soken

SMART CONTRACT
SECURITY AUDIT

Goldario

November, 2021

Website: soken.io

Table of Contents

Disclaimer

This is a comprehensive report based on our automated and manual examination of cybersecurity vulnerabilities and framework flaws. We took into consideration smart contract based algorithms, as well. Reading the full analysis report is essential to build your understanding of project's security level. It is crucial to take note, though we have done our best to perform this analysis and report, that you should not rely on the our research and cannot claim what it states or how we created it. Before making any judgments, you have to conduct your own independent research. We will discuss this in more depth in the following disclaimer - please read it fully.

DISCLAIMER: You agree to the terms of this disclaimer by reading this report or any portion thereof. Please stop reading this report and remove and delete any copies of this report that you download and/or print if you do not agree to these conditions. This report is for non-reliability information only and does not represent investment advice. No one shall be entitled to depend on the report or its contents, and Soken and its affiliates shall not be held responsible to you or anyone else, nor shall Soken provide any guarantee or representation to any person with regard to the accuracy or integrity of the report. Without any terms, warranties or other conditions other than as set forth in that exclusion and Soken excludes hereby all representations, warrants, conditions and other terms (including, without limitation, guarantees implied by the law of satisfactory quality, fitness for purposes and the use of reasonable care and skills). The report is provided as "as is" and does not contain any terms and conditions. Except as legally banned, Soken disclaims all responsibility and responsibilities and no claim against Soken is made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic loses or losses) that may be caused by you or any other person, or any damages or damages, including without limitations (whether innocent or negligent).

Security analysis is based only on the smart contracts. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Our analysis contains following steps:

1. Project Analysis;

2. Manual analysis of smart contracts:
- Deploying smart contracts on any of the network(Ropsten/Rinkeby) using Remix IDE
- Hashes of all transaction will be recorded
- Behaviour of functions and gas consumption is noted, as well.

3. Unit Testing:
- Smart contract functions will be unit tested on multiple parameters and under multiple conditions to ensure that all paths of functions are functioning as intended.
- In this phase intended behaviour of smart contract is verified.
- In this phase, we would also ensure that smart contract functions are not consuming unnecessary gas.
- Gas limits of functions will be verified in this stage.

4. Automated Testing:
- Mythril
- Oyente
- Manticore
- Solgraph

Terminology

We categorize the finding into 4 categories based on their vulnerability:

- Low-severity issue — less important, must be analyzed
- Medium-severity issue — important, needs to be analyzed and fixed
- High-severity issue —important, might cause vulnerabilities, must be analyzed and fixed
- Critical-severity issue —serious bug causes, must be analyzed and fixed.

Limitations

The security audit of Smart Contract cannot cover all vulnerabilities. Even if no vulnerabilities are detected in the audit, there is no guarantee that future smart contracts are safe. Smart contracts are in most cases safeguarded against specific sorts of attacks. In order to find as many flaws as possible, we carried out a comprehensive smart contract audit. Audit is a document that is not legally binding and guarantees nothing.

Token Contract Details for 25.11.2021

Contract Name: **Goldario**

Deployed address: **0x6EF7E2D571f9806ab8FAAB73a76A97442BF78e3b**

Total Supply: **110,000,000**

Token Tracker: **GLD**

Decimals: **18**

Token holders: **3,739**

Transactions count: **5,251**

Top 100 holders dominance: **35.05%**

Audit Details

Project Name: **Goldario**

Language: **Solidity**

Compiler Version: **v0.8.7**

Blockchain: **BSC**

Social Profiles

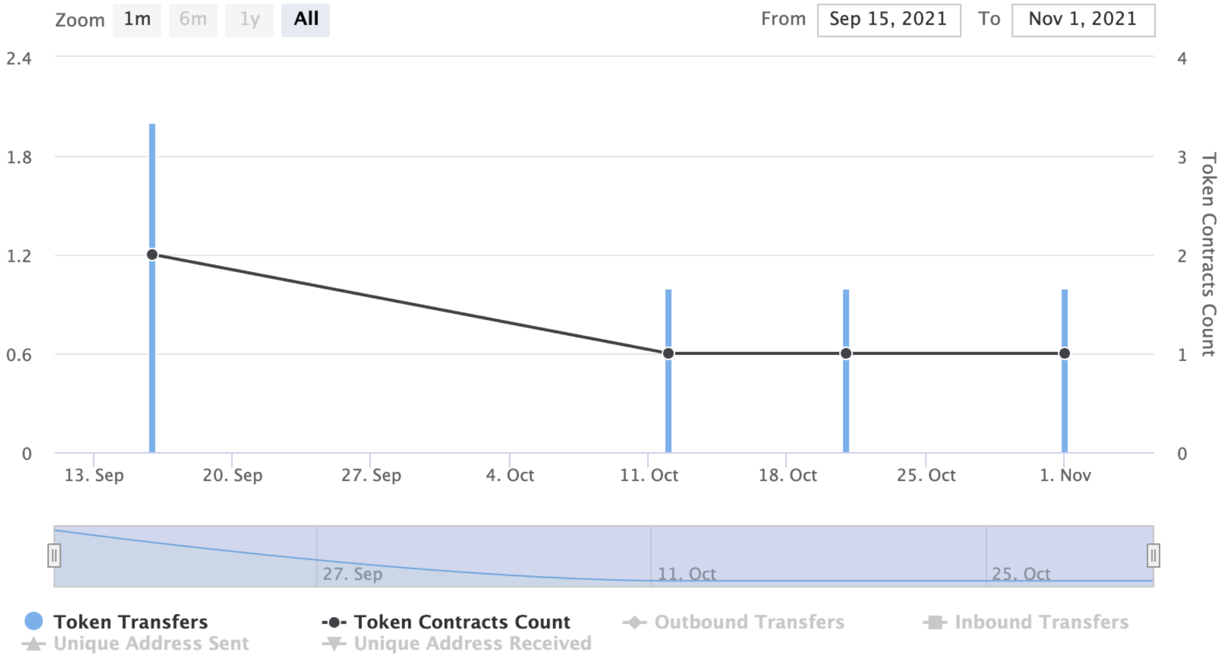
Project Website: **https://www.goldario.com/**

Project Twitter: **https://twitter.com/GoldarioToken/**

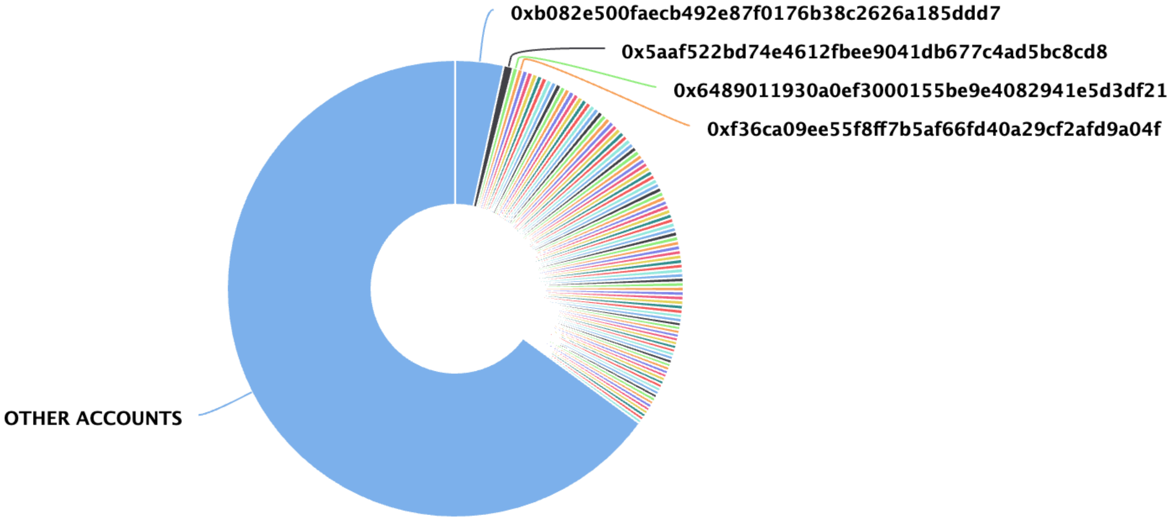
Project Telegram Group: **https://t.me/GoldarioOfficial**

Project Medium: **https://medium.com/@GoldarioToken**

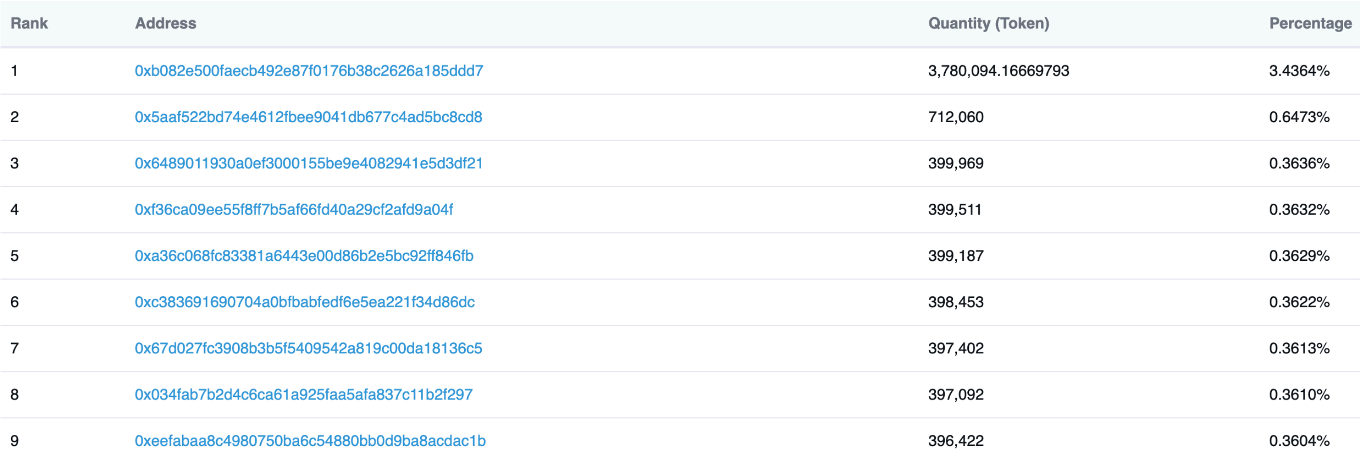
Token Analytics



GLD Token Distribution



GLD Top Holders



Rank	Address	Quantity (Token)	Percentage
1	0xb082e500faecb492e87f0176b38c2626a185ddd7	3,780,094.16669793	3.4364%
2	0x5aaf522bd74e4612fbee9041db677c4ad5bc8cd8	712,060	0.6473%
3	0x6489011930a0ef3000155be9e4082941e5d3df21	399,969	0.3636%
4	0xf36ca09ee55f8ff7b5af66fd40a29cf2afd9a04f	399,511	0.3632%
5	0xa36c068fc83381a6443e00d86b2e5bc92ff846fb	399,187	0.3629%
6	0xc383691690704a0bfbabfedf6e5ea221f34d86dc	398,453	0.3622%
7	0x67d027fc3908b3b5f5409542a819c00da18136c5	397,402	0.3613%
8	0x034fab7b2d4c6ca61a925faa5afa837c11b2f297	397,092	0.3610%
9	0xeefabaa8c4980750ba6c54880bb0d9ba8acdac1b	396,422	0.3604%

Swap Analysis

✔ Token is sellable (not a honeypot)

✔ Buy fee is less than 10% (0%)

✔ Sell fee is less than 10% (0%)

Contract Analysis

✔ Verified contract source

✔ No prior similar token contracts

✔ Source does not contain a proxy contract

✘ Source does not contain a pausable contract

✘ Ownership renounced or source does not contain an owner contract.

✔ Creator/Owner wallet contains less than 5% of token supply (0.46%)

✔ All other holders possess less than 10% of token supply

✘ Adequate liquidity present (<0.01 BNB)

Contract Function Details

+ Counters.sol
- [Int] current
- [Int] increment
- [Int] decrement
- [Int] reset

+ ECDSA.sol
- [Prv] _throwError
- [Int] tryRecover
- [Int] recover
- [Int] tryRecover
- [Int] recover
- [Int] tryRecover
- [Int] recover
- [Int] toEthSignedMessageHash
- [Int] toTypedDataHash
- [Int] _domainSeparatorV4
- [Prv] _buildDomainSeparator
- [Int] _hashTypedDataV4
- [Int] _msgSender
- [Int] _msgData

+ [Int] IERC20.sol
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom

+ [Int] IERC20Metadata is IERC20.sol
- [Ext] name
- [Ext] symbol
- [Ext] decimals

+ [Int] IERC20Permit.sol
- [Ext] permit
- [Ext] nonces
- [Ext] DOMAIN_SEPARATOR
- [Pub] paused
- [Int] _pause
- [Int] _unpause

+ ERC20 is Context, IERC20, IERC20Metadata
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transferBurnRate
- [Pub] enableFee
- [Pub] transfer
- [Pub] allowance
- [Pub] approve
- [Pub] transferFrom
- [Pub] increaseAllowance
- [Pub] decreaseAllowance
- [Int] _transfer
- [Int] _mint
- [Int] _burn
- [Int] _approve
- [Int] _beforeTokenTransfer
- [Int] _afterTokenTransfer
- [Pub] burnFrom
- [Pub] permit
- [Pub] nonces
- [Pub] _useNonce
- [Pub] owner
- [Pub] renounceOwnership
- [Pub] transferOwnership
- [Prv] _setOwner

+ ECDSA.sol
- [Pub] pause
- [Pub] unpause
- [Int] _beforeTokenTransfer

Vulnerabilities checking

Issue Description	Checking Status
Compiler Errors	Completed
Delays in Data Delivery	Completed
Re-entrancy	Completed
Transaction-Ordering Dependence	Completed
Timestamp Dependence	Completed
Shadowing State Variables	Completed
DoS with Failed Call	Completed
DoS with Block Gas Limit	Completed
Outdated Complier Version	Completed
Assert Violation	Completed
Use of Deprecated Solidity Functions	Completed
Integer Overflow and Underflow	Completed
Function Default Visibility	Completed
Malicious Event Log	Completed
Math Accuracy	Completed
Design Logic	Completed
Fallback Function Security	Completed
Cross-function Race Conditions	Completed
Safe Zeppelin Module	Completed

Security Issues

1) Ownership privileges:

The contract contains ownership functionality and ownership is not renounced which allows the creator or current owner to modify contract behavior (for example, disable selling or mint new tokens).

Conclusion

Low-severity issues exist within smart contracts. Smart contracts are free from any critical or high-severity issues.

NOTE: Please check the disclaimer above and note, that audit makes no statements or warranties on business model, investment attractiveness or code sustainability.

Soken Contact Info

Website: www.soken.io

Mob: (+1)416-875-4174

32 Britain Street, Toronto, Ontario, Canada

Telegram: @team_soken

GitHub: sokenteam

Twitter: @soken_team