BlockSAFU

ADVANCE MANUAL
SMART CONTRACT AUDIT

Project: Kasa Central

Website: https://kasacentral.net/

PASSED

BlockSAFU Score:

96

Contract Address:

0x7cfcE51E7e4a1862A94102499a708575B10b2dBC

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 KasaCentral 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	**KasaCentral**
Token Symbol	**KASA**
Token Decimal	18
Total Supply	100,000,000 **KASA**
Contract Address	0x7cfcE51E7e4a1862A94102499a708575B10b2dBC
Deployer Address	0xA11D7d8e3E0fa73AF87F4fF33f99A96C68B16c17
Owner Address	0xA11D7d8e3E0fa73AF87F4fF33f99A96C68B16c17
Tax Fees Buy	0%
Tax Fees Sell	0%
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-28-2022 12:23:59 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	v0.8.16+commit.07a7930e
Optimization	Yes with 5000 runs
Sol License	MIT License
Top 5 Holders	*will be updated after the DEX listing*
Other	default evmVersion

TAX

BUY	0%	**SELL**	0%

OVERVIEW

Mint Function

- No mint functions.

Fees

- Buy 0% (owner can’t set fees).
- Sell 0% (owner can’t set fees).

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.

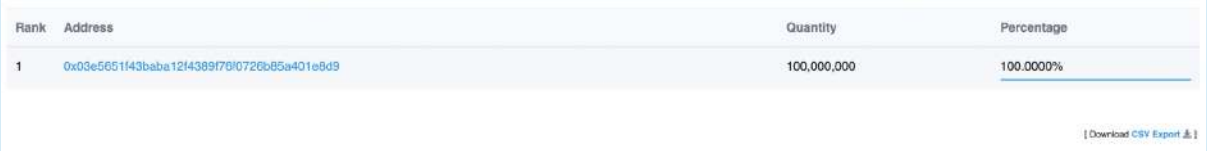
Anti Whale

- Owner cannot limit the number of wallet holdings.

Trading Cooldown

- Owner cannot set the selling time interval.

Token Holder



Rank	Address	Quantity	Percentage
1	0x03e5651f43baba12f4389f76f0726b85a401e8d9	100,000,000	100.0000%

[Download CSV Export]

Team Review

The Doge Ipa team has a nice website, their website is professionally built and the Smart contract is well developed, their social media is growing with over 10,203 people in their telegram group (count in audit date).

Official Website And Social Media

Website: https://kasacentral.net/

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

Twitter: https://twitter.com/CentralKasa

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 amount of tokens in existence.
     */
    function totalSupply() external view returns (uint256);

    /**
     * @dev Returns the amount of tokens owned by `account`.
     */
    function balanceOf(address account) external view returns
(uint256);

    /**
     * @dev Moves `amount` tokens from the caller's account to
`recipient`.
     *
     * Returns a boolean value indicating whether the operation
succeeded.
     *
     * Emits a {Transfer} event.
     */
    function transfer(address recipient, uint256 amount) external
returns (bool);

    /**
     * @dev Returns the remaining number of tokens that `spender`
will be
     * allowed to spend on behalf of `owner` through
{transferFrom}. This is
     * zero by default.
     *
     * This value changes when {approve} or {transferFrom} are
called.
     */
    function allowance(address owner, address spender) external
view returns (uint256);

    /**
     * @dev Sets `amount` as the allowance of `spender` over the
```

```
caller's tokens.
     *
     * Returns a boolean value indicating whether the operation
succeeded.
     *
     * IMPORTANT: Beware that changing an allowance with this
method brings the risk
     * that someone may use both the old and the new allowance by
unfortunate
     * transaction ordering. One possible solution to mitigate this
race
     * condition is to first reduce the spender's allowance to 0
and set the
     * desired value afterwards:
     *
https://github.com/ethereum/EIPs/issues/20#issuecomment-263524729
     *
     * Emits an {Approval} event.
     */
    function approve(address spender, uint256 amount) external
returns (bool);

    /**
     * @dev Moves `amount` tokens from `sender` to `recipient`
using the
     * allowance mechanism. `amount` is then deducted from the
caller's
     * allowance.
     *
     * Returns a boolean value indicating whether the operation
succeeded.
     *
     * Emits a {Transfer} event.
     */
    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);

    /**
     * @dev Emitted when the allowance of a `spender` for an
`owner` is set by
     * a call to {approve}. `value` is the new allowance.
     */
    event Approval(address indexed owner, address indexed spender,
uint256 value);
}
```

IERC20 Normal Base Template

3. KasaCentral Contract

```
contract KasaCentral is IERC20 {
    mapping (address => uint256) private _tOwned;
    mapping (address => bool) lpPairs;
    uint256 private timeSinceLastPair = 0;
    mapping (address => mapping (address => uint256)) private
_allowances;

    mapping (address => bool) private _liquidityHolders;
    mapping (address => bool) private _isExcludedFromProtection;
    mapping (address => bool) private _isExcludedFromLimits;
    bool private allowedPresaleExclusion = true;

    uint256 constant private startingSupply = 100_000_000;
    string constant private _name = "Kasa Central";
    string constant private _symbol = "KASA";
    uint8 constant private _decimals = 18;
    uint256 constant private _tTotal = startingSupply *
10**_decimals;

    bool public taxesAreLocked;
    IRouter02 public dexRouter;
    address public lpPair;
    address constant public DEAD =
0x000000000000000000000000000000000000dEaD;

    bool public tradingEnabled = false;
    bool public _hasLiqBeenAdded = false;
    AntiSnipe antiSnipe;

    event OwnershipTransferred(address indexed previousOwner,
address indexed newOwner);

    modifier onlyOwner() {
        require(_owner == msg.sender, "Caller =/= owner.");
        _;
    }

    constructor () payable {
        _tOwned[msg.sender] = _tTotal;
        emit Transfer(address(0), msg.sender, _tTotal);
```

```
        // Set the owner.
        _owner = msg.sender;
        originalDeployer = msg.sender;

        if (block.chainid == 56) {
            dexRouter =
IRouter02(0x10ED43C718714eb63d5aA57B78B54704E256024E);
        } else if (block.chainid == 97) {
            dexRouter =
IRouter02(0xD99D1c33F9fC3444f8101754aBC46c52416550D1);
        } else if (block.chainid == 1 || block.chainid == 4 ||
block.chainid == 3) {
            dexRouter =
IRouter02(0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D);
            //Ropstein DAI
0xaD6D458402F60fD3Bd25163575031ACDce07538D
        } else if (block.chainid == 43114) {
            dexRouter =
IRouter02(0x60aE616a2155Ee3d9A68541Ba4544862310933d4);
        } else if (block.chainid == 250) {
            dexRouter =
IRouter02(0xF491e7B69E4244ad4002BC14e878a34207E38c29);
        } else {
            revert();
        }

        lpPair =
IFactoryV2(dexRouter.factory()).createPair(dexRouter.WETH(),
address(this));
        lpPairs[lpPair] = true;

        _approve(_owner, address(dexRouter), type(uint256).max);
        _approve(address(this), address(dexRouter),
type(uint256).max);
        _liquidityHolders[_owner] = true;
    }

    receive() external payable {}

//================================================================
==============================================
//================================================================
```

```
============================================
//==========================================================
============================================
    // Ownable removed as a lib and added here to allow for custom
transfers and renouncements.
    // This allows for removal of ownership privileges from the
owner once renounced or transferred.

    address private _owner;
    address public originalDeployer;
    address public operator;

    function transferOwner(address newOwner) external onlyOwner {
        require(newOwner != address(0), "Call renounceOwnership to
transfer owner to the zero address.");
        require(newOwner != DEAD, "Call renounceOwnership to
transfer owner to the zero address.");
        if (balanceOf(_owner) > 0) {
            finalizeTransfer(_owner, newOwner, balanceOf(_owner),
true);
        }

        address oldOwner = _owner;
        _owner = newOwner;
        emit OwnershipTransferred(oldOwner, newOwner);

    }

    function renounceOwnership() external onlyOwner {
        address oldOwner = _owner;
        _owner = address(0);
        emit OwnershipTransferred(oldOwner, address(0));
    }

    // Function to set an operator to allow someone other the
deployer to create things such as launchpads.
    // Only callable by original deployer.
    function setOperator(address newOperator) external {
        require(msg.sender == originalDeployer, "Can only be
called by original deployer.");
        address oldOperator = operator;
        if (oldOperator != address(0)) {
```

```
            _liquidityHolders[oldOperator] = false;
        }
        operator = newOperator;
        _liquidityHolders[newOperator] = true;
    }

    function renounceOriginalDeployer() external {
        require(msg.sender == originalDeployer, "Can only be
called by original deployer.");
        originalDeployer = address(0);
    }
//======================================================================
========================================
//======================================================================
========================================
//======================================================================
========================================

    function totalSupply() external pure override returns
(uint256) { if (_tTotal == 0) { revert(); } return _tTotal; }
    function decimals() external pure override returns (uint8) {
if (_tTotal == 0) { revert(); } return _decimals; }
    function symbol() external pure override returns (string
memory) { return _symbol; }
    function name() external pure override returns (string memory)
{ return _name; }
    function getOwner() external view override returns (address) {
return _owner; }
    function allowance(address holder, address spender) external
view override returns (uint256) { return
_allowances[holder][spender]; }
    function balanceOf(address account) public view override
returns (uint256) {
        return _tOwned[account];
    }

    function transfer(address recipient, uint256 amount) public
override returns (bool) {
        _transfer(msg.sender, recipient, amount);
        return true;
    }
```

```
    function approve(address spender, uint256 amount) external
override returns (bool) {
        _approve(msg.sender, spender, amount);
        return true;
    }

    function _approve(address sender, address spender, uint256
amount) internal {
        require(sender != address(0), "ERC20: Zero Address");
        require(spender != address(0), "ERC20: Zero Address");

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

    function approveContractContingency() external onlyOwner
returns (bool) {
        _approve(address(this), address(dexRouter),
type(uint256).max);
        return true;
    }

    function transferFrom(address sender, address recipient,
uint256 amount) external override returns (bool) {
        if (_allowances[sender][msg.sender] != type(uint256).max)
{
            _allowances[sender][msg.sender] -= amount;
        }

        return _transfer(sender, recipient, amount);
    }

    function setInitializer(address initializer) external
onlyOwner {
        require(!tradingEnabled);
        require(initializer != address(this), "Can't be self.");
        antiSnipe = AntiSnipe(initializer);
    }

    function isExcludedFromLimits(address account) external view
returns (bool) {
        return _isExcludedFromLimits[account];
```

```
    }

    function isExcludedFromProtection(address account) external
view returns (bool) {
        return _isExcludedFromProtection[account];
    }

    function setExcludedFromLimits(address account, bool enabled)
external onlyOwner {
        _isExcludedFromLimits[account] = enabled;
    }

    function setExcludedFromProtection(address account, bool
enabled) external onlyOwner {
        _isExcludedFromProtection[account] = enabled;
    }

    function getCirculatingSupply() public view returns (uint256)
{
        return (_tTotal - (balanceOf(DEAD) +
balanceOf(address(0))));
    }

    function removeSniper(address account) external onlyOwner {
        antiSnipe.removeSniper(account);
    }

    function setProtectionSettings(bool _antiSnipe, bool
_antiBlock) external onlyOwner {
        antiSnipe.setProtections(_antiSnipe, _antiBlock);
    }

    function excludePresaleAddresses(address router, address
presale) external onlyOwner {
        require(allowedPresaleExclusion);
        require(router != address(this) && presale !=
address(this), "Just don't.");
        if (router == presale) {
            _liquidityHolders[presale] = true;
        } else {
            _liquidityHolders[router] = true;
            _liquidityHolders[presale] = true;
```

```
        }
    }

    function _hasLimits(address from, address to) internal view
returns (bool) {
        return from != _owner
            && to != _owner
            && tx.origin != _owner
            && !_liquidityHolders[to]
            && !_liquidityHolders[from]
            && to != DEAD
            && to != address(0)
            && from != address(this)
            && from != address(antiSnipe)
            && to != address(antiSnipe);
    }

    function _transfer(address from, address to, uint256 amount)
internal returns (bool) {
        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");
        bool buy = false;
        bool sell = false;
        bool other = false;
        if (lpPairs[from]) {
            buy = true;
        } else if (lpPairs[to]) {
            sell = true;
        } else {
            other = true;
        }
        if (_hasLimits(from, to)) {
            if(!tradingEnabled) {
                revert("Trading not yet enabled!");
            }
        }

        return finalizeTransfer(from, to, amount, other);
```

```
    }

    function _checkLiquidityAdd(address from, address to) internal
{
        require(!_hasLiqBeenAdded, "Liquidity already added and
marked.");
        if (!_hasLimits(from, to) && to == lpPair) {
            _liquidityHolders[from] = true;
            _hasLiqBeenAdded = true;
            if (address(antiSnipe) == address(0)){
                antiSnipe = AntiSnipe(address(this));
            }
        }
    }

    function enableTrading() public onlyOwner {
        require(!tradingEnabled, "Trading already enabled!");
        require(_hasLiqBeenAdded, "Liquidity must be added.");
        if (address(antiSnipe) == address(0)){
            antiSnipe = AntiSnipe(address(this));
        }
        try antiSnipe.setLaunch(lpPair, uint32(block.number),
uint64(block.timestamp), _decimals) {} catch {}
        tradingEnabled = true;
        allowedPresaleExclusion = false;
    }

    function sweepContingency() external onlyOwner {
        require(!_hasLiqBeenAdded, "Cannot call after
liquidity.");
        payable(_owner).transfer(address(this).balance);
    }

    function multiSendTokens(address[] memory accounts, uint256[]
memory amounts) external onlyOwner {
        require(accounts.length == amounts.length, "Lengths do not
match.");
        for (uint16 i = 0; i < accounts.length; i++) {
            require(balanceOf(msg.sender) >= amounts[i]);
            finalizeTransfer(msg.sender, accounts[i],
amounts[i]*10**_decimals, true);
        }
```

```
    }

    function finalizeTransfer(address from, address to, uint256
amount, bool other) internal returns (bool) {
        if (!_hasLiqBeenAdded) {
            _checkLiquidityAdd(from, to);
            if (!_hasLiqBeenAdded && _hasLimits(from, to) &&
!_isExcludedFromProtection[from] && !_isExcludedFromProtection[to]
&& !other) {
                revert("Pre-liquidity transfer protection.");
            }
        }

        if (_hasLimits(from, to)) { bool checked;
            try antiSnipe.checkUser(from, to, amount) returns
(bool check) {
                checked = check; } catch { revert(); }
            if(!checked) { revert(); }
        }
        _tOwned[from] -= amount;
        _tOwned[to] += amount;

        emit Transfer(from, to, amount);
        return true;
    }
}
```

READ CONTRACT (ONLY NEED TO KNOW)

1. DEAD
0x000000000000000000000000000000000000dead address
(Shows dead address)

2. _hasLiqBeenAdded
False bool
(Shows status liquidity been added)

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

4. decimals
18 uint8
(Function for read decimals)

5. dexRouter
0xd99d1c33f9fc3444f8101754abc46c52416550d1 address
(Function for read dex router)

6. getOwner
0x03e5651f43baba12f4389f76f0726b85a401e8d9 address
(Function for read owner)

7. name
Kasa Central string
(Function for read Token name)

WRITE CONTRACT

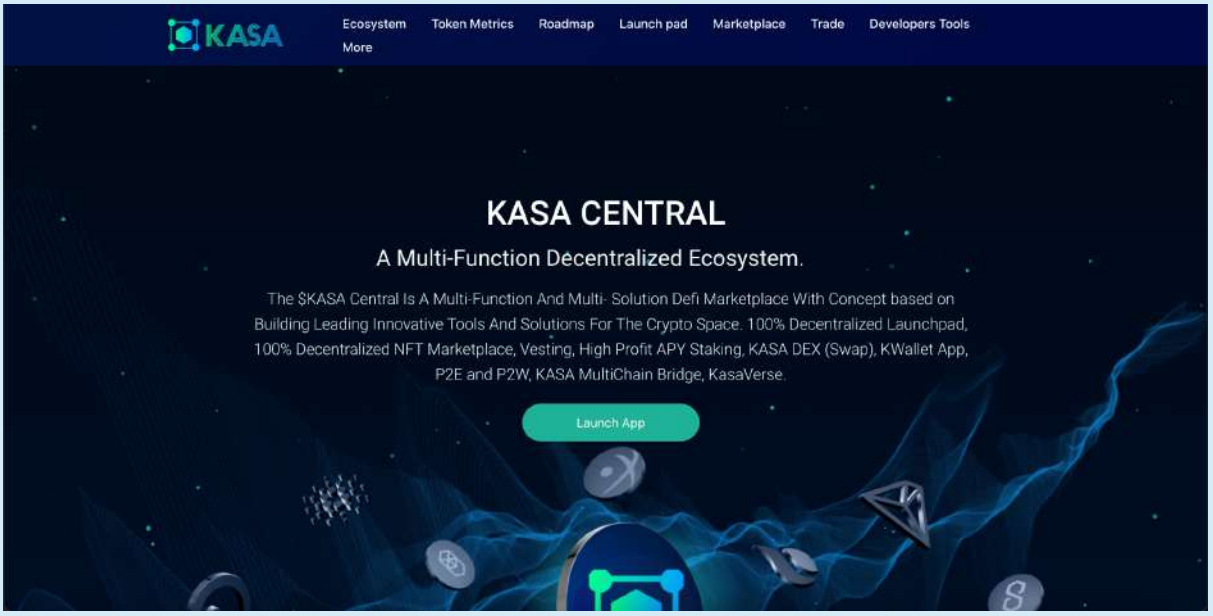
1. enableTrading
(Call action for enable trading)

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. setOperator
newOperator (addresss)
(The form is filled with address, for set Operator)

WEBSITE REVIEW



- **Mobile Friendly**
- **Contains no code error**
- **SSL Secured (By R3 SSL)**

Web-Tech stack:

Domain .net (Bluehost) - Tracked by whois

First Contentful Paint:	394ms
Fully Loaded Time	6.7s
Performance	89%
Accessibility	98%
Best Practices	100%
SEO	92%

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 KYC on Pinksale

HONEYPOT REVIEW

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

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.