Coinsult

Advanced Manual Smart Contract Audit

Project: Sodatsu

Website: https://www.sokuswap.com/

● Low-Risk	● Medium-Risk	● High-Risk
4 low-risk code issues found	0 medium-risk code issues found	0 high-risk code issues found

Contract Address

0xed641273b0c9dd7bc89f0cd4c3bd58770b662d63

Disclaimer: Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

Disclaimer

Coinsult is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

Coinsult can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	Unicrypt : Token Vesting	17,000,000	76.5000%
2	0xfd73751077c2b1f871b7d12538b181e4eb80b156	4,914,420	22.1149%
3	0xff1b8770501a2ce0e0a2fc1ae3d0e13bf441ab1b	136,982.018564977420973407	0.6164%
4	0xa3ab0167a0ab940f16f633a7ef582879b7b14d0c	111,111	0.5000%
5	0xaa3d85ad9d128dfecb55424085754f6dfa643eb1	53,738.083291520321123934	0.2418%

Source Code

Coinsult was comissioned by Sodatsu to perform an audit based on the following smart contract:

https://etherscan.io/address/0xed641273b0c9dd7bc89f0cd4c3bd58770b662d63#code

Manual Code Review

In this audit report we will highlight all these issues:

🟢 Low-Risk

4 low-risk code issues found

🟡 Medium-Risk

0 medium-risk code issues found

🔴 High-Risk

0 high-risk code issues found

The detailed report continues on the next page...

🟢 **Low-Risk:** Could be fixed, will not bring problems.

Avoid relying on block.timestamp

block.timestamp can be manipulated by miners.

```
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
        address(0),
        block.timestamp
    );
}
```

Recommendation

Do not use `block.timestamp`, now or blockhash as a source of randomness

Exploit scenario

```
contract Game {

    uint reward_determining_number;

    function guessing() external{
      reward_determining_number = uint256(block.blockhash(10000)) % 10;
    }
}
```

Eve is a miner. Eve calls `guessing` and re-orders the block containing the transaction. As a result, Eve wins the game.

🟢 **Low-Risk:** Could be fixed, will not bring problems.

Too many digits

Literals with many digits are difficult to read and review.

```
function updateGasForProcessing(uint256 newValue) public onlyOwner {
    require(
        newValue &gt;= 200000 &amp;&amp; newValue &lt;= 500000,
        &quot;SODATSUTOKEN: gasForProcessing must be between 200,000 and 500,000&quot;
    );
    require(
        newValue != gasForProcessing,
        &quot;SODATSUTOKEN: Cannot update gasForProcessing to same value&quot;
    );
    emit GasForProcessingUpdated(newValue, gasForProcessing);
    gasForProcessing = newValue;
}
```

Recommendation

Use: Ether suffix, Time suffix, or The scientific notation

Exploit scenario

```
contract MyContract{
    uint 1_ether = 10000000000000000000;
}
```

While `1_ether` looks like `1 ether`, it is `10 ether`. As a result, it’s likely to be used incorrectly.

🟢 **Low-Risk:** Could be fixed, will not bring problems.

No zero address validation for some functions

Detect missing zero address validation.

```
function setMarketingWallet(address payable wallet) external onlyOwner {
    _marketingWalletAddress = wallet;
}
```

Recommendation

Check that the new address is not zero.

Exploit scenario

```
contract C {

  modifier onlyAdmin {
    if (msg.sender != owner) throw;
    _;
  }

  function updateOwner(address newOwner) onlyAdmin external {
    owner = newOwner;
  }
}
```

Bob calls `updateOwner` without specifying the `newOwner`, soBob loses ownership of the contract.

🟢 **Low-Risk:** Could be fixed, will not bring problems.

Missing events arithmetic

Detect missing events for critical arithmetic parameters.

```
function setMarketingWallet(address payable wallet) external onlyOwner {
    _marketingWalletAddress = wallet;
}
```

Recommendation

Emit an event for critical parameter changes.

Exploit scenario

```
contract C {

  modifier onlyAdmin {
    if (msg.sender != owner) throw;
    _;
  }

  function updateOwner(address newOwner) onlyAdmin external {
    owner = newOwner;
  }
}
```

`updateOwner()` has no event, so it is difficult to track off-chain changes in the buy price.

Owner privileges

- 🟢 Owner cannot set fees higher than 25%
- 🟢 Owner cannot pause trading
- 🟢 Owner cannot change max transaction amount
- 🟡 Owner can exclude from fees

⚠️ Owner can exclude addresses from dividend
⚠️ Owner can disable antibot
⚠️ Owner can update claimwait (between 1 and 24 hours)
⚠️ Owner can update minimum token balance to be eligible for dividends

Extra notes by the team

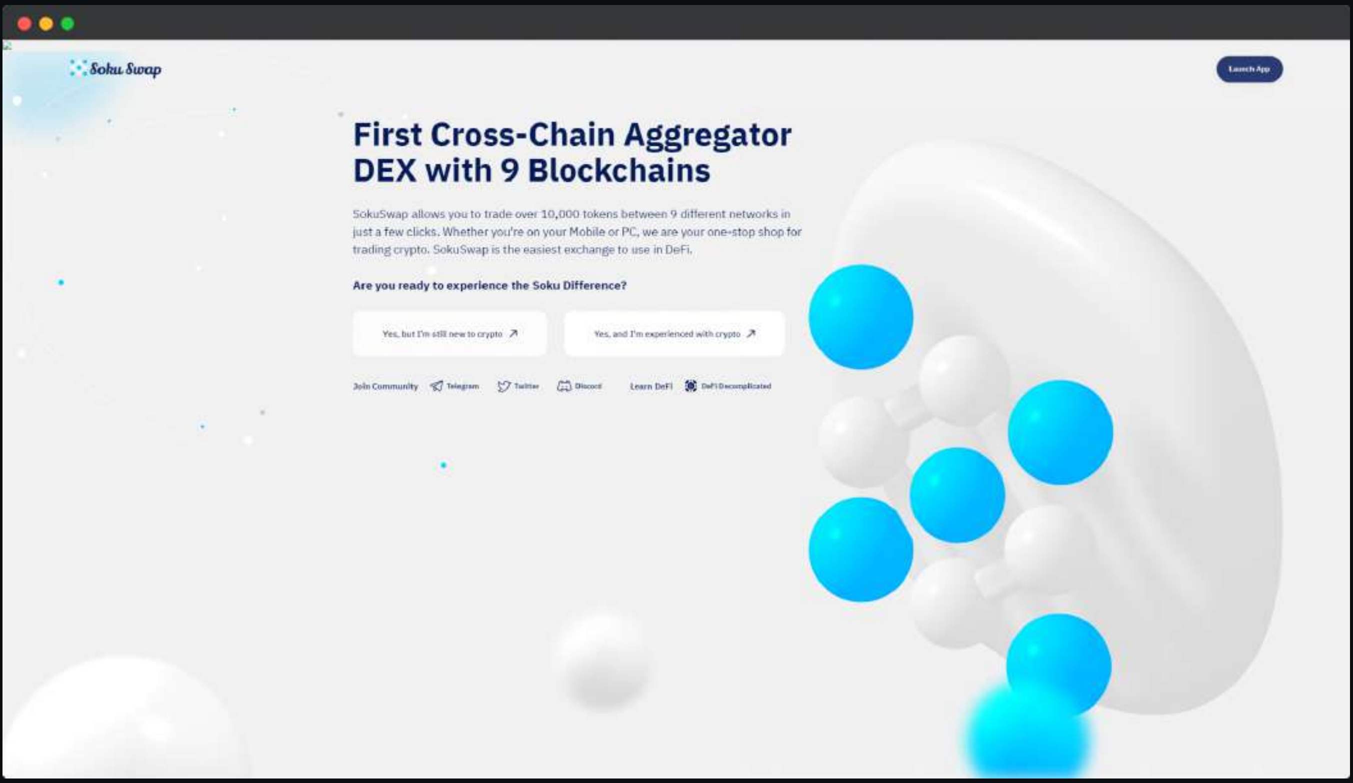
No notes

Contract Snapshot

```
contract Sodatsu_Token is ERC20, Ownable, BaseToken {
using SafeMath for uint256;

uint256 public constant VERSION = 1;

IUniswapV2Router02 public uniswapV2Router;
address public uniswapV2Pair;

bool private swapping;

SODATSUTOKENDividendTracker public dividendTracker;

address public rewardToken;

uint256 public swapTokensAtAmount;

uint256 public tokenRewardsFee;
uint256 public liquidityFee;
uint256 public marketingFee;
uint256 public totalFees;
```

Website Review

Coinsult checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.



First Cross-Chain Aggregator DEX with 9 Blockchains

SokuSwap allows you to trade over 10,000 tokens between 9 different networks in just a few clicks. Whether you're on your Mobile or PC, we are your one-stop shop for trading crypto. SokuSwap is the easiest exchange to use in DeFi.

Are you ready to experience the Soku Difference?

Yes, but I'm still new to crypto ↗
Yes, and I'm experienced with crypto ↗
Join Community
Telegram
Twitter
Discord
Learn DeFi
DeFi Decomplicated

- ● Mobile Friendly
- ● Does not contain jQuery errors
- ● SSL Secured
- ● No major spelling errors

Project Overview

● Not KYC verified by Coinsult

Sodatsu

Audited by Coinsult.net

Date: 21 August 2022

✓ Advanced Manual Smart Contract Audit