



# Smart Contract Security Audit Report

---

## Covalent Token

October 2022

Security Status



[www.hacksafe.io](https://www.hacksafe.io)



# Audit Details



## Audited project

Covalent Token



## Deployer address

0x9376d84035891505fBA7999550B1d602E688Ebe0



## Client contacts

Covalent Token Team



## Blockchain

Ethereum



## Website

<https://covalent.ai/>



# Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

**DISCLAIMER:** By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and HackSafe hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.



# Procedure

## **Step 1 - In-Depth Manual Review**

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

## **Step 2 - Automated Testing**

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

## **Step 3 – Leadership Review**

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

## **Step 4 - Resolution of Issues**

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

## **Step 5 - Published Audit Report**

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

# Background

**HackSafe was commissioned by Covalent Token to perform an audit of smart contracts:**

- <https://etherscan.io/address/0xb37a769b37224449d92aac57de379e1267cd3b00#code>

**The purpose of the audit was to achieve the following:**

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understood to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

# Contract Details

## Token contract details for 11.10.2022

Token Type	: ERC20
Contract name	: CovaToken
Contract address	: 0xB37a769B37224449d92AAc57dE379E1267Cd3B00
Total supply	: 6,500,000,000
Token ticker	: COVA
Decimals	: 18
Token holders	: 32,081
Transactions count	: 51,694
Compiler version	: v0.4.24+commit.e67f0147
Contract deployer address	: 0x9376d84035891505fBA7999550B1d602E688Ebe0
Owner address	: No owner



# Social profiles

Telegram profile	: <a href="https://t.me/covalentofficial">https://t.me/covalentofficial</a>
Twitter profile	: <a href="https://twitter.com/covatoken">https://twitter.com/covatoken</a>
Coinmarketcap profile	: <a href="https://coinmarketcap.com/currencies/cova/">https://coinmarketcap.com/currencies/cova/</a>
Coingecko profile	: <a href="https://www.coingecko.com/en/coins/covalent-cova/">https://www.coingecko.com/en/coins/covalent-cova/</a>

# Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Well Secure”**. This token contract does not contain owner control, which do make it fully decentralized as owner does not have control over the smart contract.

Insecure	Poor secured	Secure	Well-secured
----------	--------------	--------	--------------

You are here





We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

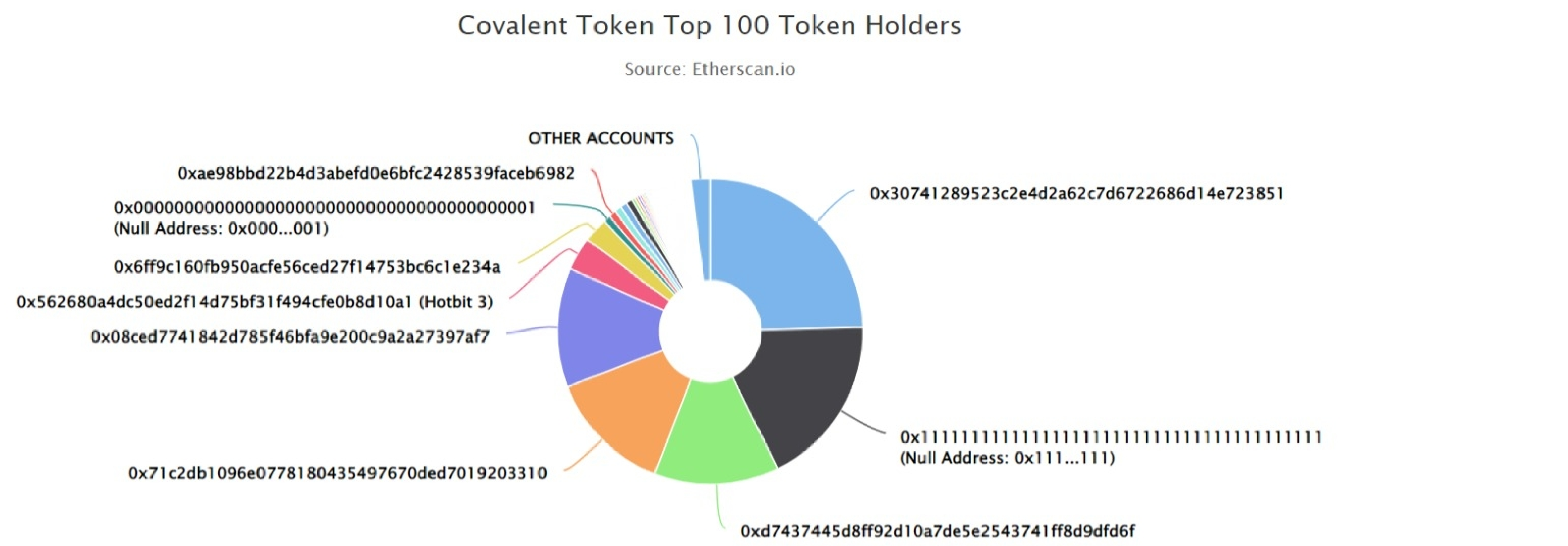
We found 0 critical, 0 high, 0 medium and 2 low and some very low-level issues.



# Covalent Token Distribution




 The top 100 holders collectively own 98.03% (6,372,189,476.69 Tokens) of Covalent Token

 Token Total Supply: 6,500,000,000.00 Token | Total Token Holders: 32,081



## Covalent Token Top 20 Token Holders

(A total of 6,372,189,476.69 tokens held by the top 100 accounts from the total supply of 6,500,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x30741289523c2e4d2a62c7d6722686d14e723851	1,597,692,149.203541141133028188	24.5799%
2	Null Address: 0x111...111	1,180,000,001	18.1538%
3	0xd7437445d8ff92d10a7de5e2543741ff8d9dfd6f	860,000,000	13.2308%
4	 0x71c2db1096e0778180435497670ded7019203310	853,125,000	13.1250%
5	0x08ced7741842d785f46bfa9e200c9a2a27397af7	819,999,999	12.6154%
6	Hotbit 3	228,795,976.79573703837942647	3.5199%
7	 0x6ff9c160fb950acfe56ced27f14753bc6c1e234a	166,208,251.492937475758858886	2.5571%
8	Null Address: 0x000...001	50,000,030.07223976	0.7692%
9	0xae98bbd22b4d3abefd0e6bfc2428539faceb6982	49,998,583.40070187	0.7692%
10	0xf99c841f3cc86413df5035a84598d963d70731a3	48,476,032.37713117	0.7458%
11	0x3541f9dd7bddca6a328a0e550772e821dbcbf327	47,827,228.594	0.7358%
12	0x2d4b3536625f6a3e689f8025f11570655a998006	45,012,133.719360727550274877	0.6925%
13	 0x3dd223968c2acb1071dfb327cc0065a5fa4d4b15	22,349,456.2356412	0.3438%
14	0x142e1450f293828189b218bfe56e6822188d70ca	19,471,286.64217956	0.2996%
15	0x803d8a7fb42384cdc51d9ee985cd75ddaba7322f	18,375,583.10102206	0.2827%
16	0x91b231e062650d6f5fd9761ff2c3b6c9c6265911	15,248,066.719322203178736153	0.2346%
17	0xb3aec527d280f9e4d332d26df8a7f8552ae3ae58	14,511,923.41189763	0.2233%
18	0xfb1d86e1c0ed757d4646b00b6fbb4c65d82edb59	11,981,548.28455868	0.1843%
19	0xd87d8ae498b124e51a2bbb473ba3e88aeeffcaa88	11,331,478.09	0.1743%
20	0x2106f1816d50014b628c81b8c8b1845a64ca9390	11,200,030	0.1723%

# Covalent Token Distribution

## Covalent Token Contract Overview





# Contract functions details

## +ERC20

- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] allowance
- [Pub] transfer
- [Pub] approve
- [Pub] transferFrom

## +[Lib] SafeMath

- [Int] mul
- [Int] div
- [Int] sub
- [Int] add
- [Int] mod

## +CovaToken (ERC20)

- [Pub] <constructor>
- [Pub] totalSupply
- [Pub] name
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] balanceOf
- [Pub] allowance
- [Pub] transfer #
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseApproval #
- [Pub] decreaseApproval #

(\$) = payable function

# = non-constant function

# Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Low issue



# Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

# Security Issues

## ✔ Critical Severity Issues

No critical severity issue found.

## ✔ High Severity Issues

No high severity issues found.

## ✔ Medium Severity Issues

No medium severity issue found.

## ✔ Low Severity Issues

Two low severity issue found..

### 1. Unlocked Compiler Version.

#### • Description

The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

#### • Recommendation

It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version 0.4.24 the contract should contain the following line:

```
pragma solidity 0.4.24;
```

### 2. Too old compiler version.

#### • Description

Contract has been deployed using too old compiler version.

#### • Recommendation

It is advisable that the compiler version of solidity should be among the new compiler versions.



# Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.