soken

SMART CONTRACT SECURITY AUDIT

OmniaVerse (BLOCK Contract)

Scan and check this report was posted at Soken Github

August, 2022

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.

Basic Security Recommendation

Unlike hardware and paper wallets, hot wallets are connected to the internet and store private keys online, which exposes them to greater risk. If a company or an individual holds significant amounts of cryptocurrency in a hot wallet, they should consider using MultiSig addresses. Wallet security is enhanced when private keys are stored in different locations and are not controlled by a single entity.

More info: **https://medium.com/coinmonks/guide-to-using-the-gnosis-multisig-wallet-eth-e76979741162**

Token Contract Details for 16.08.2022

Contract Name: **BlockVerse**

Deployed address: **0xF130A35b721f3c03C09cEE402A3731349A4b503E**

Total Supply: **1,000,000,000**

Token Tracker: **BLOCK**

Decimals: **8**

Token holders: **785**

Transactions count: **2440**

Top 100 holders dominance: **97.56%**

Audit Details

Project Name: **OmniaVerse**

Language: **Solidity**

Compiler Version: **v0.6.12**

Blockchain: **BSC**

Social Profiles

Project Website: **https://omniaverse.io/**

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

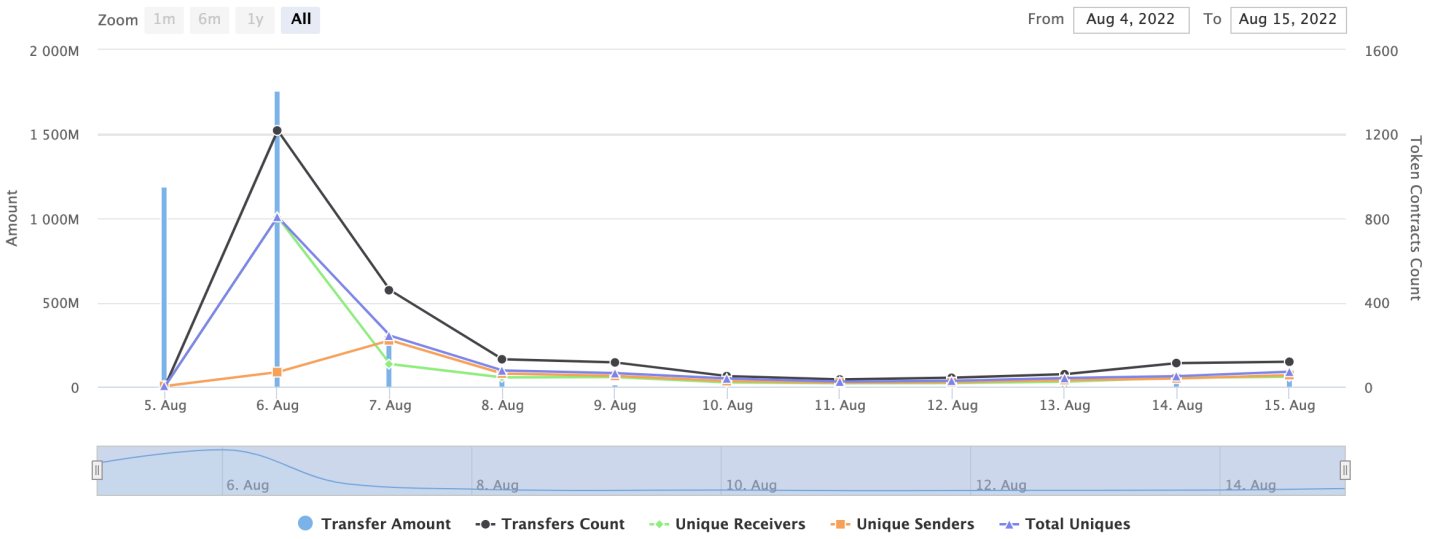
Project Telegram: **https://t.me/omniaverseOfficial**

Project Reddit: **https://www.reddit.com/r/omniaverseOfficial/**

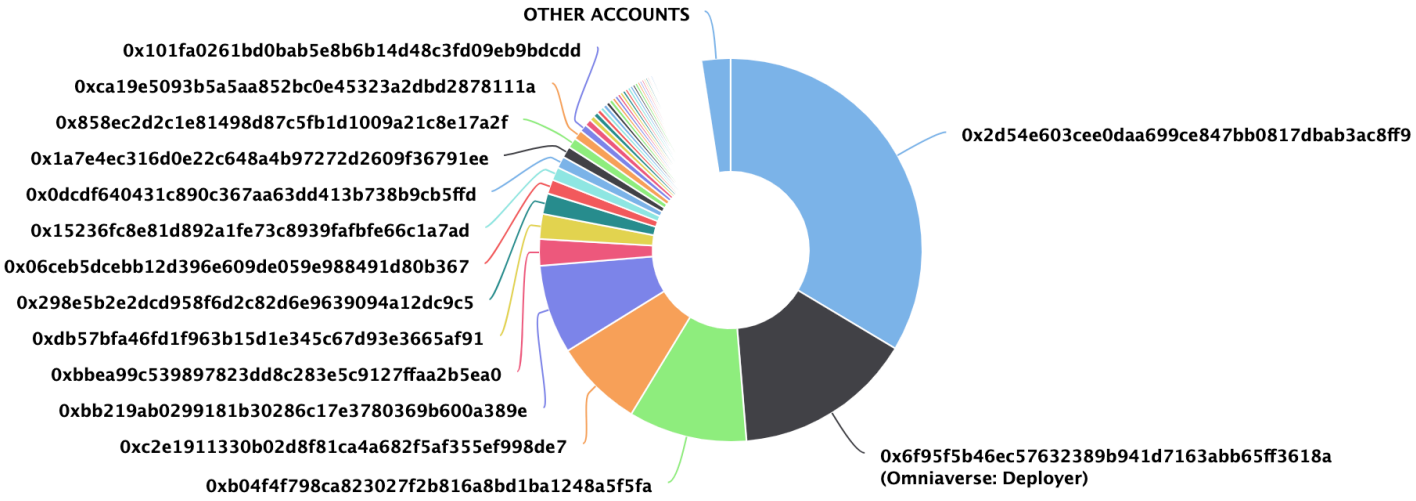
Project Medium: **https://medium.com/@Omniaverse**

Project Youtube: **https://www.youtube.com/watch?v=VSjaJXcn_Aw**

Token Analytics



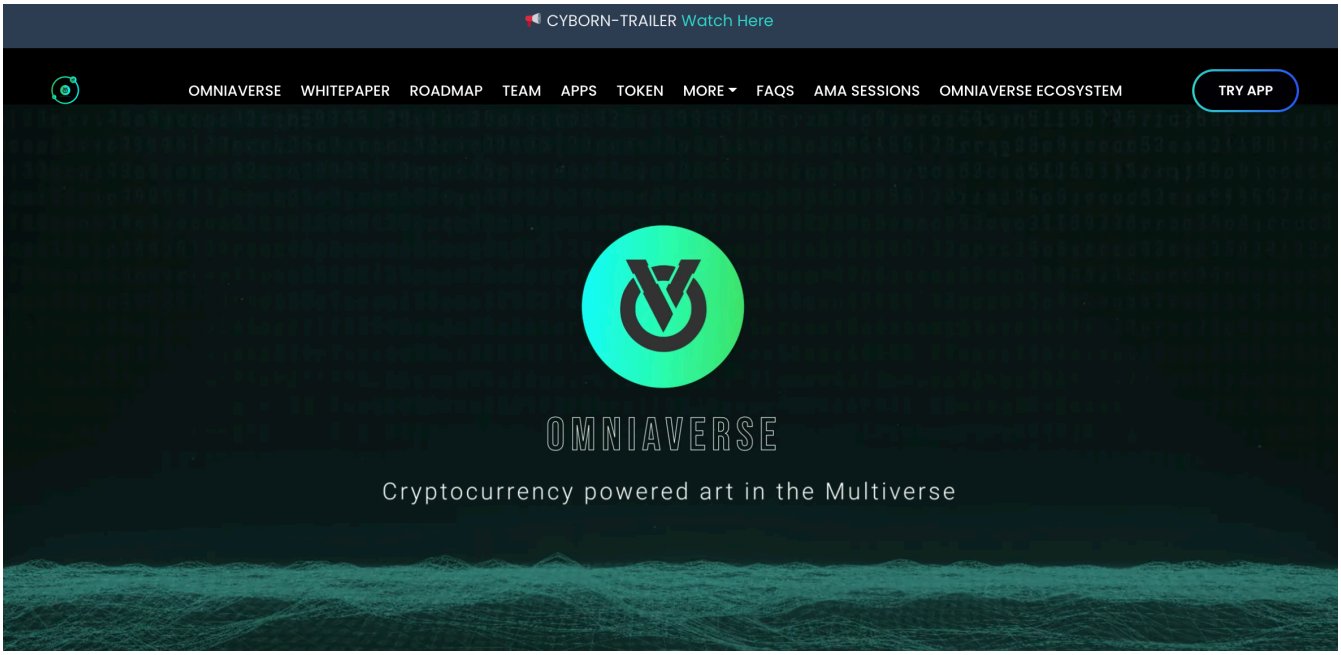
BLOCK Token Distribution



BLOCK Top 10 Holders

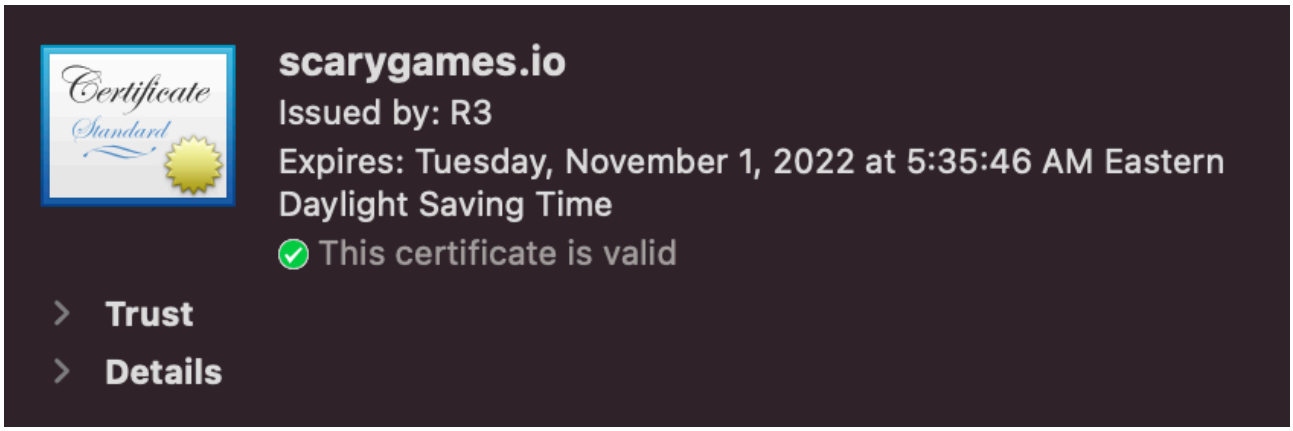
Rank	Address	Quantity (Token)	Percentage
1	0x2d54e603cee0daa699ce847bb0817dbab3ac8ff9	335,800,471	33.5800%
2	Omniaverse: Deployer	151,190,858.5	15.1191%
3	0xb04f4f798ca823027f2b816a8bd1ba1248a5f5fa	100,000,000	10.0000%
4	0xc2e1911330b02d8f81ca4a682f5af355ef998de7	75,000,804	7.5001%
5	0xbb219ab0299181b30286c17e3780369b600a389e	75,000,000	7.5000%
6	0xbbea99c539897823dd8c283e5c9127ffaa2b5ea0	22,256,756.2856389	2.2257%
7	0xdb57bfa46fd1f963b15d1e345c67d93e3665af91	21,030,612.49904442	2.1031%
8	0x298e5b2e2dcd958f6d2c82d6e9639094a12dc9c5	17,486,951.45324566	1.7487%
9	0x06ceb5dcebb12d396e609de059e988491d80b367	12,050,024.44	1.2050%
10	0x15236fc8e81d892a1fe73c8939fafbfe66c1a7ad	11,000,000.03806204	1.1000%

Project Website Overview



✓JavaScript errors hasn't been found.
✓Malware pop-up windows hasn't been detected.
✓No issues with loading elements, code, or stylesheets.

Project Website SSL Certification



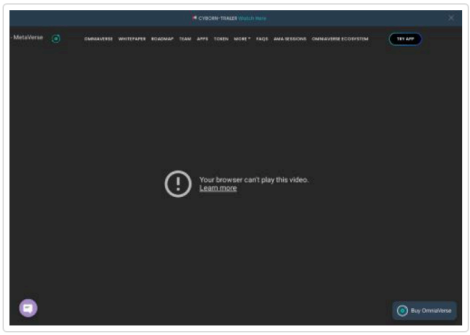
Project Website Optimization for Desktop

70

Performance

Values are approximate and subject to change. The performance level is calculated directly from these metrics. Show calculator

▲ 0–49 ■ 50–89 ● 90–100



DICATORS Expand

- First Contentful Paint 1.4 sec.
- Time to Interactive 5.6 sec.
- Speed Index 4.7 sec.
- Total Blocking Time 200ms
- Largest Contentful Paint 1.4 sec.
- Cumulative Layout Shift 0.025

Project Website Optimization for Mobile

19

Performance

Values are approximate and subject to change. The performance level is calculated directly from these metrics. Show calculator

▲ 0–49 ■ 50–89 ● 90–100

INDICATORS

- First Contentful Paint 4.5 sec.
- Time to Interactive 40.6 sec.
- Speed Index 16.3 sec.
- Total Blocking Time 1980 ms
- Largest Contentful Paint 41.4 sec.
- Cumulative Layout Shift 0.051

Whitepaper of the project

The whitepaper of OmniaVerse project has been verified on behalf of Soken team.

Whitepaper link: **https://omniaverse.io/wp-content/uploads/2022/06/omniaverse.pdf**

Contract Function Details

- [Int] _msgSender
- [Int] _msgData
- [Pub] owner
- [Pub] renounceOwnership
- [Pub] transferOwnership
- [Int] _transferOwnership
- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom
- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod
- [Int] min
- [Int] sqrt
- [Int] isContract
- [Int] sendValue
- [Int] functionCall
- [Int] functionCall
- [Int] functionCallWithValue
- [Int] functionCallWithValue
- [Prv] _functionCallWithValue
- [Ext] getOwner
- [Pub] name
- [Pub] decimals
- [Pub] symbol
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer
- [Pub] allowance
- [Pub] approve
- [Pub] transferFrom

- [Pub] increaseAllowance
- [Pub] decreaseAllowance
- [Pub] burn
- [Int] _transfer
- [Int] _mint
- [Int] _burn
- [Int] _approve
- [Int] _burnFrom
- [Int] safeTransfer
- [Int] safeTransferFrom
- [Int] safeApprove
- [Int] safeIncreaseAllowance
- [Int] safeDecreaseAllowance
- [Prv] _callOptionalReturn
- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] allowance
- [Ext] approve
- [Ext] transfer
- [Ext] transferFrom
- [Ext] DOMAIN_SEPARATOR
- [Ext] PERMIT_TYPEHASH
- [Ext] nonces
- [Ext] permit
- [Ext] MINIMUM_LIQUIDITY
- [Ext] factory
- [Ext] token0
- [Ext] token1
- [Ext] getReserves
- [Ext] price0CumulativeLast
- [Ext] price1CumulativeLast
- [Ext] kLast
- [Ext] swapFee
- [Ext] mint
- [Ext] burn
- [Ext] swap
- [Ext] skim
- [Ext] sync
- [Ext] initialize
- [Ext] setSwapFee
- [Ext] feeTo
- [Ext] feeToSetter

- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair
- [Ext] setFeeTo
- [Ext] setFeeToSetter
- [Ext] setSwapFee
- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidity
- [Ext] addLiquidityETH
- [Ext] removeLiquidity
- [Ext] removeLiquidityETH
- [Ext] removeLiquidityWithPermit
- [Ext] removeLiquidityETHWithPermit
- [Ext] swapExactTokensForTokens
- [Ext] swapTokensForExactTokens
- [Ext] swapExactETHForTokens
- [Ext] swapTokensForExactETH
- [Ext] swapExactTokensForETH
- [Ext] swapETHForExactTokens
- [Ext] quote
- [Ext] getAmountOut
- [Ext] getAmountIn
- [Ext] getAmountsOut
- [Ext] getAmountsIn
- [Ext] removeLiquidityETHSupportingFeeOnTransferTokens
- [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens
- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens
- [Pub] updateSwapAndLiquifiy
- [Ext] setDevMarketingFee
- [Ext] setfundFee
- [Ext] setLiquidityFee
- [Ext] updateShares
- [Pub] updateSphynxSwapRouter
- [Pub] excludeFromFees
- [Pub] setFeeAccount
- [Pub] excludeMultipleAccountsFromFees
- [Pub] setAutomatedMarketMakerPair
- [Prv] _setAutomatedMarketMakerPair
- [Pub] setNativeAmountToSwap
- [Pub] updateDevMarketingWallet
- [Ext] updateLiquidityWallet

- [Pub] updateFundWallet
- [Pub] setBlockNumber
- [Pub] updateMaxTxAmount
- [Pub] isExcludedFromFees
- [Int] _transfer
- [Prv] swapTokens
- [Prv] addLiquidity
- [Prv] swapTokensForNative
- [Prv] sphynxBuyBackAndBurn
- [Int] _getTokenAmountFromNative
- [Prv] transferNativeToDevMarketingWallet
- [Prv] transferNativeToFundWallet
- [Prv] transferNativeToSphynxWallet

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) Volatile Code:

The return values of functions *swapExactTokensForETHSupportingFeeOnTransferTokens* and *addLiquidityETH* are not properly handled.

Recommendation:

We recommend using variables to receive the return value of the functions mentioned above and handle both success and failure cases if needed by the business logic.

2) Integer Overflow / Underflow

```
1587          sphynxSwapRouter.swapExactETHForTokensSupportingFeeOnTransferTokens{value: nativeAmount}(
1588              0,
1589              path,
1590              address(this),
1591              block.timestamp + 120
1592          );
```

An overflow/underflow happens when an arithmetic operation reaches the maximum or minimum storage of a variable type. Integers overflow or underflow may prove fatal when during an arithmetic operation, the number goes over or under the designated limit. This may prove fatal during calculations related to ether or tokens.

Recommendation:

Solidity compiler versions >=0.8.0 automatically handle overflow and underflow validations. If you're using a lower solidity version, it is

recommended to use the SafeMath library to protect the arithmetic operations.

3) Owner Privileges

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

Conclusion

Low and medium-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