflectFee(uint256 rFee, uint256 tFee) private {
        _rTotal = _rTotal.sub(rFee);
        _tFeeTotal = _tFeeTotal.add(tFee);
    }

    function _getValues(uint256 tAmount)
        private
        view
        returns (
            uint256,
            uint256,
            uint256,
            uint256,
            uint256,
            uint256,
            uint256
        )
    {
        (
            uint256 tTransferAmount,
            uint256 tFee,
            uint256 tLiquidity,
            uint256 tCharity
        ) = _getTValues(tAmount);
        (uint256 rAmount, uint256 rTransferAmount, uint256 rFee) =
_getRValues(
            tAmount,
            tFee,
            tLiquidity,
            tCharity,
            _getRate()
```

```
        );
        return (
            rAmount,
            rTransferAmount,
            rFee,
            tTransferAmount,
            tFee,
            tLiquidity,
            tCharity
        );
    }

    function _getTValues(uint256 tAmount)
        private
        view
        returns (
            uint256,
            uint256,
            uint256,
            uint256
        )
    {
        uint256 tFee = calculateTaxFee(tAmount);
        uint256 tLiquidity = calculateLiquidityFee(tAmount);
        uint256 tCharityFee = calculateCharityFee(tAmount);
        uint256 tTransferAmount =
tAmount.sub(tFee).sub(tLiquidity).sub(
            tCharityFee
        );
        return (tTransferAmount, tFee, tLiquidity, tCharityFee);
    }

    function _getRValues(
        uint256 tAmount,
        uint256 tFee,
        uint256 tLiquidity,
        uint256 tCharity,
        uint256 currentRate
    )
        private
        pure
        returns (
```

```
            uint256,
            uint256,
            uint256
        )
    {
        uint256 rAmount = tAmount.mul(currentRate);
        uint256 rFee = tFee.mul(currentRate);
        uint256 rLiquidity = tLiquidity.mul(currentRate);
        uint256 rCharity = tCharity.mul(currentRate);
        uint256 rTransferAmount =
rAmount.sub(rFee).sub(rLiquidity).sub(
            rCharity
        );
        return (rAmount, rTransferAmount, rFee);
    }

    function _getRate() private view returns (uint256) {
        (uint256 rSupply, uint256 tSupply) = _getCurrentSupply();
        return rSupply.div(tSupply);
    }

    function _getCurrentSupply() private view returns (uint256,
uint256) {
        uint256 rSupply = _rTotal;
        uint256 tSupply = _tTotal;
        for (uint256 i = 0; i < _excluded.length; i++) {
            if (
                _rOwned[_excluded[i]] > rSupply ||
                _tOwned[_excluded[i]] > tSupply
            ) return (_rTotal, _tTotal);
            rSupply = rSupply.sub(_rOwned[_excluded[i]]);
            tSupply = tSupply.sub(_tOwned[_excluded[i]]);
        }
        if (rSupply < _rTotal.div(_tTotal)) return (_rTotal,
_tTotal);
        return (rSupply, tSupply);
    }

    function _takeLiquidity(uint256 tLiquidity) private {
        uint256 currentRate = _getRate();
        uint256 rLiquidity = tLiquidity.mul(currentRate);
        _rOwned[address(this)] =
```

```
_rOwned[address(this)].add(rLiquidity);
        if (_isExcluded[address(this)])
            _tOwned[address(this)] =
_tOwned[address(this)].add(tLiquidity);
    }

    function _takeCharityFee(uint256 tCharity) private {
        if (tCharity > 0) {
            uint256 currentRate = _getRate();
            uint256 rCharity = tCharity.mul(currentRate);
            _rOwned[_charityAddress] =
_rOwned[_charityAddress].add(rCharity);
            if (_isExcluded[_charityAddress])
                _tOwned[_charityAddress] =
_tOwned[_charityAddress].add(
                    tCharity
                );
            emit Transfer(_msgSender(), _charityAddress,
tCharity);
        }
    }

    function calculateTaxFee(uint256 _amount) private view returns
(uint256) {
        return _amount.mul(_taxFee).div(10**4);
    }

    function calculateLiquidityFee(uint256 _amount)
        private
        view
        returns (uint256)
    {
        return _amount.mul(_liquidityFee).div(10**4);
    }

    function calculateCharityFee(uint256 _amount)
        private
        view
        returns (uint256)
    {
        if (_charityAddress == address(0)) return 0;
        return _amount.mul(_charityFee).div(10**4);
```

```
    }

    function removeAllFee() private {
        if (_taxFee == 0 && _liquidityFee == 0 && _charityFee ==
0) return;

        _previousTaxFee = _taxFee;
        _previousLiquidityFee = _liquidityFee;
        _previousCharityFee = _charityFee;

        _taxFee = 0;
        _liquidityFee = 0;
        _charityFee = 0;
    }
    function restoreAllFee() private {
        _taxFee = _previousTaxFee;
        _liquidityFee = _previousLiquidityFee;
        _charityFee = _previousCharityFee;
    }
    function isExcludedFromFee(address account) public view
returns (bool) {
        return _isExcludedFromFee[account];
    }
    function _approve(
        address owner,
        address spender,
        uint256 amount
    ) private {
        require(owner != address(0), "ERC20: approve from the zero
address");
        require(spender != address(0), "ERC20: approve to the zero
address");

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

    function _transfer(
        address from,
        address to,
        uint256 amount
    ) private {
```

```
        require(from != address(0), "ERC20: transfer from the zero
address");
        require(to != address(0), "ERC20: transfer to the zero
address");
        require(amount > 0, "Transfer amount must be greater than
zero");

        if (enableAntiBot) {
            pinkAntiBot.onPreTransferCheck(from, to, amount);
        }

        // is the token balance of this contract address over the
min number of
        // tokens that we need to initiate a swap + liquidity
lock?
        // also, don't get caught in a circular liquidity event.
        // also, don't swap & liquify if sender is uniswap pair.
        uint256 contractTokenBalance = balanceOf(address(this));

        bool overMinTokenBalance = contractTokenBalance >=
            numTokensSellToAddToLiquidity;
        if (
            overMinTokenBalance &&
            !inSwapAndLiquify &&
            from != uniswapV2Pair &&
            swapAndLiquifyEnabled
        ) {
            contractTokenBalance = numTokensSellToAddToLiquidity;
            //add liquidity
            swapAndLiquify(contractTokenBalance);
        }

        //indicates if fee should be deducted from transfer
        bool takeFee = true;

        //if any account belongs to _isExcludedFromFee account
then remove the fee
        if (_isExcludedFromFee[from] || _isExcludedFromFee[to]) {
            takeFee = false;
        }

        //transfer amount, it will take tax, burn, liquidity fee
```

```
        _tokenTransfer(from, to, amount, takeFee);
    }

    function swapAndLiquify(uint256 contractTokenBalance) private
lockTheSwap {
        // split the contract balance into halves
        uint256 half = contractTokenBalance.div(2);
        uint256 otherHalf = contractTokenBalance.sub(half);

        // capture the contract's current ETH balance.
        // this is so that we can capture exactly the amount of
ETH that the
        // swap creates, and not make the liquidity event include
any ETH that
        // has been manually sent to the contract
        uint256 initialBalance = address(this).balance;

        // swap tokens for ETH
        swapTokensForEth(half); // <- this breaks the ETH -> HATE
swap when swap+liquify is triggered

        // how much ETH did we just swap into?
        uint256 newBalance =
address(this).balance.sub(initialBalance);

        // add liquidity to uniswap
        addLiquidity(otherHalf, newBalance);

        emit SwapAndLiquify(half, newBalance, otherHalf);
    }

    function swapTokensForEth(uint256 tokenAmount) private {
        // generate the uniswap pair path of token -> weth
        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
        );
    }

    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
        );
    }

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

        if (_isExcluded[sender] && !_isExcluded[recipient]) {
            _transferFromExcluded(sender, recipient, amount);
        } else if (!_isExcluded[sender] && _isExcluded[recipient])
{
            _transferToExcluded(sender, recipient, amount);
```

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

        if (!takeFee) restoreAllFee();
    }
    function _transferStandard(
        address sender,
        address recipient,
        uint256 tAmount
    ) private {
        (
            uint256 rAmount,
            uint256 rTransferAmount,
            uint256 rFee,
            uint256 tTransferAmount,
            uint256 tFee,
            uint256 tLiquidity,
            uint256 tCharity
        ) = _getValues(tAmount);
        _rOwned[sender] = _rOwned[sender].sub(rAmount);
        _rOwned[recipient] =
_rOwned[recipient].add(rTransferAmount);
        _takeLiquidity(tLiquidity);
        _takeCharityFee(tCharity);
        _reflectFee(rFee, tFee);
        emit Transfer(sender, recipient, tTransferAmount);
    }

    function _transferToExcluded(
        address sender,
        address recipient,
        uint256 tAmount
    ) private {
        (
            uint256 rAmount,
```

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

4. Tax Fee contract

```
function setTaxFeePercent(uint256 taxFeeBps) external onlyOwner {
        _taxFee = taxFeeBps;
        require(
            _taxFee + _liquidityFee + _charityFee <= 10**4 / 4,
            "Total fee is over 25%"
        );
    }

    function setLiquidityFeePercent(uint256 liquidityFeeBps)
        external
        onlyOwner
    {
        _liquidityFee = liquidityFeeBps;
        require(
            _taxFee + _liquidityFee + _charityFee <= 10**4 / 4,
            "Total fee is over 25%"
        );
    }
```

The owner can't set fees over 25%

5. PinkAntiBot

```
interface IPinkAntiBot {
  function setTokenOwner(address owner) external;

  function onPreTransferCheck(
    address from,
    address to,
    uint256 amount
  ) external;
}
...
 function setEnableAntiBot(bool _enable) external onlyOwner {
        enableAntiBot = _enable;
    }
```

The owner can set antibot to enable or not.

READ CONTRACT (ONLY NEED TO KNOW)

1. Version
1 uint256
(Shows Contract Versions)

2. _charityAddress
0x0000000000000000000000000000000000000000 address
(Shows the charity address)

3. enableAntiBot
True bool
(Function for read anti bot active or not)

4. _charityFee
0 uint256
(Function for read charity fee)

5. _liquidityFee
2 uint256
(Function for read liquidity fee)

6. _taxFee
1 uint256
(Function for read tax fee)

7. name
Tripin string
(Function for read Token name)

WRITE CONTRACT

1. setEnableAntiBot
_enable (bool)
(The form is filled with the true or false for active or deactivate anti bot)

2. renounceOwnership
(Renouncing ownership will leave the contract without an owner, thereby removing any functionality that is only available to the owner)

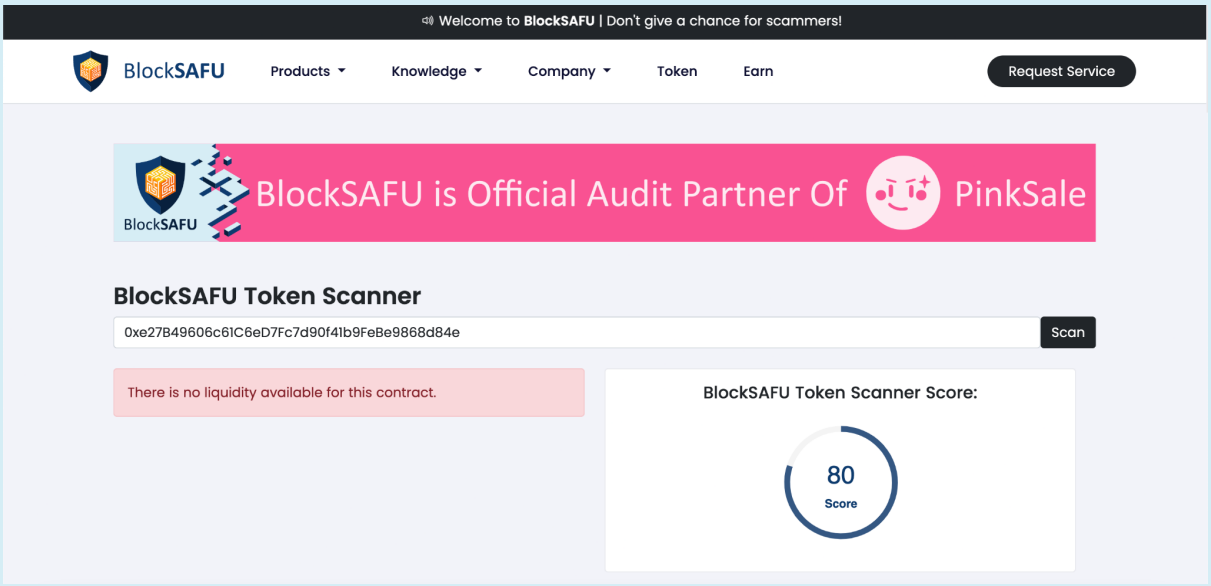
3. transferOwnership
newOwner (address)
(Its function is to change the owner)

4. setLiquiditFeePercent (cannot set over 25%)
liquidityFeeBps (uint 256)
(The form is filled with new fee, for change liquidity fee)

5. setTaxFeePercent (cannot set over 25%)
taxFeeBps (uint 256)
(The form is filled with new fee, for change Tax fee)

BlockSAFU TOKEN SCANNER

https://blocksafu.com/token-scanner



Token Information

Indicator	Value
Token Name	Tripin
Token Symbol	TRIP
Total Supply	1,000,000,000,000,000
Already Listed On Dex	Already Listed
Dex Listed	PancakeV2
Open Source	Open Source
Price	$0.00000000
Volume 24H	$0.00
Liquidity	$0 (0.00 BNB)
Tx Count 24H	0
Marketcap	$0

Security Information

Indicator	Value
Honeypot	Liquidity Not Available
Buy Fees	0%
Sell Fees	0%
Buy Gas	0 **Gwei (0.000000 BNB / $0.00)**
Sell Gas	0 **Gwei (0.000000 BNB / $0.00)**
Holder Count	2 **Holders**

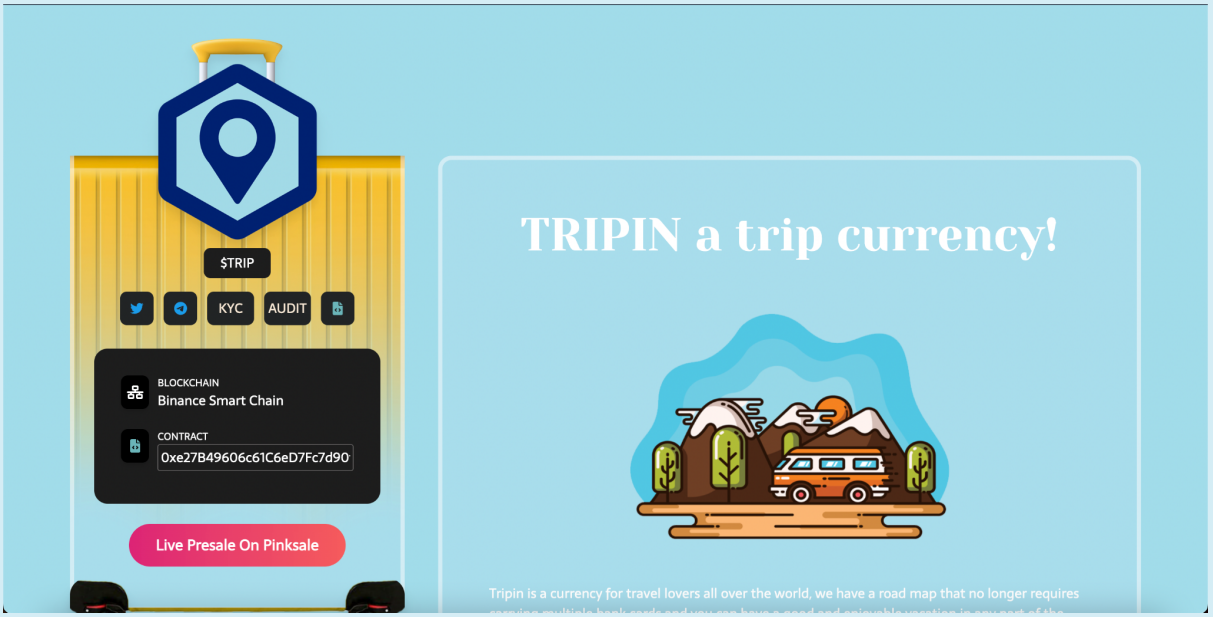
Honeypot Safety

Indicator	Value
Can Take Back Ownership	Not detected
Owner Change Balance	Not detected
Blacklist	Not detected
Modify Fees	Detected
Proxy	Not detected
Whitelisted	Not detected
Anti Whale	Detected
Trading Cooldown	Not detected
Transfer Pausable	Not detected
Cannot Sell All	Not detected

Rug Pull Safety

Indicator	Value
Hidden Owner	Not detected
Creator Address	0x2a688caa...5cc
Creator Balance	500,000,000,000,000 TRIP
Creator Percent	50%
Owner Address	0x2a688caa...5cc
Owner Balance	500,000,000,000,000 TRIP
Owner Percent	50%
Lp Holder Count	0
Lp Total Supply	NaN
Mint	Not detected

WEBSITE REVIEW



- **Mobile Friendly**
- **Contains no code error**
- **SSL Secured (By Sectigot SSL)**

Web-Tech stack: jQuery, FontAwesome, Slick

Domain .io (namecheap) - Tracked by whois

First Contentful Paint:	1.0s
Fully Loaded Time	1.9s
Performance	60%
Accessibility	76%
Best Practices	83%
SEO	70%

RUG-PULL REVIEW

Based on the available information analyzed by us, we come to the following conclusions:

- Locked Liquidity (Locked by pinksale)

  (*Will be updated after DEX listing*)

- TOP 5 Holder.

  (*Will be updated after DEX listing*)

- The Team No KYC on Blocksafu

HONEYPOT REVIEW

- Ability to sell.
- The owner is not able to pause the contract.
- The owner can’t set fees over 25%
- PinkAntiBot

Note: Please check the disclaimer above and note, that the audit makes no statements or warranties on the business model, investment attractiveness, or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by the project owner.