verichains

SECURITY AUDIT OF

ANTA TOKEN AND VESTING TOKEN SMART CONTRACTS

Public Report

Mar 28, 2022

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.
ERC20	ERC20 (BEP20 in Binance Smart Chain or *x*RP20 in other chains) tokens are blockchain-based assets that have value and can be sent and received. The primary difference with the primary coin is that instead of running on their own blockchain, ERC20 tokens are issued on a network that supports smart contracts such as Ethereum or Binance Smart Chain.

EXECUTIVE SUMMARY

This Security Audit Report prepared by Verichains Lab on Mar 28, 2022. We would like to thank the Tribalpunk 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 Anta Token and Vesting Token Smart Contracts. 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 issue in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Anta Token and Vesting Token Smart Contracts

Tribalpunk: Cryptoverse is an Idle/ RPG Collectible Card Game mixed with NFT technology. It was once released on Android/ iOS under the name of Tribal Punk - now modified with blockchain and turned into a fresh product in order to tackle the uprising NFT Gaming Market

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the smart contracts of Anta Token and Vesting Token Smart Contracts. It was conducted on commit a8d3e38fd86f9620c4a57858561b78b2eb3f4bac from git repository *https://github.com/tannct/SC_ANTA/tree/main/contracts*.

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

SHA256 Sum	File
5766fdbb4031757cd862dc6a3c7044d51ea8b2f3f89873e3818fc2061a276143	**AntaToken.sol**
ff0b7efd6de09b25e7a8874a221bd4dd996e9d7e08a3862e9344969ea92b36a4	**VestingToken.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 was 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 Anta Token and Vesting Token Smart Contracts was written in Solidity language, with the required version to be ^0.8.3.

2.1.1. AntaToken contract

The contract imported the ERC20PresetFixedSupply contract which was implemented by OpenZeppelin. The ERC20PresetFixedSupply contract allows the deployer to pre-mint amount of the tokens for an exact user.

Table 2 lists some properties of the audited Anta Token Smart Contract (as of the report writing time).

PROPERTY	VALUE
Name	ANTA
Symbol	ANTA
Decimals	18
Total Supply	1,000,000,000 ($x10^{18}$) Note: the number of decimals is 18, so the total representation token will be 1,000,000,000 or 1 billion.

2.1.2. VestingToken contract

This is the vesting contract in the Anta Token and Vesting Token Smart Contracts, which extends the Ownable contract. With Ownable, by default, Token Owner is contract deployer, but he can transfer ownership to another address at any time. The contract releases the tokens following the times that are hardcoded in the getUnlockAmount function. Only the owner of the contract may claim the tokens in this contract.

2.2. Findings

During the audit process, the audit team found no vulnerability issue in the given version of Anta Token and Vesting Token Smart Contracts.

APPENDIX

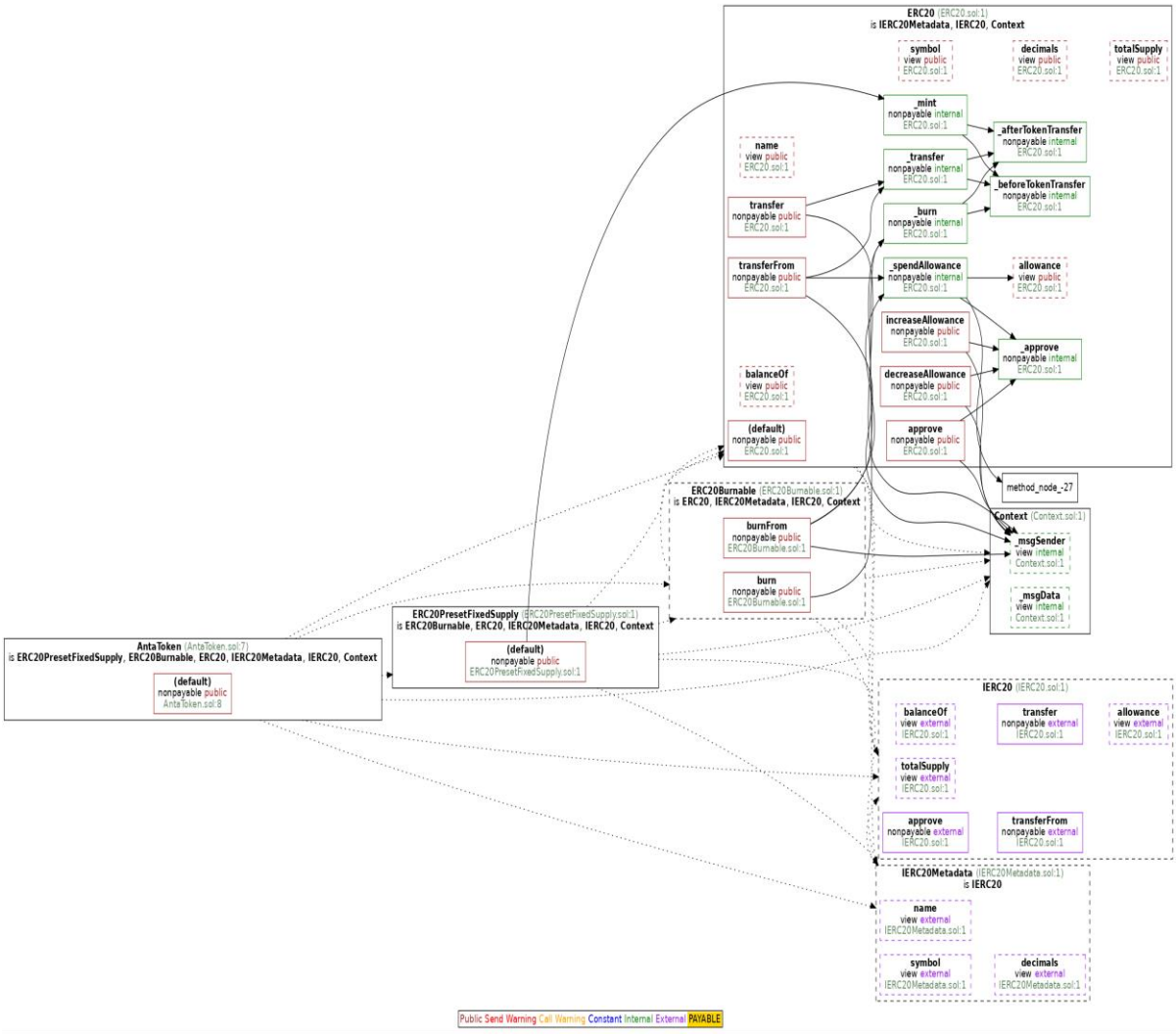

Image 1. AntaToken Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Mar 28, 2022*	Public Report	Verichains Lab

Table 2. Report versions history