

USDTTRC20

Smart Contract Self-Audit Report

Version 1.0

Audit Type

Internal Self-Audit / Owner Review

Audit Date

2025

Blockchain

TRON

Contract Address

TFeTsVWHeq6hHYoaG7ACv6NLT2wZ3HAMj2

Token Standard

TRC20

1. Introduction

This document presents the results of an internal self-audit conducted on the USDTTRC20 smart contract deployed on the TRON blockchain. The purpose of this review is to assess the contract's core functionality, access control mechanisms, and common security considerations relevant to TRC20 tokens.

This audit was performed by the contract owner as an internal review and does not constitute a third-party or certified security audit. The findings are provided to support transparency and assist users, reviewers, and platforms in understanding the contract's design and behavior.

2. Scope of Review

The audit focused on the following areas:

- TRC20 token functionality
- Ownership and access control
- Supply management logic
- Transfer and allowance mechanisms
- Administrative features (pause, blacklist, fees)
- Common vulnerability checks

The audit did not include:

- Formal penetration testing
- Gas optimization analysis
- Economic or market risk evaluation
- Third-party dependency analysis

3. Contract Overview

The USDTTRC20 contract is a TRC20-compliant token implemented in Solidity using compiler version 0.8.x. The contract includes standard token operations along with administrative controls intended for operational management and emergency handling.

Key characteristics include:

- Fixed decimals (6)
- Owner-controlled administration

- Optional transaction fee logic
 - Pause and blacklist functionality
 - Minting and burning capabilities
-

4. Access Control Review

Ownership

- The contract uses a single owner model.
- Owner-only functions are protected by an `onlyOwner` modifier.
- Ownership transfer is supported and restricted to non-zero addresses.

Assessment:

Access control logic is straightforward and functions as intended.

5. Token Transfer Logic

Transfers

- Transfers validate sufficient balances.
- Transfers to the zero address are prevented.
- Optional fee calculation is applied consistently.

Allowances

- Approve, increase, and decrease allowance functions are implemented.
- `transferFrom` correctly checks balances and allowances.

Assessment:

Transfer and allowance logic follows standard TRC20 patterns and shows no immediate issues.

6. Supply Management

Issuance (Minting)

- New tokens can be issued only by the owner.
- Total supply and owner balance are updated accordingly.
- Relevant events are emitted.

Redemption (Burning)

- Token burning is restricted to the owner.
- Supply reduction is correctly reflected in total supply and balances.

Assessment:

Supply changes are centralized but transparent and traceable on-chain.

7. Administrative Controls

Pause / Unpause

- Transfers can be paused by the owner.
- Useful for emergency situations.
- Pause status is clearly enforced.

Blacklist

- Addresses can be added or removed from a blacklist.

- Blacklisted addresses are prevented from transferring tokens.
- Blacklisted funds can be destroyed if required.

Assessment:

These features increase control but also introduce centralization risk, which is disclosed.

8. Fee Mechanism Review

- Fees are calculated using basis points.
- A maximum fee cap is enforced.
- Fees, when applied, are credited to the owner address.

Assessment:

Fee logic is simple, capped, and predictable.

9. Security Considerations

Arithmetic Safety

- Solidity 0.8.x provides built-in overflow and underflow protection.
- No external math libraries are required.

Reentrancy

- No external contract calls are present in critical functions.
- Reentrancy risk is considered low.

Event Logging

- All major state-changing actions emit events.

- Enhances transparency and auditability.
-

10. Known Limitations & Risks

- The contract is centrally managed by a single owner.
- Administrative functions require trust in the owner.
- No automatic decentralization or governance mechanisms are implemented.
- Market and liquidity risks are outside the scope of this audit.

Users should evaluate these factors independently before interacting with the token.

11. Conclusion

Based on this internal self-audit, the USDTTRC20 smart contract demonstrates expected behavior for a TRC20 token with administrative controls. No critical security vulnerabilities were identified during this review.

This report reflects an internal assessment only and does not replace a professional third-party security audit. Future independent audits are recommended as the project evolves.

12. Disclaimer

This self-audit report is provided for informational purposes only. It does not guarantee the absence of vulnerabilities and should not be interpreted as a certification or endorsement of the contract's security.