QuillAudits

Audit Report
January, 2024

For

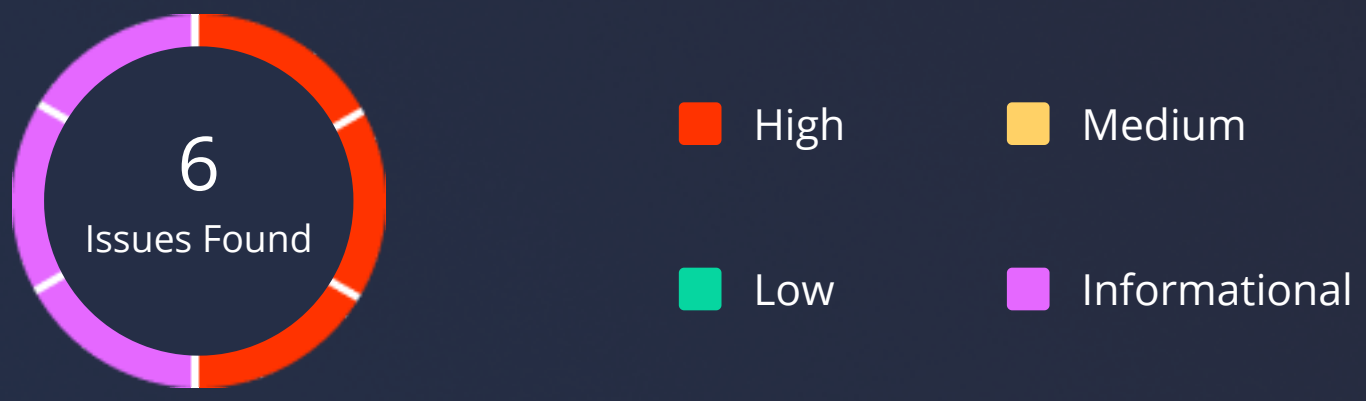
ASC

Table of Content

Executive Summary

Project Name	cNGN
Overview	The Consortium eNaira (cNGN) smart contract is an ERC-20-compliant decentralized application deployed on the Ethereum blockchain. Leveraging OpenZeppelin Contracts, it provides essential features such as pausability, blacklisting, minting, burning, and ownership controls. The contract ensures the security and integrity of the cNGN stablecoin, which acts as a pioneering use case for the CBN eNaira. With a focus on blockchain's potential as an alternative global payment rail, the cNGN contract aligns with the rising trend of blockchain adoption by governments and Fortune 500 companies.
Timeline	2nd January 2024 - 4th January 2024
Updated Code Received	8th January 2024
Second Review	8th January 2024
Method	Manual Review, Functional Testing, Automated Testing, etc. All the raised flags were manually reviewed and re-tested to identify any false positives.
Audit Scope	The scope of this audit was to analyze the cNGN code for quality, security, and correctness.
Source Code	*https://github.com/asc-africa/stablecoin/blob/4540e09589613071042 65e0fdc4dd4449adbe614/contracts/cngn.sol*
Branch	Main
Fixed In	*397ff4f*

Number of Security Issues per Severity



	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	0	0	0	1
Partially Resolved Issues	0	0	0	0
Resolved Issues	3	0	0	2

Checked Vulnerabilities

- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level

Techniques and Methods

Throughout the audit of smart contracts, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behavior.
- Token distribution and calculations are as per the intended behavior mentioned in the whitepaper.
- Implementation of ERC-20 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods, and tools were used to review all the smart contracts.

Structural Analysis

In this step, we have analyzed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

Static Analysis

A static Analysis of Smart Contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

Code Review / Manual Analysis

Manual Analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analyzed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption

In this step, we have checked the behavior of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

Tools and Platforms used for Audit

Hardhat, Foundry.

Types of Severity

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

High Severity Issues

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

Low Severity Issues

Low-level severity issues can cause minor impact and are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational

These are four severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

These are the issues identified in the initial audit and have been successfully fixed.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/impact of the security issue, but are not completely resolved.

High Severity Issues

1. Blacklisted address is allowed to transfer tokens if allowance>0

Path

https://github.com/asc-africa/stablecoin/blob/169aaecf4309a54022a9f05403645eb3614c0511/contracts/cngn.sol#L114

Function

transferFrom()

Description

If a blacklisted function has allowance to transfer tokens of non-blacklisted address then it can transfer it using transferFrom function.

Recommendation

Include a check to see if msg.sender is not blacklisted.

Status

Resolved

2. Any non-blacklisted address can transfer tokens to a blacklisted address

Path

https://github.com/asc-africa/stablecoin/blob/169aaecf4309a54022a9f05403645eb3614c0511/contracts/cngn.sol#L97

https://github.com/asc-africa/stablecoin/blob/169aaecf4309a54022a9f05403645eb3614c0511/contracts/cngn.sol#L114

Function

transfer(), transferFrom()

Description

Any non-blacklisted address can send tokens to a blacklisted address.

Recommendation

Include a check to see if **to** address is not blacklisted.

Status

Resolved

3. The owner might mistakenly mint tokens to blacklisted address

Path

https://github.com/asc-africa/stablecoin/blob/169aaecf4309a54022a9f05403645eb3614c0511/contracts/cngn.sol#L139

Function

mint()

Description

The mint function does not check if the address passed is blacklisted or not. The owner might mistakenly pass a blacklisted address to it.

Recommendation

Include a check to see if **_mintTo** address is not blacklisted.

Status

Resolved

Informational Issues

4. Experimental ABIEncoderV2 is deprecated

Path

https://github.com/asc-africa/stablecoin/blob/4540e09589613071042 65e0fdc4dd4449adbe614/contracts/cngn.sol#L5

Description

Compiler version 0.8.0 and above support ABIEncoderV2 by default and experimental ABIEncoderV2 is deprecated. **Doc**

Recommendation

Remove pragma experimental ABIEncoderV2;

Status

Resolved

5. Use the latest compiler version

Path

https://github.com/asc-africa/stablecoin/blob/4540e09589613071042 65e0fdc4dd4449adbe614/contracts/cngn.sol#L4

Description

Use the latest solidity compiler instead of 0.8.4 to avoid any security issues.

Recommendation

Replace 0.8.4 with 0.8.23

Status

Acknowledged

6. Unused Reentrancy contract import

Path

https://github.com/asc-africa/stablecoin/blob/4540e09589613071042 65e0fdc4dd4449adbe614/contracts/cngn.sol#L11

Description

Reentrancy guard is imported but not used anywhere, so it will just consume gas on deployment.

Recommendation

Remove the reentrancy guard from the contract as it is not required, as no external call is being made in the contract.

Status

Resolved

Automated Tests

No major issues were found. Some false positive errors were reported by the tools. All the other issues have been categorized above according to their level of severity.

Closing Summary

In this report, we have considered the security of the cNGN Token Contract. We performed our audit according to the procedure described above.

Some issues of Medium, Low and informational severity were found, Some suggestions and best practices are also provided in order to improve the code quality and security posture.

Disclaimer

QuillAudits Smart contract security audit provides services to help identify and mitigate potential security risks in cNGN smart contracts. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of cNGN smart contracts. One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your smart contracts for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of the cNGN to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks.

About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem.

850+
Audits Completed

$30B
Secured

$30B
Lines of Code Audited

Follow Our Journey

Audit Report
January, 2024

For

ASC

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com

audits@quillhash.com