



verichains

SECURITY AUDIT OF
DOGEINFINITY TOKEN SMART
CONTRACT



Public Report

Jan 05, 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 xRP20 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 Jan 05, 2022. We would like to thank the DogeInfinity 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 DogeInfinity Token Smart Contract. 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	5
1.1. About DogeInfinity Token Smart Contract.....	5
1.2. Audit scope	5
1.3. Audit methodology.....	5
1.4. Disclaimer	6
2. AUDIT RESULT	7
2.1. Overview	7
2.2. Findings	7
3. VERSION HISTORY	9

1. MANAGEMENT SUMMARY

1.1. About DogeInfinity Token Smart Contract

DogeInfinity Token Smart Contract is ERC20 token which runs on BSC blockchain.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the DogeInfinity Token Smart Contract.

It was conducted on commit [3679529098a9680f5ce09f85e9131a294e929436](#) from git repository <https://github.com/DoginDev/dogin-smartcontract>.

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

SHA256 Sum	File
03551a7fff692565142354ebfeae92eacf39f344a7819d86ed636f446d26a03f	DogeInfinityToken.so

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

This table lists some properties of the audited DogeInfinity Token Smart Contract (as of the report writing time).

PROPERTY	VALUE
Name	DogeInfinity Token
Symbol	DOGIN
Decimals	18
Total Supply	100,000,000,000 ($\times 10^{18}$) Note: the number of decimals is 18, so the total representation token will be 100,000,000,000 or 100 billion.

Table 2. The DogeInfinity Token Smart Contract properties

DogeInfinity Token Smart Contract extends [AccessControl](#), [ERC20](#), [ERC20Snapshot](#) and [ERC20Pausable](#) contracts. [ERC20Snapshot](#) help Token Owner take a snapshot of the balances and total supply at a time for later access. [AccessControl](#) allows the contract to implement role-based access control mechanisms which add token owner (contract deployer) [OWNER_ROLE](#) role.

Token Owner can pause/unpause contract using [ERC20Pausable](#) contract, user can only transfer tokens when contract is not paused.

The contract also implements bot prevent by setting (only [OWNER_ROLE](#) can set) [maxBalanceAmount](#) and [maxTransferAmount](#) which limit max transfer amount and max balance of receiver respectively.

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of DogeInfinity Token Smart Contract.

Security Audit – DogeInfinity Token Smart Contract

Version: 1.0 - Public Report

Date: Jan 05, 2022



APPENDIX

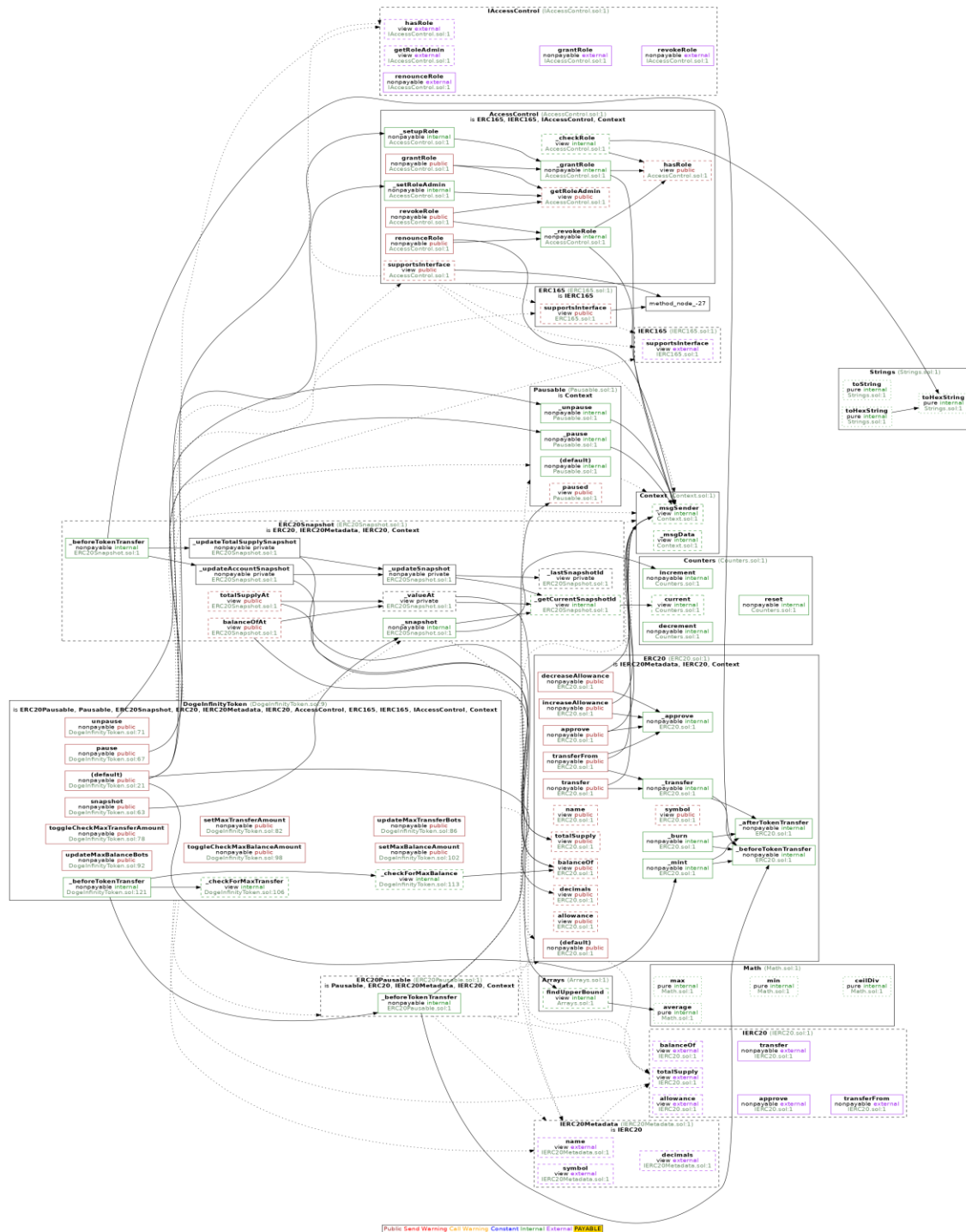


Image 1. DogeInfinity Token Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	<i>Jan 05, 2022</i>	Public Report	Verichains Lab

Table 3. Report versions history