soken

SMART CONTRACT
SECURITY AUDIT

xto8

Scan and check this report
was posted at Soken Github

October, 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 04.10.2022

Contract Name: **INFINITY_XRC20**

Deployed address: **0x1a8731065A334cD60658b04FE4B4455Bf5f5eF1B**

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

Token Tracker: **INFINITY**

Decimals: **8**

Audit Details

Project Name: **xto8**

Language: **Solidity**

Compiler Version: **v0.5.17**

Blockchain: **BSC**

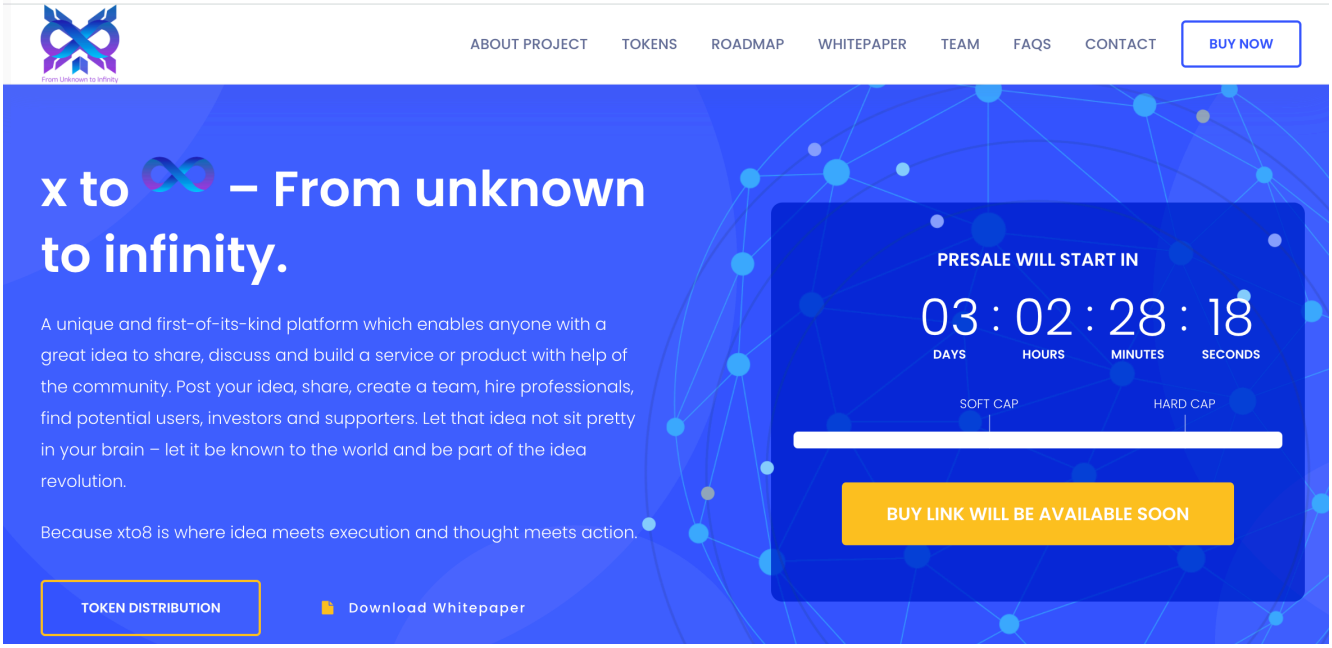
Social Profiles

Project Website: **https://xto8.io/**

Project Twitter: **https://twitter.com/FromXto8**

Project Telegram: **https://t.me/FromXto8**

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

Issued To

Common Name (CN)	xto8.io
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Go Daddy Secure Certificate Authority - G2
Organization (O)	GoDaddy.com, Inc.
Organizational Unit (OU)	http://certs.godaddy.com/repository/

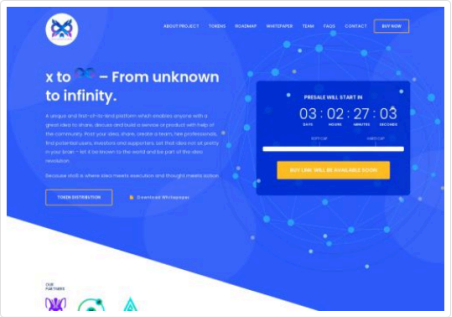
Project Website Optimization for Desktop

88

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 Expand

- First Contentful Paint 0.9 sec.
- Time to Interactive 1.2 sec.
- Speed Index 1.6 sec.
- Total Blocking Time 0 ms
- Largest Contentful Paint 2.0 sec.
- Cumulative Layout Shift 0.006

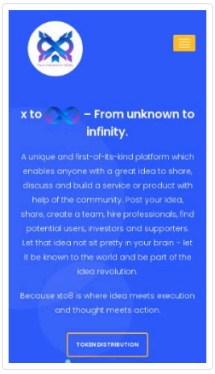
Project Website Optimization for Mobile

55

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 7.0 sec.
- Speed Index 6.0 sec.
- Total Blocking Time 90ms
- Largest Contentful Paint 8.9 sec.
- Cumulative Layout Shift 0.109

Whitepaper of the project

The whitepaper of xto8 project has been verified on behalf of Soken team.

What is xto8?

xto8, or "X to Infinity" is a platform for discussing and collaborating on ideas which have real life utilities. Often times, a person with a revolutionary idea is not able to take it to the next level because of many missing pieces of the puzzle.

And the fact is, there are no direct means available to find the missing pieces. For a given idea, there are hundreds of thousands with required skills, similar interests, answers to the critical questions, reviewers, potential users of the product and investors – but they are not connected. And xto8 strives to bridge that big disconnect.

No potential idea should be left unexecuted.
No cool concept should stay away from the light of the day just because one doesn't know what's next for turning it into a service or a product.

Whitepaper link: **https://xto8.io/whitepaper/**

Contract Function Details

- [Ext] setAdmin
- [Int] _transfer
- [Ext] deduct
- [Ext] transfer
- [Pub] transferFrom
- [Pub] approve
- [Pub] burn
- [Pub] burnFrom

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) Outdated compiler version: Low-severity

Using an outdated compiler version can be problematic especially if there are publicly disclosed bugs and issues that affect the current compiler version. The following outdated versions were detected: contract.sol - >=0.4.23 <0.6.0

Recommendation:

It is recommended to use a recent version of the Solidity compiler that should not be the most recent version, and it should not be an outdated version as well. Using very old versions of Solidity prevents the benefits of bug fixes and newer security checks. Consider using the solidity version 0.8.7, which patches most solidity vulnerabilities.

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