



World Token

OTC Contract

SMART CONTRACT AUDIT

22.02.2021

Made in Germany by Chainsulting.de



Table of contents

1. Disclaimer.....	3
2. About the Project and Company	4
2.1 Project Overview.....	5
3. Vulnerability & Risk Level	6
4. Auditing Strategy and Techniques Applied.....	7
4.1 Methodology	7
4.2 Used Code from other Frameworks/Smart Contracts	8
4.3 Tested Contract Files	9
4.4 Metrics / CallGraph.....	10
4.5 Metrics / Source Lines	11
4.6 Metrics / Capabilities	12
4.7 Metrics / Source Unites in Scope.....	13
5. Scope of Work.....	14
5.1 Manual and Automated Vulnerability Test.....	15
5.2. SWC Attacks & Special Checks.....	16
7. Test Deployment.....	20
7.1 Deploy WORLD Token	20
7.2 Deploy WorldOTC contract.....	21
7.3 Transfer WOLRD to WorldOTC contract.....	21
7.4 Set vesting cliff duration and vesting duration	22
7.5 Set Rate for vestings	23
7.6 Vesting 1 Ether and WORLD tokens.....	24



7.7	Withdraw Funds.....	24
7.8	Withdraw Tokens.....	24
7.2.	Verify Claims	25
8.	Executive Summary.....	26
9.	Deployed Smart Contract	26

1. Disclaimer

The audit makes no statements or warranties 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 World Token. 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 (15.02.2021)	Layout
0.5 (16.02.2021)	Automated Security Testing Manual Security Testing
0.8 (17.02.2021)	Testing SWC Checks
0.9 (18.02.2021)	Summary and Recommendation
1.0 (18.02.2021)	Final document
1.2 (22.02.2021)	Added deployed contracts

2. About the Project and Company

Company address: NA (ANON)

Website: <https://worldtoken.network/>

GitHub: <https://github.com/worldtoken/>

Twitter: <https://twitter.com/worldtoken>

Telegram: <https://t.me/worldtokenofficial>

Etherscan (WORLD Token): <https://etherscan.io/token/0xbf494f02ee3fde1f20bee6242bce2d1ed0c15e47>

2.1 Project Overview

WORLD is a unique platform that combines the best tokenomics of current frictionless yield protocols for instant rewards with the additional benefits of staking in our upcoming marketplace. This way the best rewards can be guaranteed without any token inflation. A 3% transaction tax goes to holders (later on merchants too), stakers, and a perpetual marketing and development fund. This project is built to keep going and continually expand further until it has its own ecosystem to call its own. The \$WORLD system guarantees token rewards to LP stakers on every block, regardless if there was a \$WORLD transaction on it or not. Under the same system, rewards will scale as the project grows, whilst ensuring the rewards pool can never run out.

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 (direct imports)

1. SafeMath.sol

<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v3.4.0/contracts/math/SafeMath.sol>

2. IERC20.sol

<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v3.4.0/contracts/token/ERC20/IERC20.sol>

3. SafeERC20.sol

<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v3.4.0/contracts/token/ERC20/SafeERC20.sol>

4. Ownable.sol

<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v3.4.0/contracts/access/Ownable.sol>

5. Clones.sol

<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v3.4.0/contracts/proxy/Clones.sol>

6. Initializable.sol

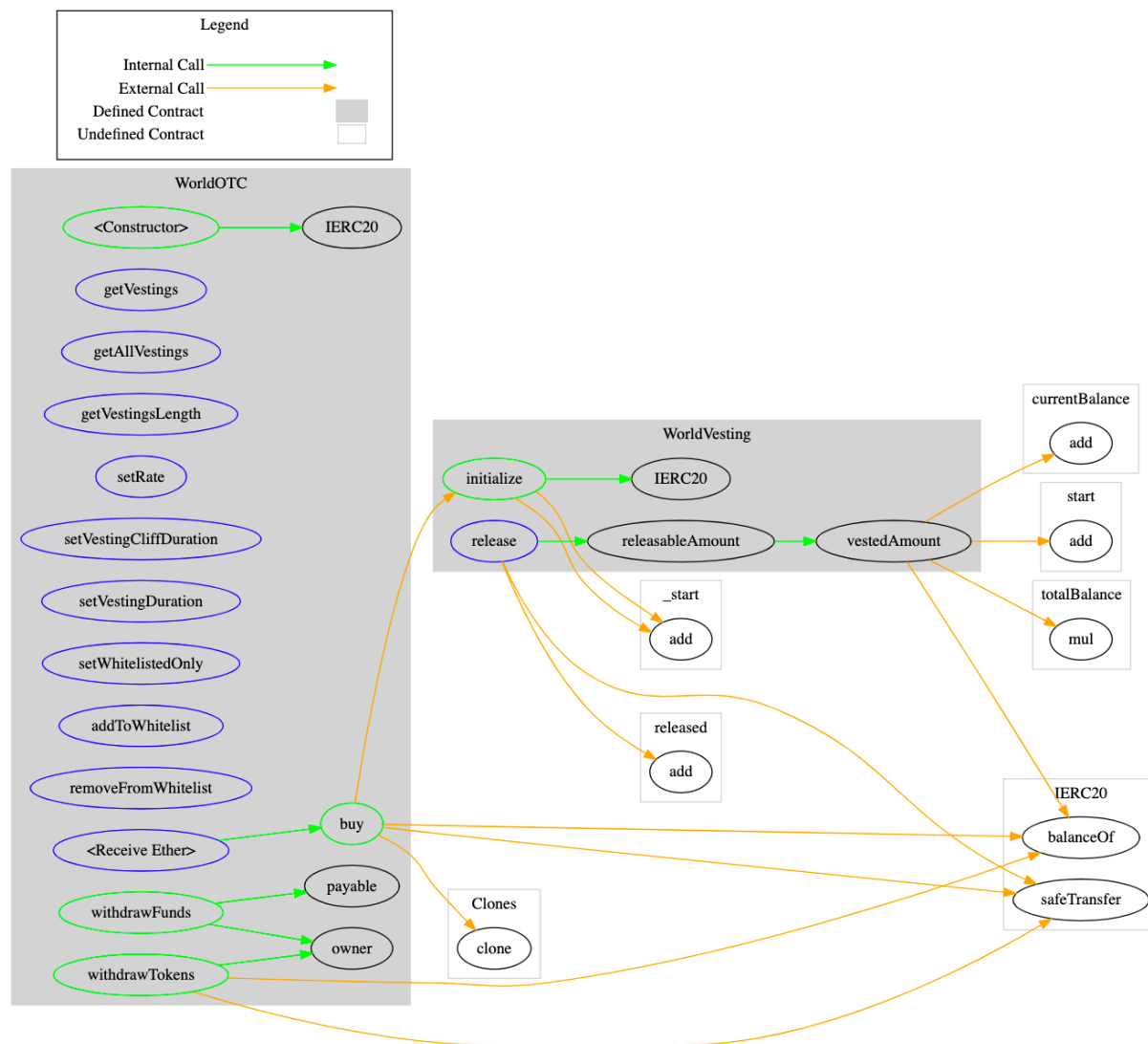
<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v3.4.0/contracts/proxy/Initializable.sol>

4.3 Tested Contract Files

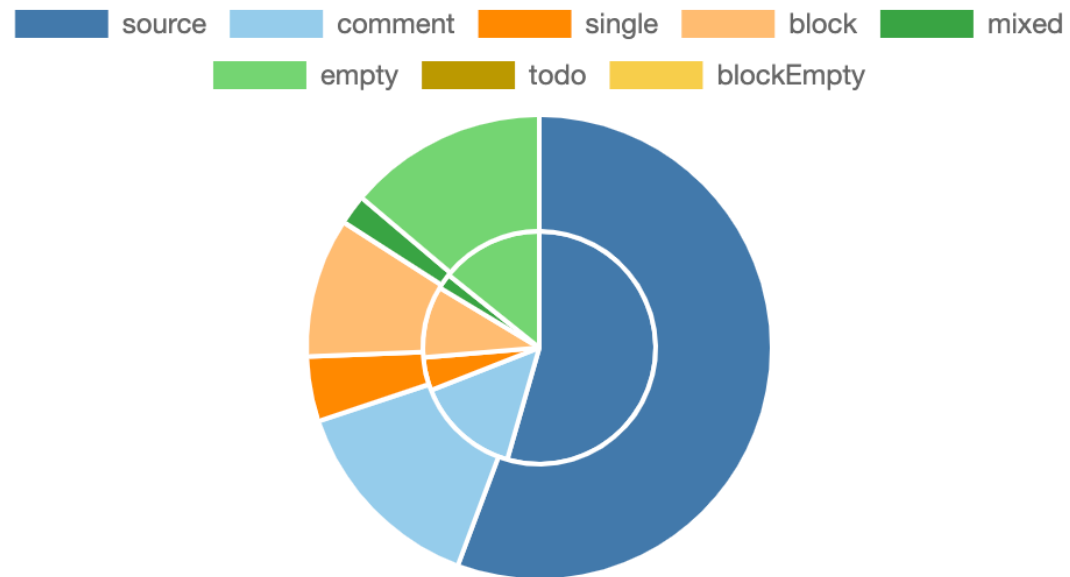
The following are the MD5 hashes of the reviewed files. A file with a different MD5 hash has been modified, intentionally or otherwise, after the security review. You are cautioned that a different MD5 hash could be (but is not necessarily) an indication of a changed condition or potential vulnerability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

File	Fingerprint (MD5)
WorldOTC.sol	03f30de3a5e945b05050daea62bc8da3
WorldVesting.sol	6ee13e86793dc30fbaa84216af804126





4.4 Metrics / CallGraph











4.5 Metrics / Source Lines








4.6 Metrics / Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts
0.7.4		yes	**** (0 asm blocks)	

 Transfers ETH	 Low-Level Calls	 DelegateCall	 Uses Hash Functions	 ECRrecover	 New/Create/Create2
yes					

 Public	 Payable			
17	2	External	Internal	Private
		Pure	View	
		11	11	0
			0	5

4.7 Metrics / Source Unites in Scope

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex Score	Capabilities
	WorldOTC.sol	1	_____	127	127	101	1	109	
	WorldVesting.sol	1	_____	109	101	52	40	47	_____
	Totals	2	_____	236	228	153	41	156	

5. Scope of Work

The World Token Team provided us with the files that needs to be tested. The scope of the audit is the WorldOTC contract.

Following contracts with the direct imports been tested

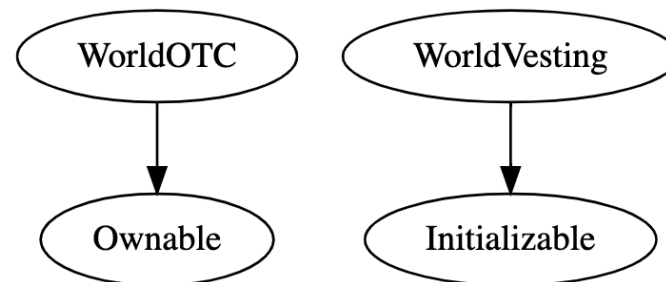
WorldOTC.sol

WorldVesting.sol

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

- OTC Buyer is able to withdraw vested World Token after vesting period ends
- Owner is able to withdraw raised funds
- Deployer cannot burn any vested funds during the vesting period
- Deployer cannot pause the contract

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 & Special Checks

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	
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	

7. Test Deployment

7.1 Deploy WORLD Token

CONTRACT

WorldToken - browser/contracts/4_WORLD.sol

DEPLOY

_MARKETINGADDRESS: 0x97E1cD3a5a366fc624399A4209C8E681EcFE3c1a

transact

Tx: <https://ropsten.etherscan.io/tx/0x0f1b7e075425cf6011345d2227ec603cd5946d5cc698060cd35c1adfe70bdbcd>

Contract: [0x6dB2cBCBd90269750a087E1729C8476C78337190](#)

7.2 Deploy WorldOTC contract

CONTRACT

WorldOTC - browser/contracts/5_WORLDOTC.sol

DEPLOY

_WORLD: 0x6dB2cBCBd90269750a087E1729C8476C78337190

_VESTINGLOGIC: 0x11F8Ab8137cf797cFFDa160D5a355616a71EDBfD

_RATE: 50

transact

Tx: <https://ropsten.etherscan.io/tx/0x28e4cf9b5aa0c46babdb5686bd1c069846b1f38dcc569419b9d07d2891c002c6>

Contract: [0x4EEa3C91A403DE9f42c3E5017c751e6609883eeb](#)

7.3 Transfer WOLRD to WorldOTC contract

Tx: <https://ropsten.etherscan.io/tx/0x6874e9a2893df6394a5edec5558c36ee2a5ebb367e7693f537b34809f061fec0>

7.4 Set vesting cliff duration and vesting duration

vestingCliffDuration

0: uint256: 604800

vestingDuration

0: uint256: 2419200

setVestingCliffDuration transaction:

Tx: <https://ropsten.etherscan.io/tx/0xeb16033f7783c5a3132f3512e6699810a3b1306fd8210b99772233f0e02961cd>

setVestingDuration transaction:

Tx: <https://ropsten.etherscan.io/tx/0x956da736d91992a67953861058514c3bba8db11a2e4a1a317c57fc06bd3077e8>

vestingCliffDuration

0: uint256: 30

vestingDuration

0: uint256: 60

setRate

rate

0:

7.6 Vesting 1 Ether and WORLD tokens

The minimum vesting amount is 1 Ether.

Vesting address: 0x2f1602fd37228b32ad8d13137b1b620862771909 (vester)

getVestingsLength

_account: "0x2F1602FD37228b32Ad8D13137b1B620862771909"



call

0: uint256: 0

Tx: <https://ropsten.etherscan.io/tx/0x217a395c12775c50e91edce9e3a4cc27ad0e168c625346131cac20203cb8ba25>

getVestingsLength

_account: "0x2F1602FD37228b32Ad8D13137b1B620862771909"



call

0: uint256: 1

7.7 Withdraw Funds

This function can only be called by the contract owner!

Receipient address: 0x97E1cD3a5a366fc624399A4209C8E681EcF3c1a (owner)

Tx: <https://ropsten.etherscan.io/tx/0x34b77428a3c929e2a103fb8a598e3184f646aa9d3a4dd5f201176f91e4863522>

7.8 Withdraw Tokens

Tx: <https://ropsten.etherscan.io/tx/0xdf3ee7d24b44bda8f85a89ff03ab97f03f6e5ba999403c7fffeb195d101911c6>



7.2. Verify Claims

7.2.1 OTC Buyer is able to withdraw vested World Token after vesting period ends 

Status: tested and verified

7.2.2 Owner is able to withdraw raised funds 

Status: tested and verified

7.2.3 Deployer cannot burn any vested funds during the vesting period 

Status: tested and verified

7.2.4 Deployer cannot pause the contract 

Status: tested and verified

7.2.5 Checking the overall security 

8. Executive Summary

The overall code quality of the project is good. It correctly implemented widely-used and reviewed contracts from OpenZeppelin and for safe mathematical operations.

The main goal of the audit was to verify the claims regarding the security of the smart contract and the functions. During the audit, no issues were found after the manual and automated security testing and the claims been successfully verified.

9. Deployed Smart Contract

VERIFIED

BSC Contract is deployed here:

<https://bscscan.com/address/0xB11843965f6396C315a477C6D61B2A7b970E4fA3#code>

ETH Contract is deployed here:

<https://etherscan.io/address/0x1f2f6E2F06d6723638175f285bAE0A900d1b5BFA#code>