Bumblebee

Security Assessment

12th May 2023

TRUSCOVA

TRUSTED CODE VALIDATION

Prepared for: Bumblebee

Prepared by: Dr. Muhammad Hassan

WE SECURE YOUR SMART CONTRACTS

About Truscova

Founded in last quarter of 2022 and headquartered in Bremen, Germany, Truscova aims to secure Web 3.0 by providing security assessment, audit, advisory and training services using formal verification and other leading technologies. Truscova founders include eminent scientists with more than 35 books, several patents, and more than 20,000 google scholar citations in the areas of verification, testing, security, and machine learning.

We focus on smart contracts testing and code review projects in Ethereum ecosystem, supporting client organizations in technology, defense, and finance industries, as well as government entities. We specialize in applying formal verification, dynamic analysis, fuzz testing, metamorphic testing, advanced coverage metrics, and static analysis to secure Web 3.0 projects.

We maintain an exhaustive list of publications at https://github.com/Truscova, with links to papers, presentations, public audit reports, and blog articles.

To explore our latest news and developments, please follow @truscova on Twitter or LinkedIn. You can also explore our repository at https://github.com/Truscova or blog articles at https://truscova.com/blog.php. To engage us directly, visit our “Contact” page at https://www.truscova.com/.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Notices and Remarks

Copyright and Distribution

This report is produced by Truscova for public information. It is licensed to Neoki Multi Metaverse under the terms of the project agreement and is being made public as per project agreement.

Test Coverage Disclaimer

All activities undertaken by Truscova in this project were performed in accordance with terms of the project agreement.

Truscova uses a combination of automated testing techniques and manual inspection to conduct security assessments and identify security flaws of the target system. Each method carries its own limitations.

Security assessments are time bound (hence not exhaustive) and are reliant on information provided by the client. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Contents

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Executive Summary

Engagement Overview and Scope

Bumblebee engaged Truscova GmbH from 10th May 2023 till 13th May 2023 to review and audit the code base provided via online deployed contract available at following address:

0x94E67fda4311dC1f3fdCbEc0b47215c401d1584f

The scope of audit is limited to the following:

- 0x94E67fda4311dC1f3fdCbEc0b47215c401d1584f

One security expert at Truscova audited the above code base using static analysis, symbolic execution, fuzzing, formal verification, and manual inspection. A summary of findings is discussed in the next subsection.

Summary of Findings

The uncovered vulnerabilities in codebase during the course of the audit are summarized in the following table:

Vulnerability Classification

Classification	*Count*
Informational	1

Vulnerability Categorization

Category	*Count*
Library Use	1

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Summary

Contact Information

Following officials from Truscova participated in this project.

Dr. Muhammad Naiman Jalil, naiman@truscova.com	Project Coordination
Dr. Muhammad Hassan, hassan@truscova.com	Security Assessment Expert

Project Timeline

The significant project events and milestones are as follows:

Date	**Event**
10th May, 2023	First Contact
10th May, 2023	Contract Agreement
10th May, 2023	Assessment Start
12th May, 2023	Assessment Complete
12th May, 2023	Final Audit Report Submitted

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Goals

The engagement was scoped to assess the security of Bumblebee token contracts. Specifically, we focused to answer the following non-exhaustive list of questions:

- Are there appropriate access controls in place?
- Are user-provided parameters sufficiently validated?
- Are the arithmetic calculations and state changes performed during token purchases, correct?
- Could an attacker steal funds from the system?
- Could an attacker take over the contract's ownership?
- How does the minting of tokens work?

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Targets

The engagement involved a review and testing of the following targets:

Bumblebee

1. Contract 0x94E67fda4311dC1f3fdCbEc0b47215c401d1584f

Codebase Type: Solidity

Platform: BNB Smart Chain

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Coverage

This section provides an overview of the analysis coverage of the review, as determined by our high-level engagement goals. Our approaches and their results include the following:

Bumblebee Token

Bumblebee token is a standard token, which is ERC-20 compliant, and is designed to be deployed on the BNB smart chain. ERC-20 is a technical standard for tokens on the Ethereum blockchain that defines a common set of rules for tokens to follow. This standard ensures interoperability between different tokens and enables developers to create decentralized applications that can work with a wide range of tokens.

The contract implements the **IERC20** interface, which is defined in the **IERC20.sol** file. The **IERC20** interface defines a set of functions that a token contract must implement to be considered ERC-20 compliant. The contract also uses the **Ownable** and **BaseToken** contracts, which are defined elsewhere in the codebase.

The contract has the following state variables:

- **VERSION**: a public constant that represents the version of the token contract.
- **_balances**: a private mapping that stores the balance of each address that holds the token.
- **_allowances**: a private mapping that stores the amount of tokens that an address is allowed to spend on behalf of another address.
- **_name**: a private string that represents the name of the token.
- **_symbol**: a private string that represents the symbol of the token.
- **_decimals**: a private uint8 that represents the number of decimal places that the token uses.
- **_totalSupply**: a private uint256 that represents the total supply of the token.

The contract has a constructor that takes the following parameters:

- **name_**: the name of the token.
- **symbol_**: the symbol of the token.
- **decimals_**: the number of decimal places used by the token.
- **totalSupply_**: the initial total supply of the token.
- **serviceFeeReceiver_**: the address of the account that will receive the service fee.
- **serviceFee_**: the amount of the service fee to be paid.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

The constructor initializes the state variables **_name**, **_symbol**, **_decimals**, and **_totalSupply**, and mints the total supply of the token to the owner's account. It also emits a **TokenCreated** event with the **TokenType** set to **standard**. Finally, it transfers the service fee to the **serviceFeeReceiver_** address.

The contract has the following public functions:

- **name()**: a view function that returns the name of the token.
- **symbol()**: a view function that returns the symbol of the token.
- **decimals()**: a view function that returns the number of decimal places used by the token.
- **totalSupply()**: a view function that returns the total supply of the token.
- **balanceOf(address account)**: a view function that returns the balance of the specified account.
- **transfer(address recipient, uint256 amount)**: a function that transfers tokens from the caller's account to the specified recipient.
- **allowance(address owner, address spender)**: a view function that returns the amount of tokens that the spender is allowed to spend on behalf of the owner.
- **approve(address spender, uint256 amount)**: a function that sets the allowance for the specified spender.
- **transferFrom(address sender, address recipient, uint256 amount)**: a function that transfers tokens from the sender's account to the recipient's account.
- **increaseAllowance(address spender, uint256 addedValue)**: a function that increases the allowance of the specified spender.
- **decreaseAllowance(address spender, uint256 subtractedValue)**: a function that decreases the allowance of the specified spender

We conducted a review of the contract and investigated the following:

- We reviewed if an attacker could bypass the access control on minting and burning functions.
- We checked the arithmetic operations.
- We checked if roles could be updated or not.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Automated Testing

In this evaluation, Echidna, a smart contract fuzzer, was utilized to swiftly examine various system states and verify security properties through malicious, coverage-guided test case generation. Automated testing techniques were employed to supplement manual security reviews rather than replace them. However, each technique has limitations, such as Echidna's inability to randomly generate an edge case that violates a property. To maximize the effectiveness of security testing, a consistent process is followed. In the case of Echidna, 100,000 test cases are generated per property.

The focus of our automated testing and verification efforts was on the essential properties and elements of the Bumblebee Token. Our aim was to ensure that the critical system properties are maintained to ensure correct protocol behavior.

Basic properties for standard functions

Property	Result
Total supply should be constant for non-mintable and non-burnable tokens.	Passed
No user balance should be greater than the token's total supply.	Passed
The sum of users balances should not be greater than the token's total supply.	Passed
Token balance for address zero should be zero.	Passed
transfers to zero address should not be allowed.	Passed
transferFroms to zero address should not be allowed.	Passed
Self transfers should not break accounting.	Passed
Self transferFroms should not break accounting.	Passed
transfers for more than account balance should not be allowed.	Passed
transferFroms for more than account balance should not be allowed.	Passed
transfers for zero amount should not break accounting.	Passed
transferFroms for zero amount should not break accounting.	Passed
Valid transfers should update accounting correctly.	Passed
Valid transferFroms should update accounting correctly.	Passed
Allowances should be set correctly when approve is called.	Passed
Allowances should be updated correctly when approve is called twice.	Passed
After transferFrom, allowances should be updated correctly.	Passed

Tests for burnable tokens

Property	Result
User balance and total supply should be updated correctly when burn is called.	Passed
User balance and total supply should be updated correctly when burnFrom is called.	Passed
Allowances should be updated correctly when burnFrom is called.	Passed

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Tests for mintable tokens

Property	Result
User balance and total supply should be updated correctly after minting.	Passed

Tests for pausable tokens

Property	Result
Token transfers should not be possible when paused state is enabled.	Passed
Token transferFroms should not be possible when paused state is enabled.	Passed

Tests for tokens implementing increaseAllowance and decreaseAllowance

Property	Result
Allowance should be updated correctly when increaseAllowance is called.	Passed
Allowance should be updated correctly when decreaseAllowance is called.	Passed

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Summary of Findings

The table below summarizes the findings of the review, including type and severity details.

ID	Title	Type	Severity
1	Use of SafeMath library	Library use	Informational

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Detailed Findings

1. Use of SafeMath library

Severity: Informational	Difficulty: -
Type: Library use	Finding ID: TCV-NK-1
Target: StandardToken	

Description

The Bumblebee Token uses SafeMath library in addition to Solidity version 0.8.0+. This is unnecessary as the integer overflow/underflow checks are now built into the compiler starting from Solidity 0.8.0+. Hence, SafeMath can be safely removed.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

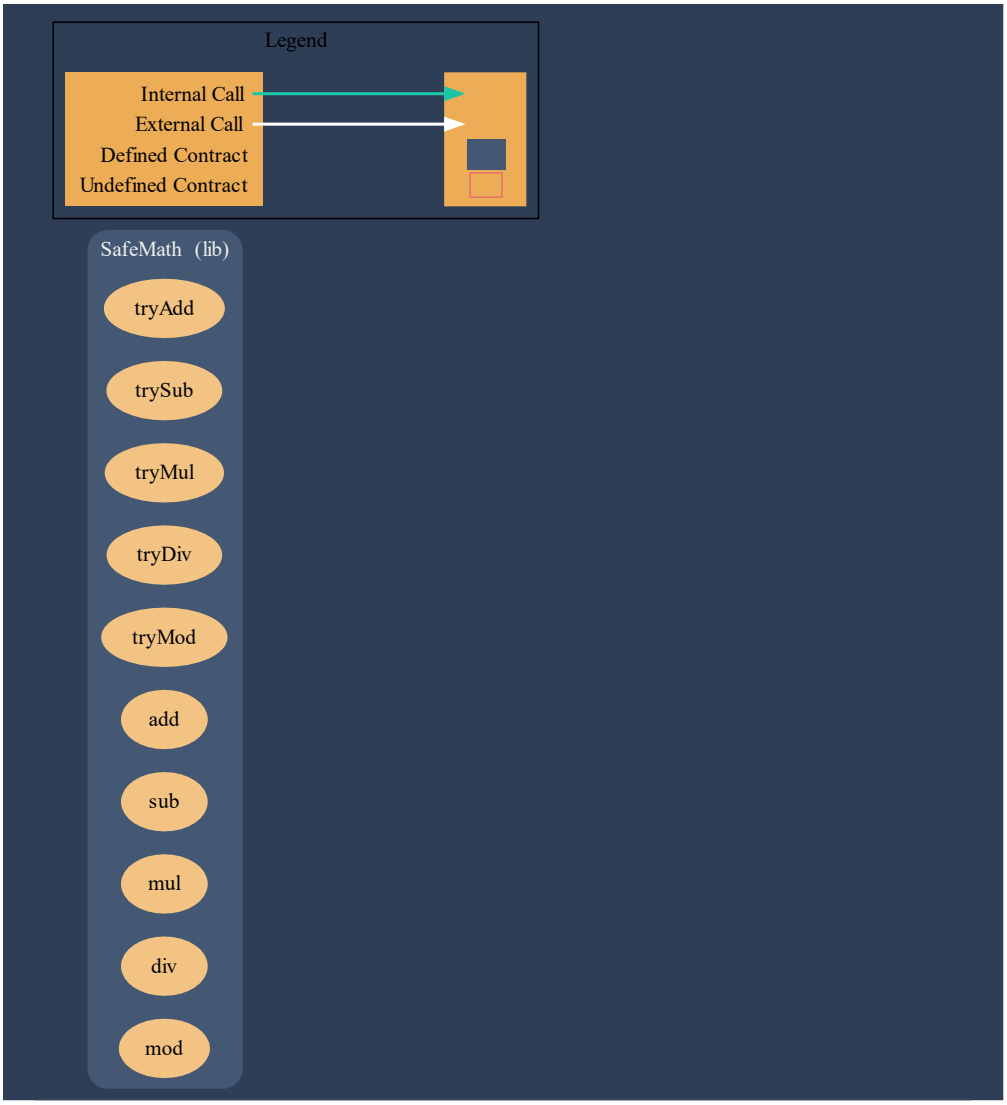
Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Call Graph for SafeMath and Bumblebee Token



Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

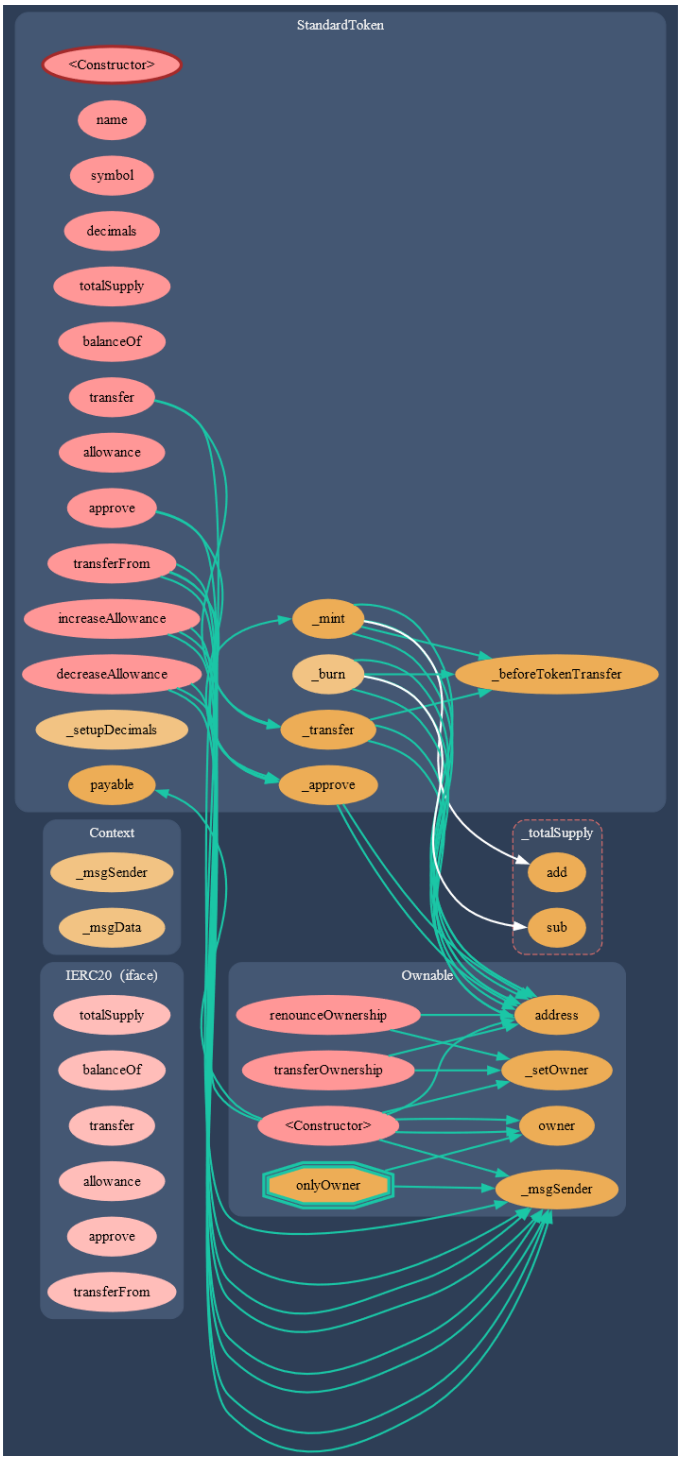
Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Call Graph for Bumblebee Token



Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

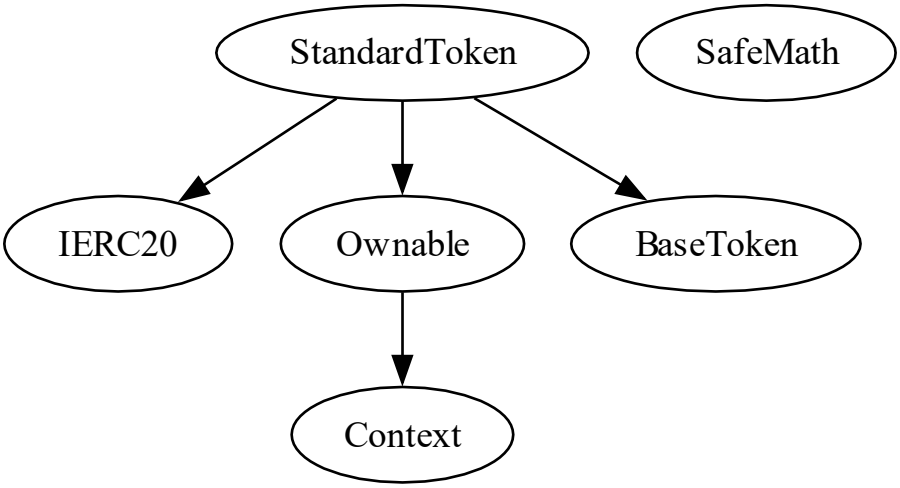
Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Inheritance Graph for Bumblebee Token



Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Summary of Recommendations

The Bumblebee Token is an ERC20 token and it satisfies the necessary properties of ERC20 tokens. These include constant total supply, correct user balances, the ability to set allowances, the prevention of transfers to the zero address, and the ability to burn tokens. The fulfillment of these properties ensures the token's security and functionality. Truscova recommends that Bumblebee Token team address the following for future iterations:

- Develop a detailed incident response plan to ensure that any issues that arise can be addressed promptly and without confusion.
- Create good documentation.
- Do not use SafeMath if Solidity 0.8.0+ is being used.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309