soken

SMART CONTRACT SECURITY AUDIT

NFTencer

Scan and check this report was posted at Soken Github

February, 2023

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 of the project's smart contract.

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. Scan and verify report's presence in the GitHub repository by a qr-code at the title page. 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://blog.soken.io/how-to-gnosis-multisig-46b1386ba8e5**

Token Contract Details for 27.02.2023

Deployed address: **0x64b682aE14F40cAB8733840cCAC400BAA3B3306e**

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

Token Tracker: **NFTC**

Decimals: **18**

Token holders: **120**

Transactions count: **201**

Audit Details

Language: **Solidity**

Compiler Version: **v0.8.0**

Blockchain: **BSC**

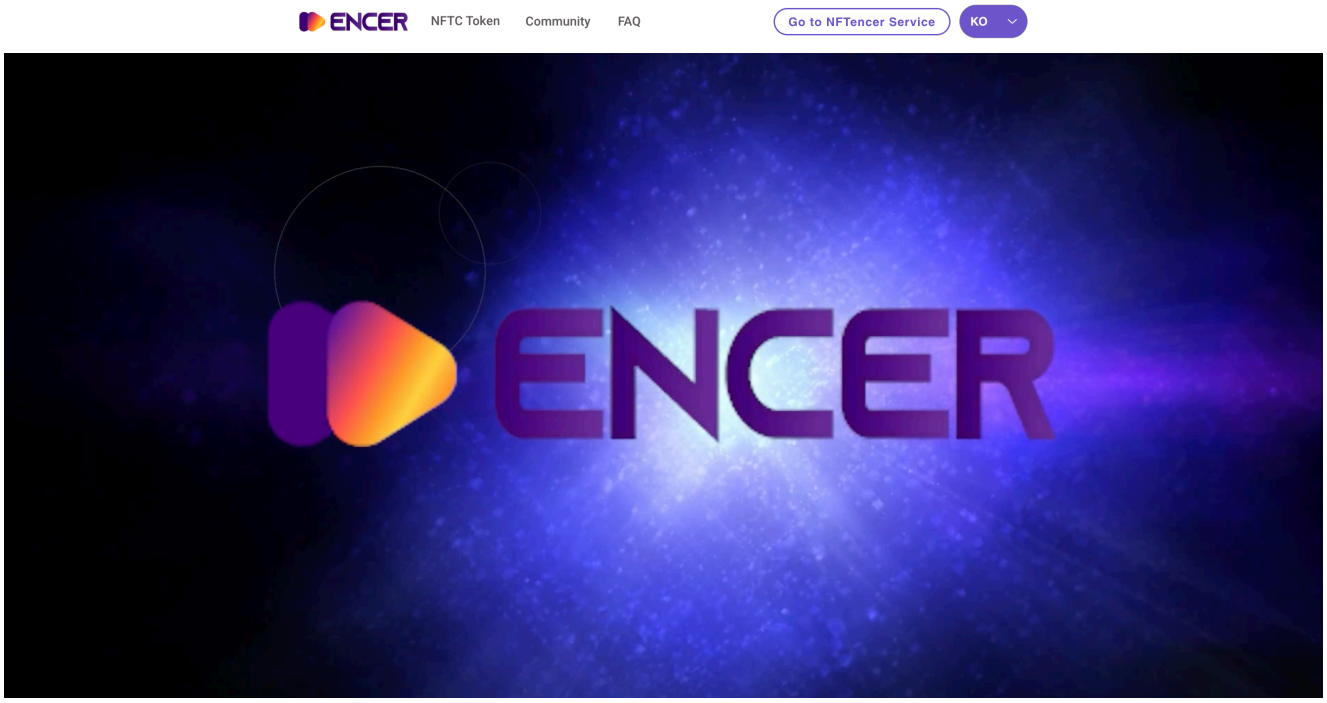
Social Profiles

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

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

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

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)	fwclegends.games
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	R3
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

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) USE OF FLOATING PRAGMA: Informational. Line #2

Solidity source files indicate the versions of the compiler they can be compiled with using a pragma directive at the top of the solidity file. This can either be a floating pragma or a specific compiler version. The contract was found to be using a floating pragma which is not considered safe as it can be compiled with all the versions described. The following affected files were found to be using floating pragma: / NFTC Source code (2).sol - ^0.8.0

Conclusion for project owner

Informational issues exist within smart contracts.

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

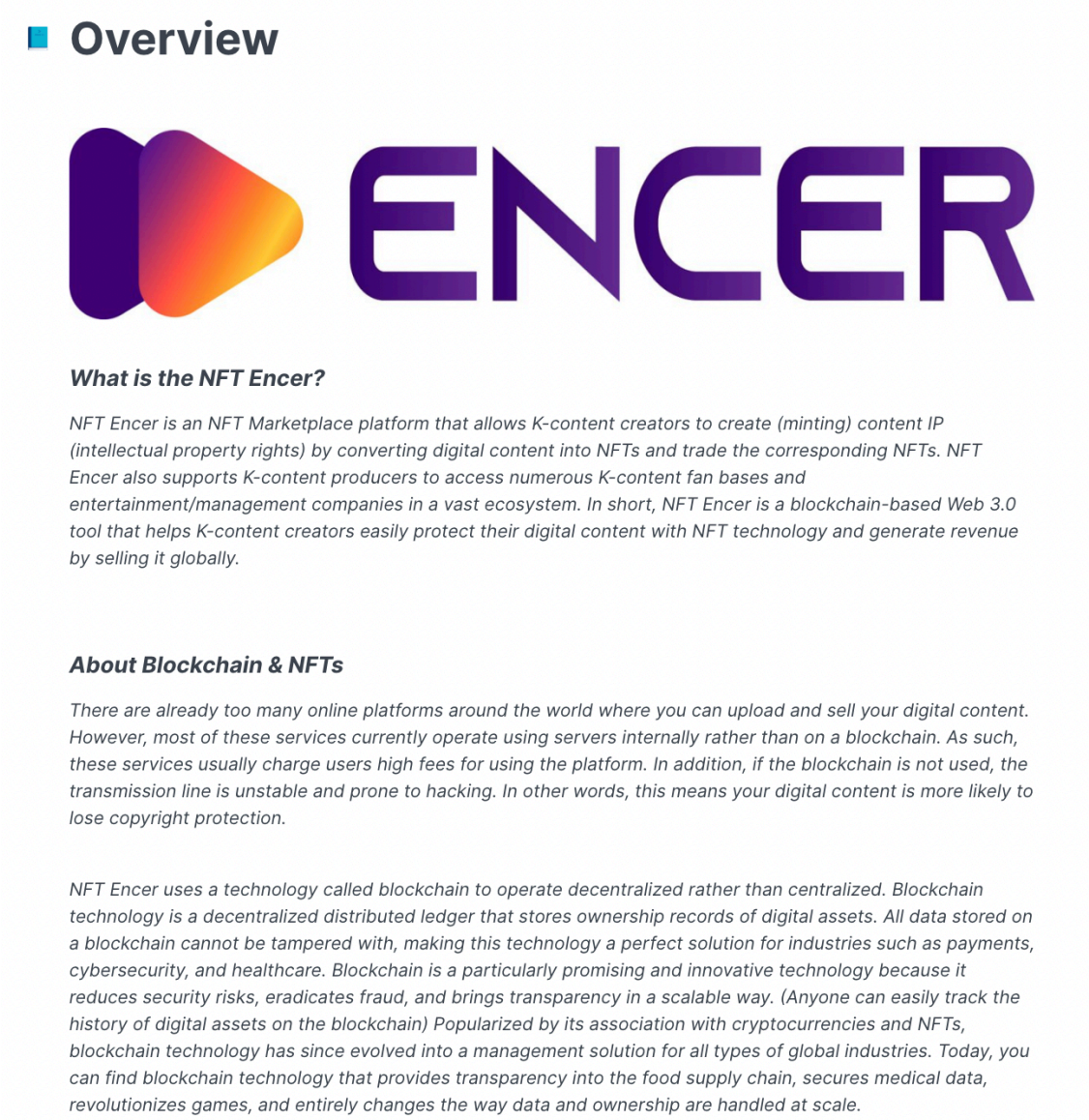
SECURITY REPORT
FOR COMMUNITY

NFTencer

soken

Whitepaper of the project

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



Overview

ENCER

What is the NFT Encer?

NFT Encer is an NFT Marketplace platform that allows K-content creators to create (minting) content IP (intellectual property rights) by converting digital content into NFTs and trade the corresponding NFTs. NFT Encer also supports K-content producers to access numerous K-content fan bases and entertainment/management companies in a vast ecosystem. In short, NFT Encer is a blockchain-based Web 3.0 tool that helps K-content creators easily protect their digital content with NFT technology and generate revenue by selling it globally.

About Blockchain & NFTs

There are already too many online platforms around the world where you can upload and sell your digital content. However, most of these services currently operate using servers internally rather than on a blockchain. As such, these services usually charge users high fees for using the platform. In addition, if the blockchain is not used, the transmission line is unstable and prone to hacking. In other words, this means your digital content is more likely to lose copyright protection.

NFT Encer uses a technology called blockchain to operate decentralized rather than centralized. Blockchain technology is a decentralized distributed ledger that stores ownership records of digital assets. All data stored on a blockchain cannot be tampered with, making this technology a perfect solution for industries such as payments, cybersecurity, and healthcare. Blockchain is a particularly promising and innovative technology because it reduces security risks, eradicates fraud, and brings transparency in a scalable way. (Anyone can easily track the history of digital assets on the blockchain) Popularized by its association with cryptocurrencies and NFTs, blockchain technology has since evolved into a management solution for all types of global industries. Today, you can find blockchain technology that provides transparency into the food supply chain, secures medical data, revolutionizes games, and entirely changes the way data and ownership are handled at scale.

Whitepaper link: **https://undefined-281.gitbook.io/nft-encer-whitepaper/nft-encer-2.0/overview**

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