verichains

SECURITY AUDIT OF

OCTAN SOULBOUND TOKEN

Public Report

Mar 17, 2023

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Ethereum	An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications.
Ether (ETH)	A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network.
Smart contract	A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
Solidity	A contract-oriented, high-level language for implementing smart contracts for the Ethereum platform.
Solc	A compiler for Solidity.
ERC721	The ERC-721 introduces a standard for NFT, in other words, this type of Token is unique and can have different value than another Token from the same Smart Contract, maybe due to its age, rarity or even something else like its visual

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Mar 17, 2023. We would like to thank the Octan Network for trusting Verichains Lab in auditing smart contracts. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the Octan SoulBound Token. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team had identified no vulnerable issues in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Octan SoulBound Token

In the rapidly growing world of Web3, building trustworthy identities and managing personal data across multiple chains and Dapps are challenges.

Octan tackles it by developing Octan 1ID & SBT, innovations that aim to provide a secure and reliable solution to the Web3 identity and fragmented data management problems.

Octan Soulbound Token (Octan SBT) are a type of soulbound token proposed by Vitalik Buterin, designed and implemented by Octan Labs to enhance the concept of Web3 identity by measuring user reputation, behavior and contributions.

The SBT, which is connected with 1ID, is a critical feature of the Octan Network. Each SBT includes Wallet Reputation Score and Category Reputation Score. While Wallet Reputation Score is automatically updated on a periodic basis, users can pay a small token fee to update Category RS.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the Octan SoulBound Token.

The latest version of the following files were made available in the course of the review:

SHA256 Sum	File
ca7ef6c4b8cd8d4ae2fe1bd3dedcc59b	Management.sol
523e3f327aebbfcbd4a2fc0a289f5e3e	Reputation.sol
8d57bd494fde62116587b9de61c7a6d9	Service.sol
5636591fdcd56b733809becd569867ca	Attribute.sol
091c033c7b9ae8f703e6327298a11a5b	Helper.sol
9c663b11e1f37b9d485c0a65242cd812	Helper.sol
fd5cb092a5fd5ff940dcdf8e621deb3a	Helper.sol
90e7675b913fb4c5c4f6ccb0c93897ca	SoulBound.sol
f9591965a65985375e0079c988492f1e	SoulBoundMintable.sol

1.3. Audit methodology

Our security audit process for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using public and RK87, our in-house smart contract security analysis tool.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that were considered during the audit of the smart contract:

- Integer Overflow and Underflow
- Timestamp Dependence
- Race Conditions
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert
- DoS with Block Gas Limit
- Gas Usage, Gas Limit and Loops
- Redundant fallback function
- Unsafe type Inference
- Reentrancy
- Explicit visibility of functions state variables (external, internal, private and public)
- Logic Flaws

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the contract functioning; creates a critical risk to the contract; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the contract with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 1. Severity levels

1.4. Disclaimer

Please note that security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a 100% secure smart contract. However, auditing allows discovering vulnerabilities that were unobserved, overlooked during development and areas where additional security measures are necessary.

2. AUDIT RESULT

2.1. Overview

The Octan SoulBound Token was written in `Solidity` language, with the required version to be `^0.8.0`. The source code was written based on OpenZeppelin's library.

The Octan SoulBound Token have some main external functions such as:

- `issue()`: Allows the user to mint a new token and the previous owner of a revoked token to mint it again.
- `revoke()`: Allows user to remove their ownership from a token.
- `change()`: Allows user to change token ownership, but only if the target address is either an unassigned address or a previously assigned one to that token.

Note: All of above functions can only be called by user when their message has an authorized signature that was signed by `AUTHORIZER_ROLE`.

2.1.1. Management.sol

The functions are restricted based on the roles of the caller, and only the accounts with the necessary roles can execute specific functions.

The contract defines five different roles:

- `DEFAULT_ADMIN_ROLE`: Manages governance settings, has the authority to change treasury address.
- `MANAGER_ROLE`: Has the authority to do special tasks such as settings.
- `MINTER_ROLE`: Has an authority to issue/burn SoulBound tokens.
- `OPERATOR_ROLE`: Grant a special privilege to add attribute of a specific SoulBound token and update reputation score.
- `AUTHORIZER_ROLE`: Has an authority to sign and to provide authorized signatures.

The contract includes a mapping of blacklisted and whitelisted accounts. The `MANAGER_ROLE` can pause/unpause the contract, and add/remove accounts from the blacklist/whitelist using the `addToList()` function.

2.1.2. Reputation.sol

This is a smart contract for managing reputation scores of SoulBound profiles. It extends the SoulBoundMintable contract and imports several other contracts such as `Attribute.sol` and `IManagement.sol`.

2.1.3. Service.sol

This contract allow a user to request the update of reputation scores for a list of soulboundIds or a single soulboundId with a specified attributeId via `generalRequest()` and `categoryRequest()` function.

The `MANAGER_ROLE` can set new values for the management contract address, fee, and delay time, respectively.

2.1.4. Minter.sol

Minter contract is a part of a Reputation-based system. It allows users to create, revoke and change ownership of SoulBound token.

The contract has three main functions: issue, revoke, and change. These functions allow the user issue, revoke and change the ownership of SoulBound token when user's message was authorized signature.

Ownership of a SoulBound token can be changed when `to` address is either an unassigned address or a previously assigned address to this SoulBound.

`setPayment()` is only called by `MANAGER_ROLE`.

From `Minter.sol` users can interact with internal function in `SoulBound.sol` and `SoulBoundMintable.sol`.

2.2. Findings

During the audit process, the audit team had identified no vulnerable issues in the smart contracts code.

APPENDIX

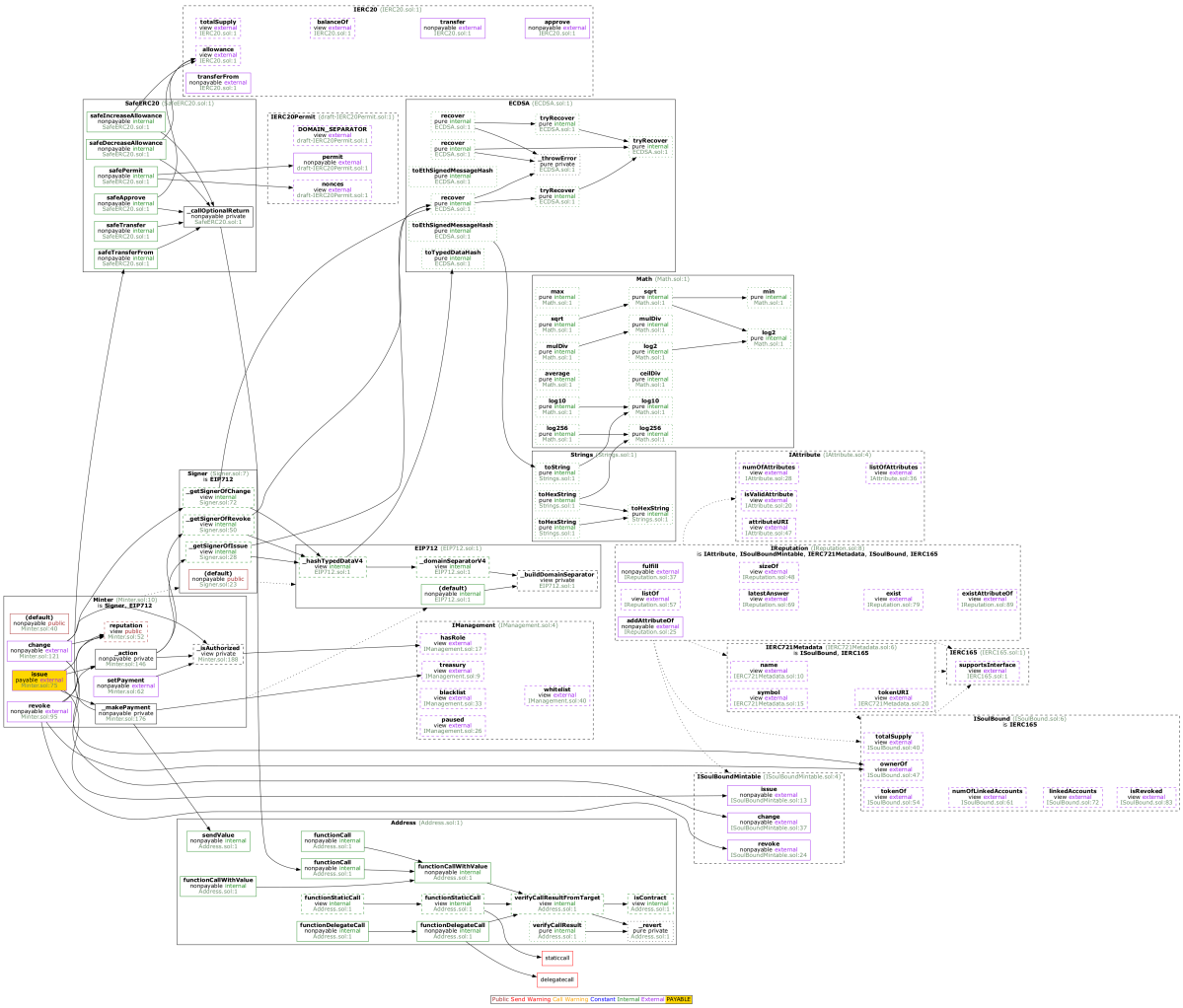

Image 1. Octan SoulBound Token call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Mar 13, 2023*	Public Report	Verichains Lab
1.0	*Mar 17, 2023*	Public Report	Verichains Lab

Table 2. Report versions history