



# Source Code Review

Prepared for Doc.Ai • August 2017

v1.0

## 1. Table of Contents

[1. Table of Contents](#)

[2. Executive Summary](#)

[3. Introduction](#)

[4. Summary Of Findings](#)

[5. Disclaimer](#)

## 2. Executive Summary

In August 2017, [doc.ai](#) engaged **Coinspect** to perform a security audit of the NRNToken.sol, the SaleTracker smart contracts, and several other contracts from the [OpenZeppelin](#) library, sent to us in a private tgz archive on August 22th 2017. The objective of the the audit was to evaluate the security of the ERC20 token and the sale contract implementation. During the assessment, Coinspect identified 0 high-risk issues, 0 medium-risk issues, and 0 low-risk issues.

## 3. Introduction

The contract NRNToken is an ERC20-compliant contract based on OpenZeppelin StandardToken, which uses SafeMath methods to prevent overflows. The token contract assigns all pre-sale tokens to the contract creator.

The contract SaleTracker is a contract to track sales, assumed to be related to the NRN token. This contract differs from other standard contracts by the fact that it does not generate any tokens on-the-fly associated with the received buy orders. All tokens are generated by a manual method that is not specified in the received contracts. Also the SaleTracker does not sets a cap nor a limit date for the sell, but however it allows the contract owner to pause sells at any time.

A whitebox security audit was conducted on these two contracts. The present report was completed on August 23th by Coinspect and includes results from the audit.

The SHA256 hashes of the contracts reviewed are the following:

SHA256 hash of file NRNToken.sol:

4da9a280e9f2dd30864fd67691ad10567af8688d3c577b16f93253b9a59a10ed

SHA256 hash of file SaleTracker.sol:

4bc9af14e41214e29a8c2623cf20931bfa9329176ecf2f31dd7bec484536c488

## 4. Summary Of Findings

No vulnerabilities were found.

## 5. Disclaimer

The present security audit is limited to smart contract code. It does not cover the technologies and designs related to these smart contracts, nor the frameworks and wallets that communicate with the contracts, nor the general operational security of the company behind this project. This document should not be read as investment advice or an offering of tokens.