WSN Token (ws.ninja)

SMART CONTRACT AUDIT

20.06.2021

Made in Germany by Chainsulting.de

Table of contents

1. Disclaimer

The audit makes no statements or warrantees about utility of the code, safety of the code, suitability of the business model, investment advice, endorsement of the platform or its products, regulatory regime for the business model, or any other statements about fitness of the contracts to purpose, or their bug free status. The audit documentation is for discussion purposes only.

The information presented in this report is confidential and privileged. If you are reading this report, you agree to keep it confidential, not to copy, disclose or disseminate without the agreement of ws.ninja project. If you are not the intended receptor of this document, remember that any disclosure, copying or dissemination of it is forbidden.

Major Versions / Date	Description
0.1 (19.06.2021)	Layout
0.4 (19.06.2021)	Automated Security Testing Manual Security Testing
0.5 (20.06.2021)	Verify Claims and Test Deployment
0.6 (20.06.2021)	Testing SWC Checks
0.9 (20.06.2021)	Summary and Recommendation
1.1 (20.06.2021)	Final document

2. About the Project and Company

Website: https://www.ws.ninja

GitHub: https://github.com/wsninja

Twitter: https://twitter.com/thewallstninja

Medium: https://medium.com/wall-street-ninja#

Telegram: https://t.me/wsninja

Reddit: https://www.reddit.com/r/WallStreetNinja/

2.1 Project Overview

The Wall Street Ninja finance suite (WSNS) is a complete decentralized finance solution, where users can access the DeFi ecosystem chain of their choice, in a more simplistic manner, broadening accessibility and fostering mainstream adoption. We feel the barrier to adoption is the need to install browser extensions and smartphone wallet apps. There are already a multitude of protocols and liquidity available within the DeFi ecosystem, but largely inaccessible to the average person. Essentially we want to give people accessibility to existing infrastructure in a more user friendly fashion. Our solution is to provide an easy to use web application that does not require browser extensions or userside web3 plugins. Instead we intend to take advantage of blockchain relay and protocol APIs such as Pocket Network and 1inch. In sticking with the decentralized nature of the ecosystem, we intend to host the suite on Dfinity's Internet Computer, which will also provide a single sign-on facility via Dfinity's Internet Identity, however initially we will also provide an option for password (with seed phrase backup) with 2fa sign-on. The most popular technology device in the world is the mobile phone. There are 5.27 billion unique mobile phone users in the world today. WSNS will be accessible across the globe with multilingual support via mobile phone and desktop, making it the users personal decentralized finance solution.

3. Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 – 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

4. Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

4.1 Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
   i. Review of the specifications, sources, and instructions provided to Chainsulting to make sure we understand the size, scope, and functionality of the smart contract.
   ii. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
   iii. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Chainsulting describe.
2. Testing and automated analysis that includes the following:
   i. Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
   ii. Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

4.2 Used Code from other Frameworks/Smart Contracts

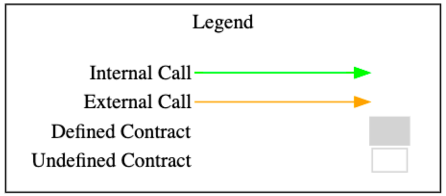
Dependency / Import Path	Source
@openzeppelin/contracts/access/Context.sol	https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/utils/Context.sol
@openzeppelin/contracts/access/Ownable.sol	https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/access/Ownable.sol
@openzeppelin/contracts/math/SafeMath.sol	https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/math/SafeMath.sol

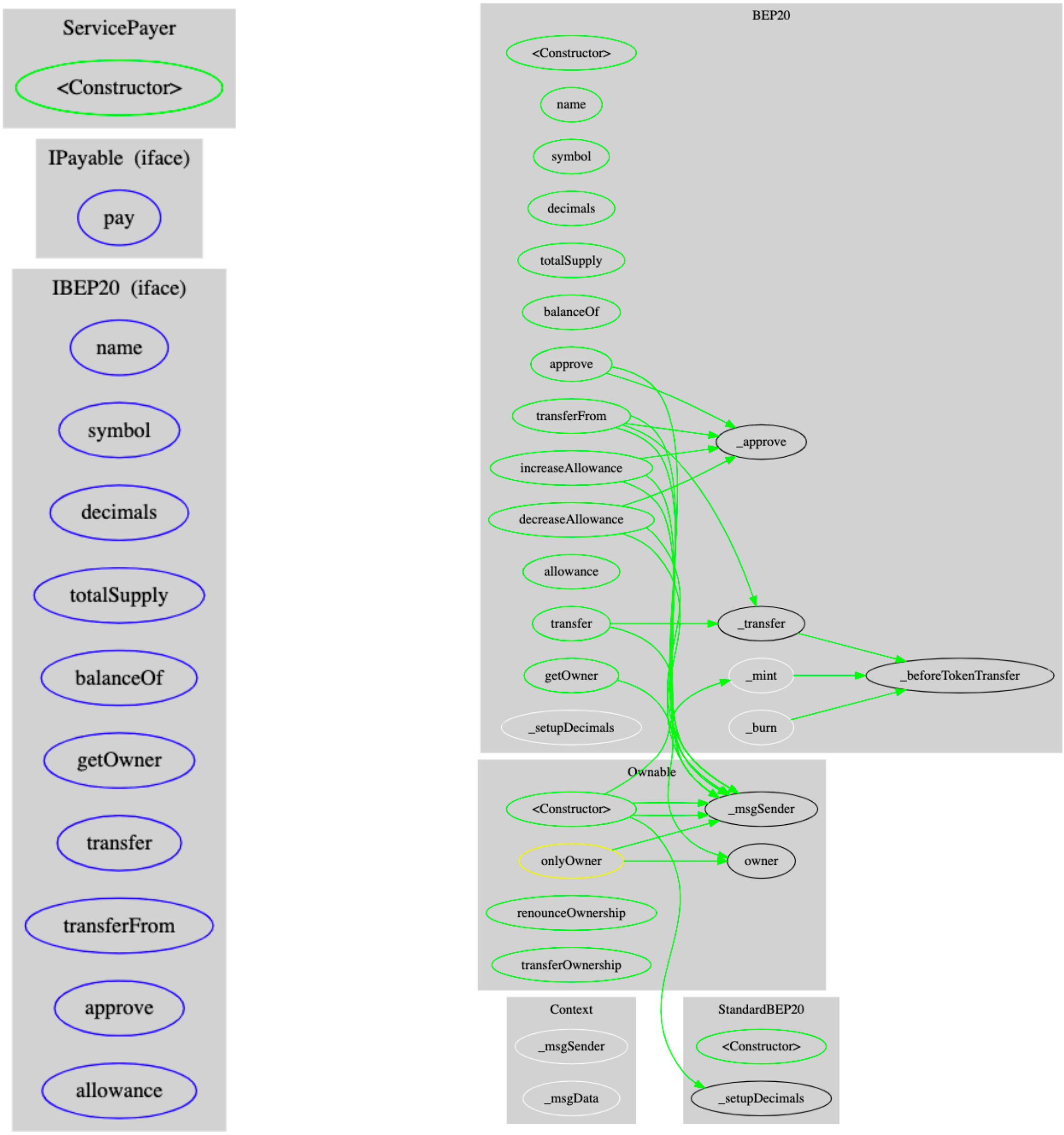
4.3 Tested Contract Files

The following are the MD5 hashes of the reviewed files. A file with a different MD5 hash has been modified, intentionally or otherwise, after the security review. You are cautioned that a different MD5 hash could be (but is not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of the review

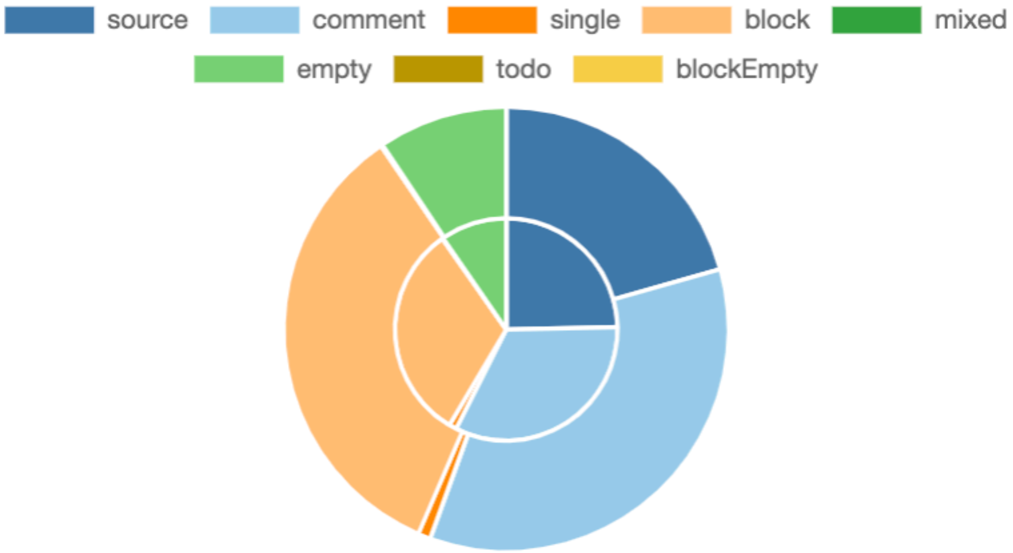
File	Fingerprint (MD5)
wsn_token.sol	6d30aeea2eac12e86e2e1723eccf264d

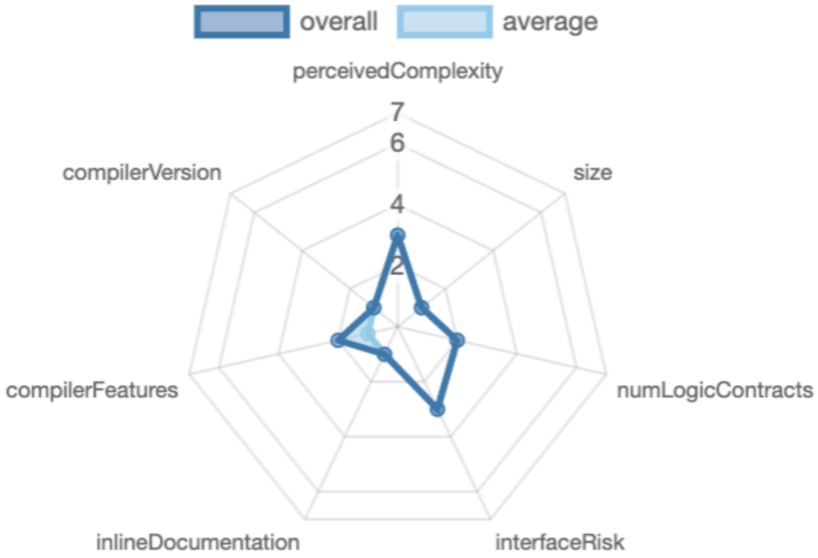
4.4 Metrics / CallGraph





4.5 Metrics / Source Lines & Risk





4.6 Metrics / Capabilities

Solidity Versions observed	🧪 Experimental Features	💰 Can Receive Funds	🖥 Uses Assembly	💣 Has Destroyable Contracts
`^0.8.0`		`yes`	**** (0 asm blocks)	

📤 Transfers ETH	⚡ Low-Level Calls	👥 DelegateCall	🧮 Uses Hash Functions	🔖 ECRecover	🌀 New/Create/Create2

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

🌐Public	💰Payable
26	3

External	Internal	Private	Pure	View
11	26	0	0	17

StateVariables

Total	🌐Public
7	0

4.7 Metrics / Source Unites in Scope

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
📝🔍 🎨	contracts/wsn_token.sol	5	2	572	494	182	308	149	💰
📝🔍 🎨	**Totals**	**5**	**2**	**572**	**494**	**182**	**308**	**149**	💰

Legend: [➖]

- **Lines**: total lines of the source unit
- **nLines**: normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
- **nSLOC**: normalized source lines of code (only source-code lines; no comments, no blank lines)
- **Comment Lines**: lines containing single or block comments
- **Complexity Score**: a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

5. Scope of Work

The WallStreetNinja Team provided us with the file that needs to be tested. The scope of the audit is the WallStreetNinja WSN Token contract.

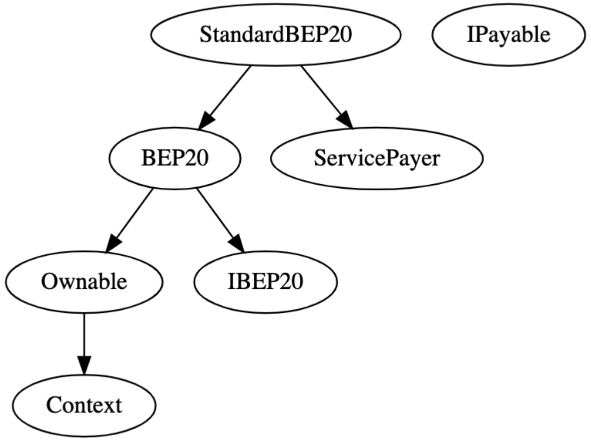
Following contracts with the direct imports has been tested:

- wsn_token.sol

The team put forward the following assumptions regarding the security, usage of the contracts:

- BEP-20 Token standard implementation
- Developer cannot mint any new tokens.
- Developer cannot burn or lock user funds
- Developer cannot pause the contract
- The smart contract is coded according to the newest standards and in a secure way

The main goal of this audit was to verify these claims. The auditors can provide additional feedback on the code upon the client's request.



5.1 Manual and Automated Vulnerability Test

CRITICAL ISSUES

During the audit, Chainsulting‘s experts found **no** **Critical issues** in the code of the smart contract.

HIGH ISSUES

During the audit, Chainsulting’s experts found **no** **High issues** in the code of the smart contract.

MEDIUM ISSUES

During the audit, Chainsulting’s experts found **no** **Medium issues** in the code of the smart contract.

LOW ISSUES

During the audit, Chainsulting’s experts found **no** **Low issues** in the code of the smart contract.

5.2. SWC Attacks

ID	Title	Relationships	Test Result
SWC-131	Presence of unused variables	CWE-1164: Irrelevant Code	✅
SWC-130	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	✅
SWC-129	Typographical Error	CWE-480: Use of Incorrect Operator	✅
SWC-128	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	✅
SWC-127	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	✅
SWC-125	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	✅
SWC-124	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	✅
SWC-123	Requirement Violation	CWE-573: Improper Following of Specification by Caller	✅

ID	Title	Relationships	Test Result
SWC-122	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	☑
SWC-121	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	☑
SWC-120	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	☑
SWC-119	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	☑
SWC-118	Incorrect Constructor Name	CWE-665: Improper Initialization	☑
SWC-117	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	☑
SWC-116	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	☑
SWC-115	Authorization through tx.origin	CWE-477: Use of Obsolete Function	☑
SWC-114	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	☑

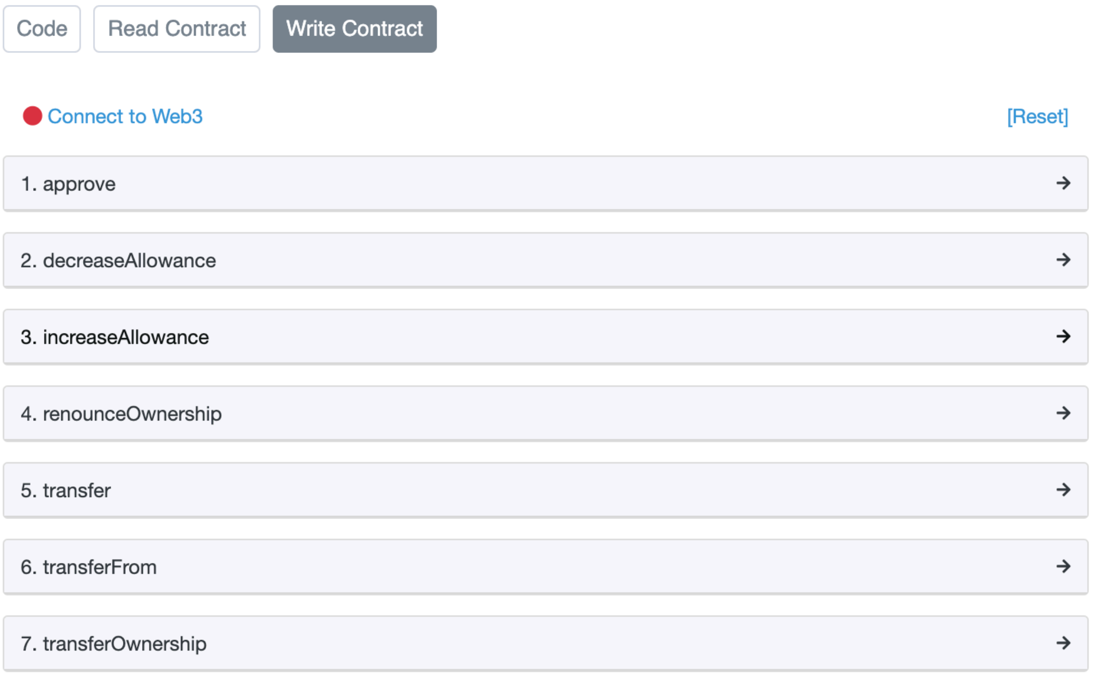
ID	Title	Relationships	Test Result
SWC-113	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	✅
SWC-112	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	✅
SWC-111	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	✅
SWC-110	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	✅
SWC-109	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	✅
SWC-108	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	✅
SWC-107	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	✅
SWC-106	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	✅
SWC-105	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	✅
SWC-104	Unchecked Call Return Value	CWE-252: Unchecked Return Value	✅

ID	Title	Relationships	Test Result
SWC-103	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	X
SWC-102	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	☑
SWC-101	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	☑
SWC-100	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	☑

6. Verify claims

7.1 BEP-20 Token standard implementation
Status: tested and verified ☑

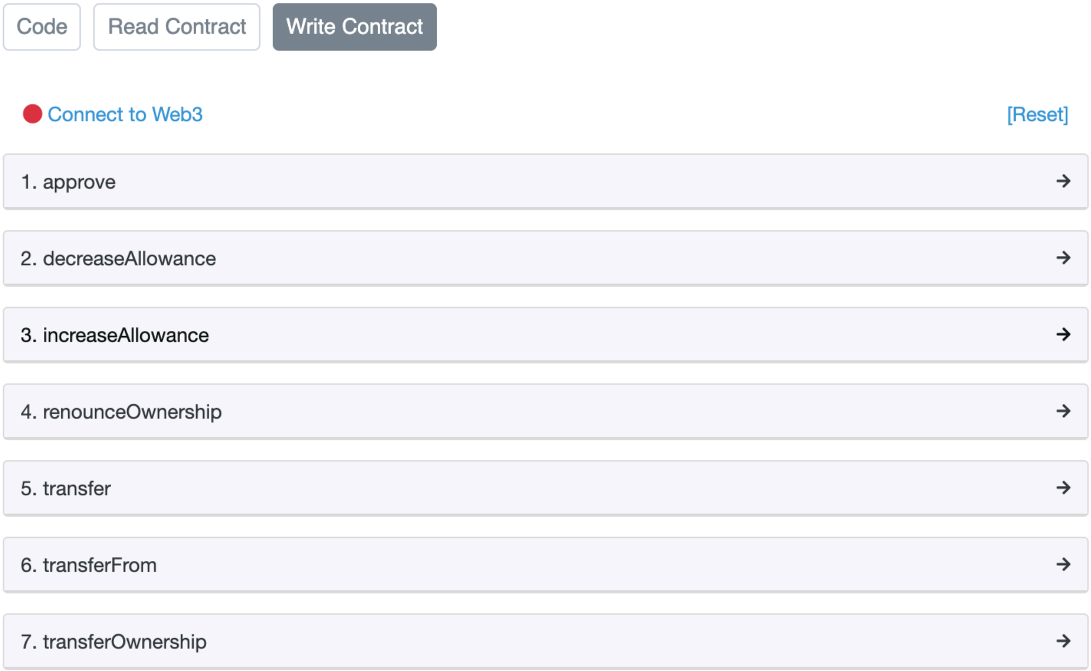
7.2 Developer cannot mint any new tokens.
Status: tested and verified ☑



1. approve
2. decreaseAllowance
3. increaseAllowance
4. renounceOwnership
5. transfer
6. transferFrom
7. transferOwnership

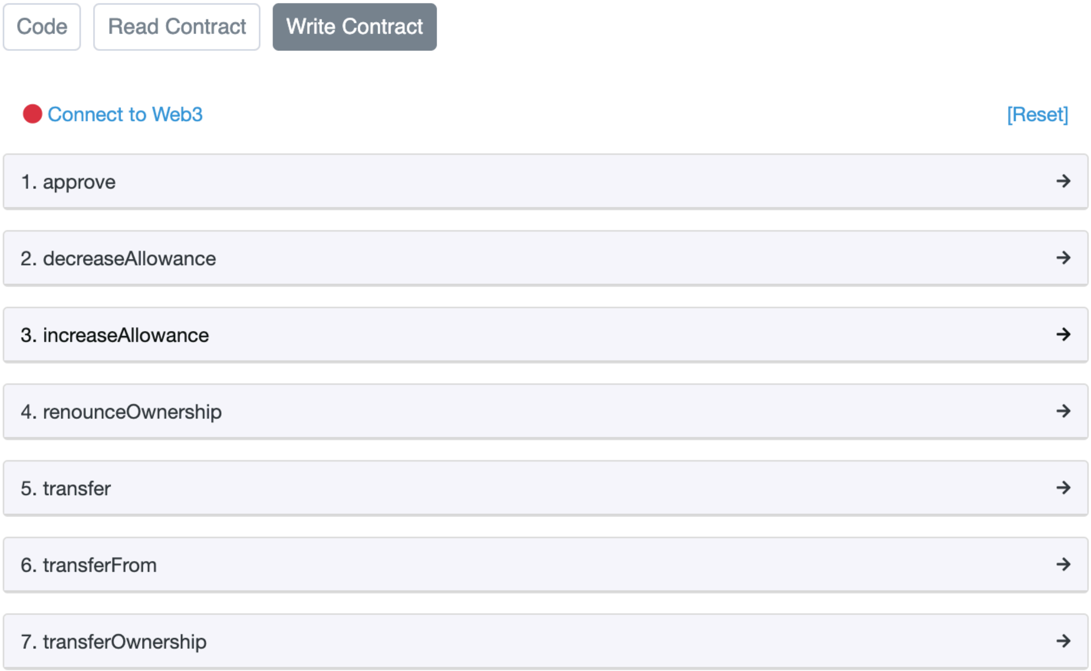
7.3 Developer cannot burn or lock user funds

Status: tested and verified ✅



7.4 Developer cannot pause the contract

Status: tested and verified ✅



1. approve →
2. decreaseAllowance →
3. increaseAllowance →
4. renounceOwnership →
5. transfer →
6. transferFrom →
7. transferOwnership →

7.5 The smart contract is coded according to the newest standards and in a secure way

Status: tested and verified ✅

7. Executive Summary

Two (2) independent Chainsulting experts performed an unbiased and isolated audit of the smart contract codebase. The final debrief took place on the June 20th, 2021. The overall code quality of the project is very good, not overloaded with unnecessary functions, these is greatly benefiting the security of the contract. It correctly implemented widely-used and reviewed contracts from OpenZeppelin.

The main goal of the audit was to verify the claims regarding the security of the smart contract and the claims inside the scope of work. During the audit, no issues were found after the manual and automated security testing.

8. Deployed Smart Contract

VERIFIED

Deployed Smart Contract
https://bscscan.com/address/0x7fa4cd8aeedcb8d36dbc5d856e3a1bee490d7b36#code