SUPERVIP

Security Assessment

08 June 2024

TRUSCOVA

TRUSTED CODE VALIDATION

Prepared for: SUPERVIP

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 SUPERVIP 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

SUPERVIP engaged Truscova GmbH from 27th May 2024 till 10th June 2024 to review and audit the code base provided via online deployed contract available at following address:

0x8526475Ca1802B0093F4DEa17749a577aeA17029

The scope of audit is limited to the following:

- SPVToken

One security expert at Truscova audited the above code base using formal verification, static analysis, fuzzing, proprietary Truscova Tools, 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*
High	1
Informational	1

Vulnerability Categorization

Category	*Count*
Arithmetic	1
Missing code	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**
28th March, 2024	First Contact
27th May, 2024	Contract Agreement
27th May, 2024	Assessment Start
08th June, 2024	Assessment Complete
09th June, 2024	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 SUPERVIP token SPV 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?
- Are there any centralization risks?

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:

SUPERVIP SPV Token

1. Contract 0x8526475Ca1802B0093F4DEa17749a577aeA17029

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:

SPV Token

The SPVToken contract is an ERC20 compliant token that incorporates additional features such as fee mechanisms for transactions, token minting, and integration with the Uniswap decentralized exchange. The contract is designed with the following functionalities:

Token Details:

- Name: SUPERVIP
- Symbol: SPV
- Max Supply: 21,000,000 SPV tokens

Dependencies:

- Inherits functionalities from OpenZeppelin's ERC20, Ownable, and ERC20Burnable contracts.
- Utilizes Uniswap interfaces for liquidity pool management.

Key Variables:

- uniswapV2Router: Address of the Uniswap V2 Router used for creating and managing liquidity pools.
- uniswapV2Pair: Address of the Uniswap V2 Pair (liquidity pool) for SPV and USDT.
- buyFee and sellFee: Transaction fees for buying and selling tokens, expressed in basis points (1/100th of a percent).
- feeWallet: Address where transaction fees are collected.
- _isExcludedFromFees: Mapping to track accounts exempt from transaction fees.
- automatedMarketMakerPairs: Mapping to track liquidity pool pairs for automated market making.

Constructor:

- Initializes the token with a specified fee wallet and fee structure.
- Excludes the contract deployer, contract itself, and a burn address (0xdead) from transaction fees.

Fees and Exemptions:

- Allows the owner to update the buy and sell fees, with a maximum cap of 50% for each.
- Provides functions to exclude specific addresses from fees.

Minting:

- Only the owner can mint new tokens.
- The total supply cannot exceed the maximum supply cap of 21,000,000 SPV tokens.

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

Uniswap Integration:

- Allows the owner to initialize and update the Uniswap V2 Router and Pair for SPV and USDT.
- Manages automated market maker pairs, ensuring the primary liquidity pool cannot be removed.

Transaction Logic:

- Overrides the _transfer function to implement buy and sell fees.
- When transferring tokens, if the transaction involves a liquidity pool, the appropriate fee (buy or sell) is deducted and sent to the fee wallet.

Stuck Funds Recovery:

- Provides functions for the owner to withdraw any tokens or BNB accidentally sent to the contract.

Events:

- UpdateUniswapV2Router: Emitted when the Uniswap V2 Router address is updated.
- SetAutomatedMarketMakerPair: Emitted when a new automated market maker pair is set or updated.

Functions:

- **Public Functions:**
  - mint(address to, uint256 amount): Mint new tokens up to the maximum supply cap.
  - initializeRouterAndPair(address _router, address _usdt): Set up or update the Uniswap Router and Pair.
  - updateFeeWallet(address _feeWallet): Update the address where fees are collected.
  - updateFees(uint256 _buyFee, uint256 _sellFee): Update the transaction fees for buying and selling.
  - excludeFromFees(address account, bool excluded): Exclude or include an account from transaction fees.
  - setAutomatedMarketMakerPair(address pair, bool value): Manage liquidity pool pairs.
  - isExcludedFromFees(address account): Check if an account is excluded from fees.
- **Internal Functions:**
  - _updateFeeWallet(address _feeWallet): Internal function to update the fee wallet address.
  - _updateFees(uint256 _buyFee, uint256 _sellFee): Internal function to update buy and sell fees.

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

- _excludeFromFees(address account, bool excluded): Internal function to manage fee exemptions.
- _setAutomatedMarketMakerPair(address pair, bool value): Internal function to set automated market maker pairs.
- _transfer(address from, address to, uint256 amount): Internal function to handle token transfers and fee deductions.

- **Helper Functions:**
  - withdrawStuck(): Withdraw any SPV tokens stuck in the contract.
  - withdrawStuckBNB(address toAddr): Withdraw any BNB stuck in the contract to a specified address.

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.
- We checked if a user can buy tokens for free or sell tokens for free.

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

Formal Verification

In this evaluation, SMTChecker, a smart contract formal verification tool, was utilized to thoroughly examine various system states and verify properties. Formal verification techniques were employed to supplement manual security reviews rather than replace them. Note that formal verification helps you understand the difference between your specification and the actual implementation. However, you still need to ensure that the specification matches your intentions and that it doesn't have any unintended effects.

The focus of our formal verification efforts was to verify the following behaviours:

- Arithmetic underflow and overflow.
- Division by zero.
- Unreachable code.
- Popping an empty array.
- Out of bounds index access.
- Insufficient funds for a transfer.

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 SPV 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

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	Missing Events for Significant Transactions	Missing code	Informational
2	Internal function "_transfer" can result in users buying/selling free SPV Tokens	Arithmetic	High

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. Missing Events for Significant Transactions

Severity: Informational	Difficulty: -
Type: Missing code	Finding ID: TCV-SPV-1
Target: SPVToken	

Description

The missing event makes it difficult to track off-chain liquidity fee changes. An event should be emitted for significant transactions calling the following functions:

```
function _updateFeeWallet(address _feeWallet) private {
        require(_feeWallet != address(0), "Zero address");
        feeWallet = _feeWallet;
    }

function _updateFees(uint256 _buyFee, uint256 _sellFee) private {
        require(_buyFee <= 5_000 && _sellFee <= 5_000, "Invalid fees"); // _buyFee and _sellFee
<= 50%
        buyFee = _buyFee;
        sellFee = _sellFee;
    }

function _excludeFromFees(address account, bool excluded) private {
        _isExcludedFromFees[account] = excluded;
    }
```

Figure 1 - Missing Events for Significant Transactions

Recommendation

We recommend emitting an event to log the update of variables in the functions in Figure 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

2. Internal function "_transfer" can result in users buying/selling free SPV Tokens

Severity: High	Difficulty: Low
Type: Arithmetic	Finding ID: TCV-SPV-2
Target: SPVToken	

Description

The SPV Token has defined an internal "_transfer" function which is never called /used. However, if it is used in future, it has to be used with very well defined parameters, i.e., buyFee, sellFee, and amount. So that the division does not round down to 0. The code excerpt for function "_transfer" is shown below:

```
if (
        !_isExcludedFromFees[from] &&
        !_isExcludedFromFees[to] &&
        automatedMarketMakerPairs[to] &&
        sellFee > 0
  ) {
        uint256 fee = (amount * sellFee) / 10000;
        transferAmount = amount - fee;
        super._transfer(from, feeWallet, fee);
} else if (
        !_isExcludedFromFees[from] &&
        !_isExcludedFromFees[to] &&
        automatedMarketMakerPairs[from] &&
        buyFee > 0
  ) {
        uint256 fee = (amount * buyFee) / 10000;
        transferAmount = amount - fee;
        super._transfer(from, feeWallet, fee);
 }
```

Figure 2 - "_transfer" can result in users buying/selling free SPV Tokens

Consider a scenario where the "_transfer" function is called with amount 30. With the current buyFee of 120, the corresponding fee will be 0.36 (3600 / 10000). However, solidity does not take care of decimals, hence, the division operation will round down 0.36 to 0. As a consequence, the fee will be 0 and the attacker can buy 30 SPV Tokens without paying any fee. The same scenario can be replayed using sellFee and smaller number of token to sell.

This highlights one of the scenarios, but more of such scenarios exist.

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

Recommendation

Please set a minimum amount a user should buy or sell and also the minimum percentage of buyFee or sellFee that the user should pay. Otherwise, a combination of both amount and fee percentage will result in users getting SPV tokens without any paying any fee.

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

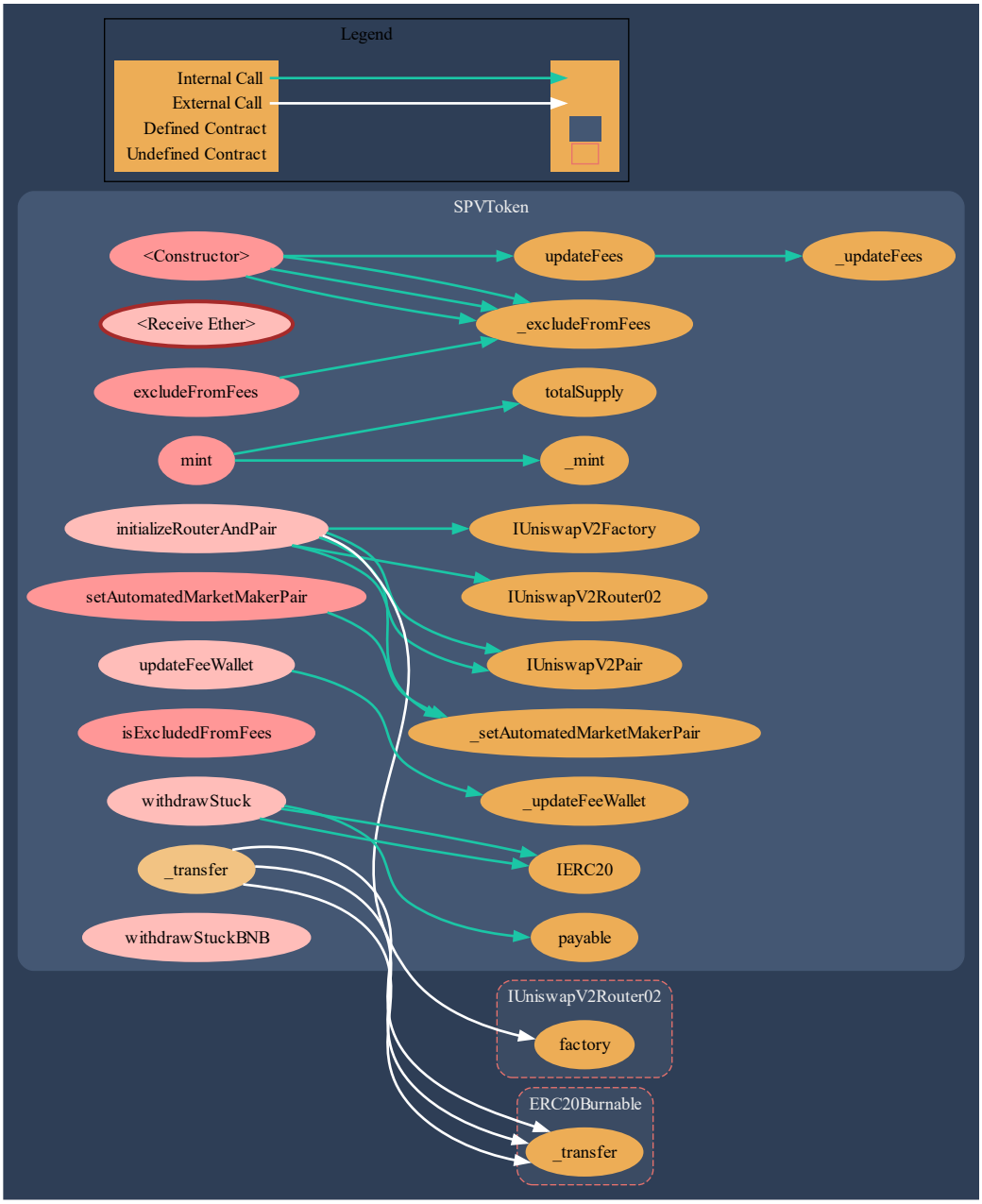
Geschäftsführung
Dr. Muhammad Hassan

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 SPV Token



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

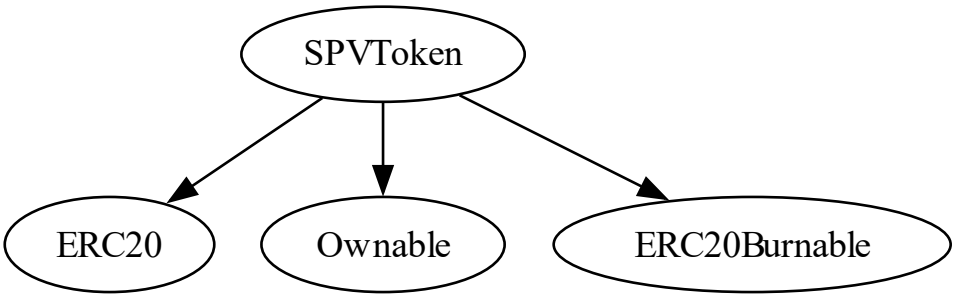
Geschäftsführung
Dr. Muhammad Hassan

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 SPV Token



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

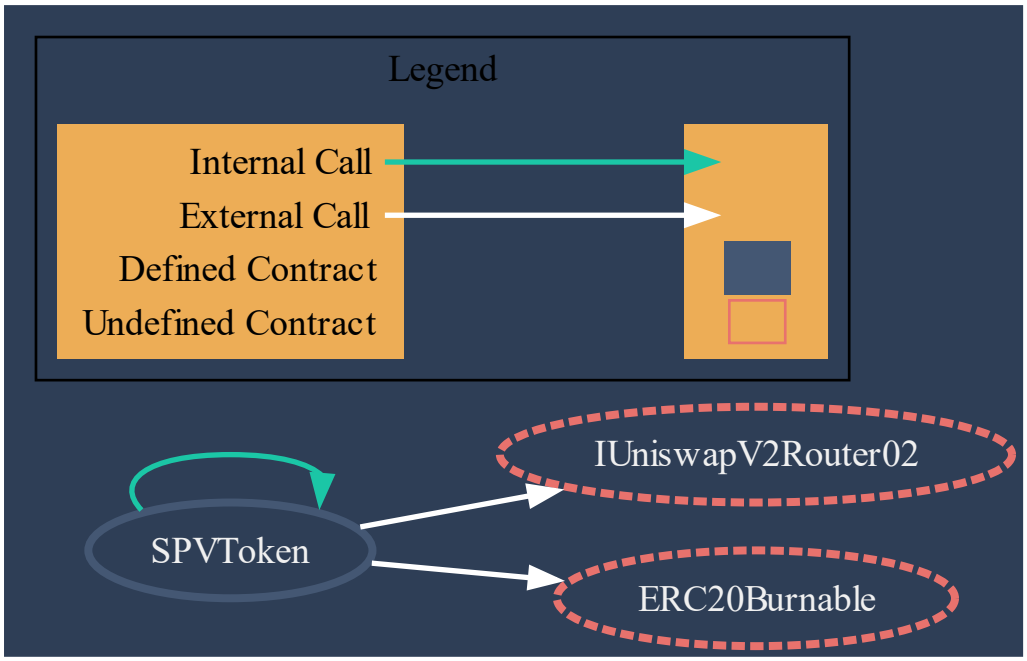
Geschäftsführung
Dr. Muhammad Hassan

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

Interaction Graph for SPV 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 SUPERVIP's SPV 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 SUPERVIP 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.

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