Smart Contract Security Audit Report

Supervised by Star Tower

Audit number: STC822912023801a

StarTowerChain

Audit number：

STC822912023801a

Token name：

FanShen (**FanShen**)

Audit contract address：

0xD7314b37a63b47A52cAe00f8cBDf0EB2A81EE672

Audit contract link address：

https://bscscan.com/token/0xd7314b37a63b47a52cae00f8cbdf0eb2a81ee672#code

Audit results：

After the audit, the (FanShen) contract passed all tests, and the contract audit result was passed (excellent)

Smart contract permissions：

The basic contract does not have too many permissions

Audit team：

StarTowerChain COMPANY

Types of Audits and Results：

SN	Audit type	Audit subkey	Audit results
1	overflow audit	-	pass√
2	function call auditing	1. .call/delegatecall security audit 2. Function return value security audit 3. Self-destructing function security audit 4. Function call permission audit	pass√

		5. Compiler version safety	
3	Reentrant Attack Audit	-	pass√
4	Gas optimization audit	-	pass√
5	"Fake Top-Up" Vulnerability Audit	-	pass√
6	Pseudo-random number generation audit	-	pass√
7	Code Specification Audit	1. ERC-20 Token Standard Specification Audit 2. Redundant code audit 3. Variable coverage audit 4. Deprecated item auditing	pass√
8	Business Security Audit	1. owner permission audit 2. Business logic audit 3. Business implementation audit	pass√
9	Denial of Service Attack Audit	-	pass√
10	Block parameter dependency auditing	-	pass√

11	Abnormal reachability status audit	-	**pass√**

Note: Please refer to the code comments for audit opinions and suggestions!

(StarTowerChain Statement: StarTowerChain only issues this report based on the attacks or vulnerabilities that have existed or occurred before the issuance of this report. For new attacks or vulnerabilities that exist or occur after the issuance of this report, StarTowerChain cannot judge the security of smart contracts. We do not take any responsibility for the possible impact of the situation. The security audit analysis and other contents in this report are only based on the documents and information provided by the FanShen contract provider to StarTowerChain before the issuance of this report, and this part of the documents and information Made under the premise that there is no defect, tampering, deletion or concealment; if the documents and materials provided have information lacking, tampering, deletion, concealment or the reflected situation does not match the actual situation or provide documents and information If there are any changes after the issuance of this report, StarTowerChain will not be responsible for any losses and adverse effects caused thereby.)

一.Basic information of Token

Token name	FanShen
Token symbol	**FanShen**
decimals	**18**
totalSupply	**2,00,000**

Token type	**BEP-20**

The contract source code is as follows:

```
/**
 *Submitted for verification at BscScan.com on 2024-05-19
*/


//SPDX-License-Identifier: Unlicensed
pragma solidity ^0.8.0;


/**
 * @dev Provides information about the current execution context, including the
 * sender of the transaction and its data. While these are generally available
 * via msg.sender and msg.data, they should not be accessed in such a direct
 * manner, since when dealing with meta-transactions the account sending and
 * paying for execution may not be the actual sender (as far as an application
 * is concerned).
 *
 * This contract is only required for intermediate, library-like contracts.
 */
abstract contract Context {
    function _msgSender() internal view virtual returns (address) {
        return msg.sender;
    }
```

```
    function _msgData() internal view virtual returns (bytes calldata) {
        return msg.data;
    }
}

/**
 * @dev Contract module which provides a basic access control mechanism, where
 * there is an account (an owner) that can be granted exclusive access to
 * specific functions.
 *
 * By default, the owner account will be the one that deploys the contract. This
 * can later be changed with {transferOwnership}.
 *
 * This module is used through inheritance. It will make available the modifier
 * `onlyOwner`, which can be applied to your functions to restrict their use to
 * the owner.
 */
abstract contract Ownable is Context {
    address private _owner;

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

    /**
     * @dev Initializes the contract setting the deployer as the initial owner.
```

```
 */
constructor() {
    _transferOwnership(_msgSender());
}

/**
 * @dev Returns the address of the current owner.
 */
function owner() public view virtual returns (address) {
    return _owner;
}

/**
 * @dev Throws if called by any account other than the owner.
 */
modifier onlyOwner() {
    require(owner() == _msgSender(), "Ownable: caller is not the owner");
    _;
}

/**
 * @dev Leaves the contract without owner. It will not be possible to call
 * `onlyOwner` functions anymore. Can only be called by the current owner.
 *
 * NOTE: Renouncing ownership will leave the contract without an owner,
 * thereby removing any functionality that is only available to the owner.
```

```
     */
    function renounceOwnership() public virtual onlyOwner {
        _transferOwnership(address(0));
    }

    /**
     * @dev Transfers ownership of the contract to a new account (`newOwner`).
     * Can only be called by the current owner.
     */
    function transferOwnership(address newOwner) public virtual onlyOwner {
        require(newOwner != address(0), "Ownable: new owner is the zero address");
        _transferOwnership(newOwner);
    }

    /**
     * @dev Transfers ownership of the contract to a new account (`newOwner`).
     * Internal function without access restriction.
     */
    function _transferOwnership(address newOwner) internal virtual {
        address oldOwner = _owner;
        _owner = newOwner;
        emit OwnershipTransferred(oldOwner, newOwner);
    }
}
```

```
/**
 * @dev Interface of the ERC20 standard as defined in the EIP.
 */
interface IERC20 {
    /**
     * @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);

    /**
     * @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 `to`.
     *
     * Returns a boolean value indicating whether the operation succeeded.
     *
     * Emits a {Transfer} event.
     */
    function transfer(address to, 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 `from` to `to` 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 from,
        address to,
```

```
        uint256 amount
    ) external returns (bool);
}

/**
 * @dev Interface for the optional metadata functions from the ERC20 standard.
 *
 * _Available since v4.1._
 */
interface IERC20Metadata is IERC20 {
    /**
     * @dev Returns the name of the token.
     */
    function name() external view returns (string memory);

    /**
     * @dev Returns the symbol of the token.
     */
    function symbol() external view returns (string memory);

    /**
     * @dev Returns the decimals places of the token.
     */
    function decimals() external view returns (uint8);
}
```

```
/**
 * @dev Implementation of the {IERC20} interface.
 *
 * This implementation is agnostic to the way tokens are created. This means
 * that a supply mechanism has to be added in a derived contract using {_mint}.
 * For a generic mechanism see {ERC20PresetMinterPauser}.
 *
 * TIP: For a detailed writeup see our guide
 *
https://forum.zeppelin.solutions/t/how-to-implement-erc20-supply-mechanis
ms/226[How
 * to implement supply mechanisms].
 *
 * We have followed general OpenZeppelin Contracts guidelines: functions revert
 * instead returning `false` on failure. This behavior is nonetheless
 * conventional and does not conflict with the expectations of ERC20
 * applications.
 *
 * Additionally, an {Approval} event is emitted on calls to {transferFrom}.
 * This allows applications to reconstruct the allowance for all accounts just
 * by listening to said events. Other implementations of the EIP may not emit
 * these events, as it isn't required by the specification.
 *
 * Finally, the non-standard {decreaseAllowance} and {increaseAllowance}
 * functions have been added to mitigate the well-known issues around setting
 * allowances. See {IERC20-approve}.
```

```
 */
contract ERC20 is Context, IERC20, IERC20Metadata {
    mapping(address => uint256) private _balances;

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

    uint256 private _totalSupply;

    string private _name;
    string private _symbol;

    /**
     * @dev Sets the values for {name} and {symbol}.
     *
     * The default value of {decimals} is 18. To select a different value for
     * {decimals} you should overload it.
     *
     * All two of these values are immutable: they can only be set once during
     * construction.
     */
    constructor(string memory name_, string memory symbol_) {
        _name = name_;
        _symbol = symbol_;
    }

    /**
```

```
     * @dev Returns the name of the token.
     */
    function name() public view virtual override returns (string memory) {
        return _name;
    }

    /**
     * @dev Returns the symbol of the token, usually a shorter version of the
     * name.
     */
    function symbol() public view virtual override returns (string memory) {
        return _symbol;
    }

    /**
     * @dev Returns the number of decimals used to get its user representation.
     * For example, if `decimals` equals `2`, a balance of `505` tokens should
     * be displayed to a user as `5.05` (`505 / 10 ** 2`).
     *
     * Tokens usually opt for a value of 18, imitating the relationship between
     * Ether and Wei. This is the value {ERC20} uses, unless this function is
     * overridden;
     *
     * NOTE: This information is only used for _display_ purposes: it in
     * no way affects any of the arithmetic of the contract, including
     * {IERC20-balanceOf} and {IERC20-transfer}.
```

```
     */
    function decimals() public view virtual override returns (uint8) {
        return 18;
    }

    /**
     * @dev See {IERC20-totalSupply}.
     */
    function totalSupply() public view virtual override returns (uint256) {
        return _totalSupply;
    }

    /**
     * @dev See {IERC20-balanceOf}.
     */
    function balanceOf(address account) public view virtual override returns
(uint256) {
        return _balances[account];
    }

    /**
     * @dev See {IERC20-transfer}.
     *
     * Requirements:
     *
     * - `to` cannot be the zero address.
```

```
     * - the caller must have a balance of at least `amount`.
     */
    function transfer(address to, uint256 amount) public virtual override returns (bool) {
        address owner = _msgSender();
        _transfer(owner, to, amount);
        return true;
    }

    /**
     * @dev See {IERC20-allowance}.
     */
    function allowance(address owner, address spender) public view virtual override returns (uint256) {
        return _allowances[owner][spender];
    }

    /**
     * @dev See {IERC20-approve}.
     *
     * NOTE: If `amount` is the maximum `uint256`, the allowance is not updated on
     * `transferFrom`. This is semantically equivalent to an infinite approval.
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
```

```
     */
    function approve(address spender, uint256 amount) public virtual override
returns (bool) {
        address owner = _msgSender();
        _approve(owner, spender, amount);
        return true;
    }

    /**
     * @dev See {IERC20-transferFrom}.
     *
     * Emits an {Approval} event indicating the updated allowance. This is not
     * required by the EIP. See the note at the beginning of {ERC20}.
     *
     * NOTE: Does not update the allowance if the current allowance
     * is the maximum `uint256`.
     *
     * Requirements:
     *
     * - `from` and `to` cannot be the zero address.
     * - `from` must have a balance of at least `amount`.
     * - the caller must have allowance for ``from``'s tokens of at least
     * `amount`.
     */
    function transferFrom(
        address from,
```

```
        address to,
        uint256 amount
    ) public virtual override returns (bool) {
        address spender = _msgSender();
        _spendAllowance(from, spender, amount);
        _transfer(from, to, amount);
        return true;
    }

    /**
     * @dev Atomically increases the allowance granted to `spender` by the caller.
     *
     * This is an alternative to {approve} that can be used as a mitigation for
     * problems described in {IERC20-approve}.
     *
     * Emits an {Approval} event indicating the updated allowance.
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
     */
    function increaseAllowance(address spender, uint256 addedValue) public virtual returns (bool) {
        address owner = _msgSender();
        _approve(owner, spender, allowance(owner, spender) + addedValue);
```

```
        return true;
    }

    /**
     * @dev Atomically decreases the allowance granted to `spender` by the caller.
     *
     * This is an alternative to {approve} that can be used as a mitigation for
     * problems described in {IERC20-approve}.
     *
     * Emits an {Approval} event indicating the updated allowance.
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
     * - `spender` must have allowance for the caller of at least
     * `subtractedValue`.
     */
    function decreaseAllowance(address spender, uint256 subtractedValue) public virtual returns (bool) {
        address owner = _msgSender();
        uint256 currentAllowance = allowance(owner, spender);
        require(currentAllowance >= subtractedValue, "ERC20: decreased allowance below zero");
        unchecked {
            _approve(owner, spender, currentAllowance - subtractedValue);
        }
```

```
        return true;
    }

    /**
     * @dev Moves `amount` of tokens from `sender` to `recipient`.
     *
     * This internal function is equivalent to {transfer}, and can be used to
     * e.g. implement automatic token fees, slashing mechanisms, etc.
     *
     * Emits a {Transfer} event.
     *
     * Requirements:
     *
     * - `from` cannot be the zero address.
     * - `to` cannot be the zero address.
     * - `from` must have a balance of at least `amount`.
     */
    function _transfer(
        address from,
        address to,
        uint256 amount
    ) internal virtual {
        require(from != address(0), "ERC20: transfer from the zero address");
        require(to != address(0), "ERC20: transfer to the zero address");
```

```
        _beforeTokenTransfer(from, to, amount);

        uint256 fromBalance = _balances[from];
        require(fromBalance >= amount, "ERC20: transfer amount exceeds
balance");
        unchecked {
            _balances[from] = fromBalance - amount;
        }
        _balances[to] += amount;

        emit Transfer(from, to, amount);

        _afterTokenTransfer(from, to, amount);
    }

    /** @dev Creates `amount` tokens and assigns them to `account`, increasing
     * the total supply.
     *
     * Emits a {Transfer} event with `from` set to the zero address.
     *
     * Requirements:
     *
     * - `account` cannot be the zero address.
     */
    function _mint(address account, uint256 amount) internal virtual {
        require(account != address(0), "ERC20: mint to the zero address");
```

```
        _beforeTokenTransfer(address(0), account, amount);

        _totalSupply += amount;
        _balances[account] += amount;
        emit Transfer(address(0), account, amount);

        _afterTokenTransfer(address(0), account, amount);
    }

    /**
     * @dev Destroys `amount` tokens from `account`, reducing the
     * total supply.
     *
     * Emits a {Transfer} event with `to` set to the zero address.
     *
     * Requirements:
     *
     * - `account` cannot be the zero address.
     * - `account` must have at least `amount` tokens.
     */
    function _burn(address account, uint256 amount) internal virtual {
        require(account != address(0), "ERC20: burn from the zero address");

        _beforeTokenTransfer(account, address(0), amount);
```

```
        uint256 accountBalance = _balances[account];
        require(accountBalance >= amount, "ERC20: burn amount exceeds balance");
        unchecked {
            _balances[account] = accountBalance - amount;
        }
        _totalSupply -= amount;

        emit Transfer(account, address(0), amount);

        _afterTokenTransfer(account, address(0), amount);
    }

    /**
     * @dev Sets `amount` as the allowance of `spender` over the `owner` s tokens.
     *
     * This internal function is equivalent to `approve`, and can be used to
     * e.g. set automatic allowances for certain subsystems, etc.
     *
     * Emits an {Approval} event.
     *
     * Requirements:
     *
     * - `owner` cannot be the zero address.
     * - `spender` cannot be the zero address.
```

```
     */
    function _approve(
        address owner,
        address spender,
        uint256 amount
    ) internal virtual {
        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);
    }

    /**
     * @dev Updates `owner` s allowance for `spender` based on spent `amount`.
     *
     * Does not update the allowance amount in case of infinite allowance.
     * Revert if not enough allowance is available.
     *
     * Might emit an {Approval} event.
     */
    function _spendAllowance(
        address owner,
        address spender,
        uint256 amount
    ) internal virtual {
```

```
        uint256 currentAllowance = allowance(owner, spender);
        if (currentAllowance != type(uint256).max) {
            require(currentAllowance >= amount, "ERC20: insufficient
allowance");
            unchecked {
                _approve(owner, spender, currentAllowance - amount);
            }
        }
    }

    /**
     * @dev Hook that is called before any transfer of tokens. This includes
     * minting and burning.
     *
     * Calling conditions:
     *
     * - when `from` and `to` are both non-zero, `amount` of ``from``'s tokens
     * will be transferred to `to`.
     * - when `from` is zero, `amount` tokens will be minted for `to`.
     * - when `to` is zero, `amount` of ``from``'s tokens will be burned.
     * - `from` and `to` are never both zero.
     *
     * To learn more about hooks, head to
xref:ROOT:extending-contracts.adoc#using-hooks[Using Hooks].
     */
    function _beforeTokenTransfer(
```

```
        address from,
        address to,
        uint256 amount
    ) internal virtual {}

    /**
     * @dev Hook that is called after any transfer of tokens. This includes
     * minting and burning.
     *
     * Calling conditions:
     *
     * - when `from` and `to` are both non-zero, `amount` of ``from``'s tokens
     * has been transferred to `to`.
     * - when `from` is zero, `amount` tokens have been minted for `to`.
     * - when `to` is zero, `amount` of ``from``'s tokens have been burned.
     * - `from` and `to` are never both zero.
     *
     * To learn more about hooks, head to
xref:ROOT:extending-contracts.adoc#using-hooks[Using Hooks].
     */
    function _afterTokenTransfer(
        address from,
        address to,
        uint256 amount
    ) internal virtual {}
}
```

```
library Math {
    function min(uint x, uint y) internal pure returns (uint z) {
        z = x < y ? x : y;
    }

    function sqrt(uint y) internal pure returns (uint z) {
        if (y > 3) {
            z = y;
            uint x = y / 2 + 1;
            while (x < z) {
                z = x;
                x = (y / x + x) / 2;
            }
        } else if (y != 0) {
            z = 1;
        }
    }
}
/**
 * @dev Collection of functions related to the address type
 */
library Address {
    /**
     * @dev Returns true if `account` is a contract.
     *
```

```
     * [IMPORTANT]
     * ====
     * It is unsafe to assume that an address for which this function returns
     * false is an externally-owned account (EOA) and not a contract.
     *
     * Among others, `isContract` will return false for the following
     * types of addresses:
     *
     *  - an externally-owned account
     *  - a contract in construction
     *  - an address where a contract will be created
     *  - an address where a contract lived, but was destroyed
     * ====
     *
     * [IMPORTANT]
     * ====
     * You shouldn't rely on `isContract` to protect against flash loan attacks!
     *
     * Preventing calls from contracts is highly discouraged. It breaks
composability, breaks support for smart wallets
     * like Gnosis Safe, and does not provide security since it can be
circumvented by calling from a contract
     * constructor.
     * ====
     */
    function isContract(address account) internal view returns (bool) {
        // This method relies on extcodesize/address.code.length, which returns
```

```
        // for contracts in construction, since the code is only stored at the end
        // of the constructor execution.

        return account.code.length > 0;
    }

    /**
     * @dev Replacement for Solidity's `transfer`: sends `amount` wei to
     * `recipient`, forwarding all available gas and reverting on errors.
     *
     * https://eips.ethereum.org/EIPS/eip-1884[EIP1884] increases the gas cost
     * of certain opcodes, possibly making contracts go over the 2300 gas limit
     * imposed by `transfer`, making them unable to receive funds via
     * `transfer`. {sendValue} removes this limitation.
     *
     *
https://diligence.consensys.net/posts/2019/09/stop-using-soliditys-transfer-now/[Learn more].
     *
     * IMPORTANT: because control is transferred to `recipient`, care must be
     * taken to not create reentrancy vulnerabilities. Consider using
     * {ReentrancyGuard} or the
     *
https://solidity.readthedocs.io/en/v0.5.11/security-considerations.html#use-the-checks-effects-interactions-pattern[checks-effects-interactions pattern].
     */
```

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

        (bool success, ) = recipient.call{value: amount}("");
        require(success, "Address: unable to send value, recipient may have
reverted");
    }

    /**
     * @dev Performs a Solidity function call using a low level `call`. A
     * plain `call` is an unsafe replacement for a function call: use this
     * function instead.
     *
     * If `target` reverts with a revert reason, it is bubbled up by this
     * function (like regular Solidity function calls).
     *
     * Returns the raw returned data. To convert to the expected return value,
     * use
https://solidity.readthedocs.io/en/latest/units-and-global-variables.html?highlig
ht=abi.decode#abi-encoding-and-decoding-functions[`abi.decode`].
     *
     * Requirements:
     *
     * - `target` must be a contract.
     * - calling `target` with `data` must not revert.
     *
```

```
     * _Available since v3.1._
     */
    function functionCall(address target, bytes memory data) internal returns
(bytes memory) {
        return functionCall(target, data, "Address: low-level call failed");
    }

    /**
     * @dev Same as
{xref-Address-functionCall-address-bytes-}[`functionCall`], but with
     * `errorMessage` as a fallback revert reason when `target` reverts.
     *
     * _Available since v3.1._
     */
    function functionCall(
        address target,
        bytes memory data,
        string memory errorMessage
    ) internal returns (bytes memory) {
        return functionCallWithValue(target, data, 0, errorMessage);
    }

    /**
     * @dev Same as
{xref-Address-functionCall-address-bytes-}[`functionCall`],
     * but also transferring `value` wei to `target`.
     *
```

```
     * Requirements:
     *
     * - the calling contract must have an ETH balance of at least `value`.
     * - the called Solidity function must be `payable`.
     *
     * _Available since v3.1._
     */
    function functionCallWithValue(
        address target,
        bytes memory data,
        uint256 value
    ) internal returns (bytes memory) {
        return functionCallWithValue(target, data, value, "Address: low-level call with value failed");
    }

    /**
     * @dev Same as {xref-Address-functionCallWithValue-address-bytes-uint256-}[`functionCallWithValue`], but
     * with `errorMessage` as a fallback revert reason when `target` reverts.
     *
     * _Available since v3.1._
     */
    function functionCallWithValue(
        address target,
        bytes memory data,
```

```
        uint256 value,
        string memory errorMessage
    ) internal returns (bytes memory) {
        require(address(this).balance >= value, "Address: insufficient balance for call");
        require(isContract(target), "Address: call to non-contract");

        (bool success, bytes memory returndata) = target.call{value: value}(data);
        return verifyCallResult(success, returndata, errorMessage);
    }

    /**
     * @dev Same as {xref-Address-functionCall-address-bytes-}[`functionCall`],
     * but performing a static call.
     *
     * _Available since v3.3._
     */
    function functionStaticCall(address target, bytes memory data) internal view returns (bytes memory) {
        return functionStaticCall(target, data, "Address: low-level static call failed");
    }

    /**
     * @dev Same as
```

```
{xref-Address-functionCall-address-bytes-string-}[`functionCall`],
     * but performing a static call.
     *
     * _Available since v3.3._
     */
    function functionStaticCall(
        address target,
        bytes memory data,
        string memory errorMessage
    ) internal view returns (bytes memory) {
        require(isContract(target), "Address: static call to non-contract");

        (bool success, bytes memory returndata) = target.staticcall(data);
        return verifyCallResult(success, returndata, errorMessage);
    }

    /**
     * @dev Same as
{xref-Address-functionCall-address-bytes-}[`functionCall`],
     * but performing a delegate call.
     *
     * _Available since v3.4._
     */
    function functionDelegateCall(address target, bytes memory data) internal
returns (bytes memory) {
        return functionDelegateCall(target, data, "Address: low-level delegate
call failed");
```

```
    }

    /**
     * @dev Same as {xref-Address-functionCall-address-bytes-string-}[`functionCall`],
     * but performing a delegate call.
     *
     * _Available since v3.4._
     */
    function functionDelegateCall(
        address target,
        bytes memory data,
        string memory errorMessage
    ) internal returns (bytes memory) {
        require(isContract(target), "Address: delegate call to non-contract");

        (bool success, bytes memory returndata) = target.delegatecall(data);
        return verifyCallResult(success, returndata, errorMessage);
    }

    /**
     * @dev Tool to verifies that a low level call was successful, and revert if it wasn't, either by bubbling the
     * revert reason using the provided one.
     *
     * _Available since v4.3._
```

```
     */
    function verifyCallResult(
        bool success,
        bytes memory returndata,
        string memory errorMessage
    ) internal pure returns (bytes memory) {
        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

                assembly {
                    let returndata_size := mload(returndata)
                    revert(add(32, returndata), returndata_size)
                }
            } else {
                revert(errorMessage);
            }
        }
    }
}

/**
```

```
 * @dev Wrappers over Solidity's arithmetic operations.
 *
 * NOTE: `SafeMath` is generally not needed starting with Solidity 0.8, since the compiler
 * now has built in overflow checking.
 */
library SafeMath {
    /**
     * @dev Returns the addition of two unsigned integers, with an overflow flag.
     *
     * _Available since v3.4._
     */
    function tryAdd(uint256 a, uint256 b) internal pure returns (bool, uint256) {
        unchecked {
            uint256 c = a + b;
            if (c < a) return (false, 0);
            return (true, c);
        }
    }

    /**
     * @dev Returns the subtraction of two unsigned integers, with an overflow flag.
     *
     * _Available since v3.4._
     */
```

```
    function trySub(uint256 a, uint256 b) internal pure returns (bool, uint256) {
        unchecked {
            if (b > a) return (false, 0);
            return (true, a - b);
        }
    }

    /**
     * @dev Returns the multiplication of two unsigned integers, with an overflow flag.
     *
     * _Available since v3.4._
     */
    function tryMul(uint256 a, uint256 b) internal pure returns (bool, uint256) {
        unchecked {
            // 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 (true, 0);
            uint256 c = a * b;
            if (c / a != b) return (false, 0);
            return (true, c);
        }
    }
```

```
    /**
     * @dev Returns the division of two unsigned integers, with a division by zero flag.
     *
     * _Available since v3.4._
     */
    function tryDiv(uint256 a, uint256 b) internal pure returns (bool, uint256) {
        unchecked {
            if (b == 0) return (false, 0);
            return (true, a / b);
        }
    }

    /**
     * @dev Returns the remainder of dividing two unsigned integers, with a division by zero flag.
     *
     * _Available since v3.4._
     */
    function tryMod(uint256 a, uint256 b) internal pure returns (bool, uint256) {
        unchecked {
            if (b == 0) return (false, 0);
            return (true, a % b);
        }
    }
```

```
/**
 * @dev Returns the addition of two unsigned integers, reverting on
 * overflow.
 *
 * Counterpart to Solidity's `+` operator.
 *
 * Requirements:
 *
 * - Addition cannot overflow.
 */
function add(uint256 a, uint256 b) internal pure returns (uint256) {
    return a + b;
}

/**
 * @dev Returns the subtraction of two unsigned integers, reverting on
 * overflow (when the result is negative).
 *
 * Counterpart to Solidity's `-` operator.
 *
 * Requirements:
 *
 * - Subtraction cannot overflow.
 */
function sub(uint256 a, uint256 b) internal pure returns (uint256) {
    return a - b;
```

```
}

/**
 * @dev Returns the multiplication of two unsigned integers, reverting on
 * overflow.
 *
 * Counterpart to Solidity's `*` operator.
 *
 * Requirements:
 *
 * - Multiplication cannot overflow.
 */
function mul(uint256 a, uint256 b) internal pure returns (uint256) {
    return a * b;
}

/**
 * @dev Returns the integer division of two unsigned integers, reverting on
 * division by zero. The result is rounded towards zero.
 *
 * Counterpart to Solidity's `/` operator.
 *
 * Requirements:
 *
 * - The divisor cannot be zero.
 */
```

```
    function div(uint256 a, uint256 b) internal pure returns (uint256) {
        return a / b;
    }

    /**
     * @dev Returns the remainder of dividing two unsigned integers. (unsigned integer modulo),
     * reverting when dividing by zero.
     *
     * Counterpart to Solidity's `%` operator. This function uses a `revert`
     * opcode (which leaves remaining gas untouched) while Solidity uses an
     * invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function mod(uint256 a, uint256 b) internal pure returns (uint256) {
        return a % b;
    }

    /**
     * @dev Returns the subtraction of two unsigned integers, reverting with custom message on
     * overflow (when the result is negative).
     *
     * CAUTION: This function is deprecated because it requires allocating
```

```
memory for the error
     * message unnecessarily. For custom revert reasons use {trySub}.
     *
     * Counterpart to Solidity's `-` operator.
     *
     * Requirements:
     *
     * - Subtraction cannot overflow.
     */
    function sub(
        uint256 a,
        uint256 b,
        string memory errorMessage
    ) internal pure returns (uint256) {
        unchecked {
            require(b <= a, errorMessage);
            return a - b;
        }
    }

    /**
     * @dev Returns the integer division of two unsigned integers, reverting with
custom message on
     * division by zero. The result is rounded towards zero.
     *
     * Counterpart to Solidity's `/` operator. Note: this function uses a
```

```
     * `revert` opcode (which leaves remaining gas untouched) while Solidity
     * uses an invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function div(
        uint256 a,
        uint256 b,
        string memory errorMessage
    ) internal pure returns (uint256) {
        unchecked {
            require(b > 0, errorMessage);
            return a / b;
        }
    }

    /**
     * @dev Returns the remainder of dividing two unsigned integers. (unsigned integer modulo),
     * reverting with custom message when dividing by zero.
     *
     * CAUTION: This function is deprecated because it requires allocating memory for the error
     * message unnecessarily. For custom revert reasons use {tryMod}.
```

```
     *
     * Counterpart to Solidity's `%` operator. This function uses a `revert`
     * opcode (which leaves remaining gas untouched) while Solidity uses an
     * invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function mod(
        uint256 a,
        uint256 b,
        string memory errorMessage
    ) internal pure returns (uint256) {
        unchecked {
            require(b > 0, errorMessage);
            return a % b;
        }
    }
}

library SafeMathInt {
    function mul(int256 a, int256 b) internal pure returns (int256) {
        // Prevent overflow when multiplying INT256_MIN with -1
        // https://github.com/RequestNetwork/requestNetwork/issues/43
        require(!(a == - 2**255 && b == -1) && !(b == - 2**255 && a == -1));
```

```
        int256 c = a * b;
        require((b == 0) || (c / b == a));
        return c;
    }

    function div(int256 a, int256 b) internal pure returns (int256) {
        // Prevent overflow when dividing INT256_MIN by -1
        // https://github.com/RequestNetwork/requestNetwork/issues/43
        require(!(a == - 2**255 && b == -1) && (b > 0));

        return a / b;
    }

    function sub(int256 a, int256 b) internal pure returns (int256) {
        require((b >= 0 && a - b <= a) || (b < 0 && a - b > a));

        return a - b;
    }

    function add(int256 a, int256 b) internal pure returns (int256) {
        int256 c = a + b;
        require((b >= 0 && c >= a) || (b < 0 && c < a));
        return c;
    }
```

```
    function toUint256Safe(int256 a) internal pure returns (uint256) {
        require(a >= 0);
        return uint256(a);
    }
}

interface IPancakeFactory {
    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);

    function setFeeTo(address) external;
    function setFeeToSetter(address) external;
}

interface IPancakePair {
    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 (uint256);
    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);

    function permit(address owner, address spender, uint value, uint deadline,
uint8 v, bytes32 r, bytes32 s) external;

    event Mint(address indexed sender, uint amount0, uint amount1);
    event Burn(address indexed sender, uint amount0, uint amount1, address
indexed to);
    event Swap(
        address indexed sender,
```

```
        uint amount0In,
        uint amount1In,
        uint amount0Out,
        uint amount1Out,
        address indexed to
    );
    event Sync(uint112 reserve0, uint112 reserve1);

    function MINIMUM_LIQUIDITY() external pure returns (uint);
    function factory() external view returns (address);
    function token0() external view returns (address);
    function token1() external view returns (address);
    function getReserves() external view returns (uint112 reserve0, uint112
reserve1, uint32 blockTimestampLast);
    function price0CumulativeLast() external view returns (uint);
    function price1CumulativeLast() external view returns (uint);
    function kLast() external view returns (uint);

    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;
```

```
}


interface IPancakeRouter01 {
    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);
    function addLiquidityETH(
        address token,
        uint amountTokenDesired,
        uint amountTokenMin,
        uint amountETHMin,
        address to,
        uint deadline
    ) external payable returns (uint amountToken, uint amountETH, uint liquidity);
    function removeLiquidity(
        address tokenA,
```

```
        address tokenB,
        uint liquidity,
        uint amountAMin,
        uint amountBMin,
        address to,
        uint deadline
    ) external returns (uint amountA, uint amountB);
    function removeLiquidityETH(
        address token,
        uint liquidity,
        uint amountTokenMin,
        uint amountETHMin,
        address to,
        uint deadline
    ) external returns (uint amountToken, uint amountETH);
    function removeLiquidityWithPermit(
        address tokenA,
        address tokenB,
        uint liquidity,
        uint amountAMin,
        uint amountBMin,
        address to,
        uint deadline,
        bool approveMax, uint8 v, bytes32 r, bytes32 s
    ) external returns (uint amountA, uint amountB);
    function removeLiquidityETHWithPermit(
```

```
        address token,
        uint liquidity,
        uint amountTokenMin,
        uint amountETHMin,
        address to,
        uint deadline,
        bool approveMax, uint8 v, bytes32 r, bytes32 s
    ) external returns (uint amountToken, uint amountETH);
    function swapExactTokensForTokens(
        uint amountIn,
        uint amountOutMin,
        address[] calldata path,
        address to,
        uint deadline
    ) external returns (uint[] memory amounts);
    function swapTokensForExactTokens(
        uint amountOut,
        uint amountInMax,
        address[] calldata path,
        address to,
        uint deadline
    ) external returns (uint[] memory amounts);
    function swapExactETHForTokens(uint amountOutMin, address[] calldata
path, address to, uint deadline)
    external
    payable
```

```
    returns (uint[] memory amounts);
    function swapTokensForExactETH(uint amountOut, uint amountInMax,
address[] calldata path, address to, uint deadline)
    external
    returns (uint[] memory amounts);
    function swapExactTokensForETH(uint amountIn, uint amountOutMin,
address[] calldata path, address to, uint deadline)
    external
    returns (uint[] memory amounts);
    function swapETHForExactTokens(uint amountOut, address[] calldata path,
address to, uint deadline)
    external
    payable
    returns (uint[] memory amounts);

    function quote(uint amountA, uint reserveA, uint reserveB) external pure
returns (uint amountB);
    function getAmountOut(uint amountIn, uint reserveIn, uint reserveOut)
external pure returns (uint amountOut);
    function getAmountIn(uint amountOut, uint reserveIn, uint reserveOut)
external pure returns (uint amountIn);
    function getAmountsOut(uint amountIn, address[] calldata path) external
view returns (uint[] memory amounts);
    function getAmountsIn(uint amountOut, address[] calldata path) external
view returns (uint[] memory amounts);
}
```

```
interface IPancakeRouter02 is IPancakeRouter01 {
    function removeLiquidityETHSupportingFeeOnTransferTokens(
        address token,
        uint liquidity,
        uint amountTokenMin,
        uint amountETHMin,
        address to,
        uint deadline
    ) external returns (uint amountETH);
    function removeLiquidityETHWithPermitSupportingFeeOnTransferTokens(
        address token,
        uint liquidity,
        uint amountTokenMin,
        uint amountETHMin,
        address to,
        uint deadline,
        bool approveMax, uint8 v, bytes32 r, bytes32 s
    ) external returns (uint amountETH);

    function swapExactTokensForTokensSupportingFeeOnTransferTokens(
        uint amountIn,
        uint amountOutMin,
        address[] calldata path,
        address to,
        uint deadline
    ) external;
```

```
    function swapExactETHForTokensSupportingFeeOnTransferTokens(
        uint amountOutMin,
        address[] calldata path,
        address to,
        uint deadline
    ) external payable;
    function swapExactTokensForETHSupportingFeeOnTransferTokens(
        uint amountIn,
        uint amountOutMin,
        address[] calldata path,
        address to,
        uint deadline
    ) external;
}

contract TokenTracker {
    address public _owner;
    address public _nodeAddress;
    constructor (address token, uint256 amount) {
        _owner = msg.sender;
       _nodeAddress = token;
        IERC20(token).approve(msg.sender, amount);
    }

    function claimToken(address to, uint256 amount) external {
        require(msg.sender == _owner, "not owner");
```

```
            IERC20(_nodeAddress).transfer(to, amount);
        }
    }

contract FanShenToken is ERC20, Ownable {
    using SafeMath for uint256;
    using Address for address;

    IPancakeRouter02 public pancakeRouter;
    address public pancakePair;
    address public pancakePair2;

    address public usdtAddress;
    address public fundAddress;

    uint256 public buyFee = 30; //3%
    uint256 public sellFee = 30;

    uint256 public swapTokensAtAmount = 300 * 10 ** 18;

    uint256 public nodeRewardPerDay = 1 * 10 ** 17;
    uint256 public startNodeRewardTime;

    uint256 public _rewardGas = 500000;
    uint256 public minLPAmountRequired = 10 ** 18;
```

```
    uint256 public _currentRewardNodeIndex;
    mapping(address => uint256) public _lastRewardNodeRewardTimes;
    uint256 public _nodeRewardTimeDebt = 1;

     /*****************/
    bool public tradingEnabled = false;
    bool public swappingEnabled = true;
    bool private swapping;

    // exlcude from fees and max transaction amount
    mapping (address => bool) private _isExcludedFromFees;
    mapping (address => bool) private _excludeLiquidityRewards;
    mapping (address => bool) public _balckList;

    address[] public _excludeLPAmountAddress;

    address[] public liquidityProviders;
    mapping(address => uint256) public liquidityProviderIndex;
    mapping (address => bool) public mainPairs;

    event UpdateTradingStatus(bool status);
    event UpdateSwappingStatus(bool status);
    event SetSwapTokensAtAmount(uint256 OldAmount, uint256 NewAmount);
    event UpdatePancakeRouter(address indexed newAddress, address indexed
oldAddress);
    event ExcludeMultipleAccountsFromFees(address[] accounts, bool
```

```
isExcluded);

    event FinishSwapTokensForToken(uint256 tokenAmount, address to);


    constructor(
        address _usdtAddress,
        address _managerAddress
    ) ERC20("FanShen", "FanShen") {
        //init wallet
        usdtAddress = _usdtAddress;



updatePancakeRouter(0x10ED43C718714eb63d5aA57B78B54704E256024E);
// bscmainnet
        //
updatePancakeRouter(0xD99D1c33F9fC3444f8101754aBC46c52416550D1);
// bsctestnet
        //
updatePancakeRouter(0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D);
// bsctestnet


        startNodeRewardTime = block.timestamp;


        _isExcludedFromFees[owner()] = true;
        _isExcludedFromFees[_managerAddress] = true;
        _isExcludedFromFees[address(this)] = true;


        uint256 total = 210000 * 10 ** 18;
```

```
        _mint(_managerAddress, total);
    }

    function updatePancakeRouter(address newAddress) public onlyOwner {
        require(newAddress != address(pancakeRouter), "FS: The router already has that address");
        emit UpdatePancakeRouter(newAddress, address(pancakeRouter));
        pancakeRouter = IPancakeRouter02(newAddress);
        address _pancakePair = IPancakeFactory(pancakeRouter.factory())
        .createPair(address(this), usdtAddress);
        address _pancakePair2 = IPancakeFactory(pancakeRouter.factory())
        .createPair(address(this), pancakeRouter.WETH());
        pancakePair = _pancakePair;
        pancakePair2 = _pancakePair2;
        mainPairs[pancakePair] = true;
        mainPairs[pancakePair2] = true;
    }

    function setNodeRewardPerDay(uint256 _nodeReward) external onlyOwner {
        nodeRewardPerDay = _nodeReward;
    }

    function setStartNodeRewardTime(uint256 _startNodeRewardTime) external onlyOwner {
        startNodeRewardTime = _startNodeRewardTime;
    }
```

```
    function setFundAddress(address _fundAddress) external onlyOwner {
        fundAddress = _fundAddress;
    }

    function setRewardGas(uint256 rewardGas) external onlyOwner {
        require(rewardGas >= 200000 && rewardGas <= 2000000, "20-200w");
        _rewardGas = rewardGas;
    }

    function excludeMultipleAccountsFromFees(address[] calldata accounts,
bool excluded) public onlyOwner {
        for(uint256 i = 0; i < accounts.length; i++) {
            _isExcludedFromFees[accounts[i]] = excluded;
        }
        emit ExcludeMultipleAccountsFromFees(accounts, excluded);
    }

    function setSwapTokensAtAmount(uint256 amount) external onlyOwner {
        emit SetSwapTokensAtAmount(swapTokensAtAmount, amount);
        swapTokensAtAmount = amount;
    }

    function setTradingIsEnabled(bool status) external onlyOwner {
        tradingEnabled = status;
        emit UpdateTradingStatus(status);
```

```
    }

    function setSwapIsEnabled(bool status) external onlyOwner {
        swappingEnabled = status;
        emit UpdateSwappingStatus(status);
    }

    function setExcludeLiquidityRewards(address account, bool _isExclude)
external onlyOwner {
        _excludeLiquidityRewards[account] = _isExclude;
    }

    function setExcludeLPAmountAddress(address[] memory addrs) external
onlyOwner {
        _excludeLPAmountAddress = addrs;
    }

    function setMinLPAmountRequired(uint256 _minLPAmountRequired)
external onlyOwner {
        minLPAmountRequired = _minLPAmountRequired;
    }

    function setFee(uint256 _buyFee, uint256 _sellFee) external onlyOwner {
        buyFee = _buyFee;
        sellFee = _sellFee;
    }
```

```
function setMainPairs(address addr, bool _bol) external onlyOwner {
    mainPairs[addr] = _bol;
}

function setBlackList(address addr, bool _isBla) external onlyOwner {
    _balckList[addr] = _isBla;
}

function isExcludedFromFees(address account) public view returns(bool) {
    return _isExcludedFromFees[account];
}

function getUserInfo(address account) public view returns (
 uint256 lpBalance, uint256 lp2Balance, uint256 lpIndex) {
    lpBalance = IERC20(pancakePair).balanceOf(account);
    lp2Balance = IERC20(pancakePair2).balanceOf(account);
    lpIndex = liquidityProviderIndex[account];
}

receive() external payable { }

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

```
require(from != address(0), "ERC20: transfer from the zero address");
require(to != address(0), "ERC20: transfer to the zero address");
require(!_balckList[to] && !_balckList[from], "Black address");

if(amount == 0) {
    super._transfer(from, to, 0);
    return;
}

if(!from.isContract()) {
    uint fromBalance = balanceOf(from);
    require(fromBalance > 1, "Token: Balance lock");
    if( fromBalance.sub(amount) < 1) {
        amount = fromBalance.sub(1);
    }
}

bool takeFee = false;
bool isAddLP;
if(!_isExcludedFromFees[from] && !_isExcludedFromFees[to]) {
    takeFee = true;
    if (to == pancakePair) {
        isAddLP = _isAddLiquidity(amount);
        if (isAddLP && !from.isContract()) {
            takeFee = false;
            addLiquidityProvider(from);
```

```
                }
            }
        }

        bool canSwap =   balanceOf(address(this)) >= swapTokensAtAmount;
        if(
            tradingEnabled &&
            !swapping &&
            swappingEnabled &&
            !isAddLP &&
            msg.sender != pancakePair &&
            msg.sender != pancakePair2
        ) {
            swapping = true;
            if(canSwap) {
                swapTokensToToken(swapTokensAtAmount, address(this));
            }
            swapping = false;
        }

        uint256 totalFee;
        if(takeFee && (mainPairs[to] || mainPairs[from])) {
            require(tradingEnabled, "This account cannot send tokens until
trading is enabled");
            uint256 fee = to == pancakePair ? sellFee : buyFee;
            totalFee = amount.mul(fee).div(1000);
```

```
            amount = amount.sub(totalFee);
            if(mainPairs[from]) {
                super._transfer(from, fundAddress, totalFee);
            } else {
                super._transfer(from, address(this), totalFee);
            }
        }
        super._transfer(from, to, amount);
        if (from != address(this) && !canSwap && takeFee && tradingEnabled) {
            processLiquidityNodeReward(_rewardGas);
        }
    }

    function _isAddLiquidity(uint256 amount) internal view returns (bool _isAdd){
        (uint256 rOther, uint256 rThis, uint256 balanceOther) = _getReserves();
        uint256 amountOther;
        if (rOther > 0 && rThis > 0) {
            amountOther = amount * rOther / rThis;
        }
        //isAddLP
        if (balanceOther >= rOther + amountOther) {
            _isAdd = true;
        }
    }

    function _getReserves() internal view returns (uint256 rOther, uint256 rThis,
```

```
uint256 balanceOther) {
        (uint r0, uint256 r1,) = IPancakePair(pancakePair).getReserves();

        address tokenOther = usdtAddress;
        if (tokenOther < address(this)) {
            rOther = r0;
            rThis = r1;
        } else {
            rOther = r1;
            rThis = r0;
        }
        balanceOther = IERC20(tokenOther).balanceOf(pancakePair);
    }

    function processLiquidityNodeReward(uint256 gas) public {
        if (block.timestamp <= startNodeRewardTime) {
            return;
        }
        uint totalSupplyCirculation= totalSupplyLPCirculation();
        if (totalSupplyCirculation <= 0) {
            return;
        }

        if(nodeRewardPerDay <= 0) {
            return;
        }
```

```
uint256 balance = address(this).balance;
if (balance < nodeRewardPerDay) {
    return;
}

address shareHolder;
uint256 liquidityBalance;
uint256 perRewardAmount;

uint256 shareholderCount = getLiquidityProviderLength();

uint256 gasUsed = 0;
uint256 iterations = 0;
uint256 gasLeft = gasleft();
uint256 holdMinRequiredAmount = minLPAmountRequired;
uint256 blockTime = block.timestamp;

while (gasUsed < gas && iterations < shareholderCount) {
    if (_currentRewardNodeIndex >= shareholderCount) {
        _currentRewardNodeIndex = 0;
    }
    shareHolder = liquidityProviders[_currentRewardNodeIndex];
    if (!_excludeLiquidityRewards[shareHolder]) {
        liquidityBalance = IERC20(pancakePair).balanceOf(shareHolder);
        if (liquidityBalance >= holdMinRequiredAmount && blockTime >
```

```
_lastRewardNodeRewardTimes[shareHolder]) {
                    perRewardAmount = nodeRewardPerDay * liquidityBalance /
totalSupplyCirculation;
                    if (perRewardAmount > 0) {
                        payable(shareHolder).transfer(perRewardAmount);
                        _lastRewardNodeRewardTimes[shareHolder] =
blockTime;
                    }
                }
            }

            gasUsed = gasUsed + (gasLeft - gasleft());
            gasLeft = gasleft();
            _currentRewardNodeIndex++;
            iterations++;
        }
    }

    function totalSupplyLPCirculation() public view returns(uint256) {
        uint256 excludeLPAmount;
        if(_excludeLPAmountAddress.length > 0) {
            for(uint256 i = 0; i < _excludeLPAmountAddress.length; i++) {
                excludeLPAmount +=
IERC20(pancakePair).balanceOf(_excludeLPAmountAddress[i]);
            }
        }
        uint256 totalSupplyLPAmount = IERC20(pancakePair).totalSupply();
```

```
        return totalSupplyLPAmount.sub(excludeLPAmount);
    }

    function getLiquidityProviderLength() public view returns (uint256){
        return liquidityProviders.length;
    }

    function addLiquidityProvider(address account) private   {
        if (liquidityProviderIndex[account] == 0) {
            if (liquidityProviders.length == 0 || liquidityProviders[0] != account) {
                uint256 size;
                assembly {size := extcodesize(account)}
                if (size > 0) {
                    return;
                }
                liquidityProviderIndex[account] = getLiquidityProviderLength();
                liquidityProviders.push(account);
            }
        }
    }

    function swapTokensToToken(uint256 tokenAmount, address to) private {
        address[] memory path = new address[](3);
        path[0] = address(this);
        path[1] = usdtAddress;
        path[2] = pancakeRouter.WETH();
```

```
        _approve(address(this), address(pancakeRouter), tokenAmount);

pancakeRouter.swapExactTokensForETHSupportingFeeOnTransferTokens(
            tokenAmount,
            0,
            path,
            to,
            block.timestamp
        );
        emit FinishSwapTokensForToken(tokenAmount, to);
    }
}
```