



Smart Contract Audit Report

TRON

TronBank Project

V 1.0

SC.adbee5f41395



Nov. 23rd, 2025

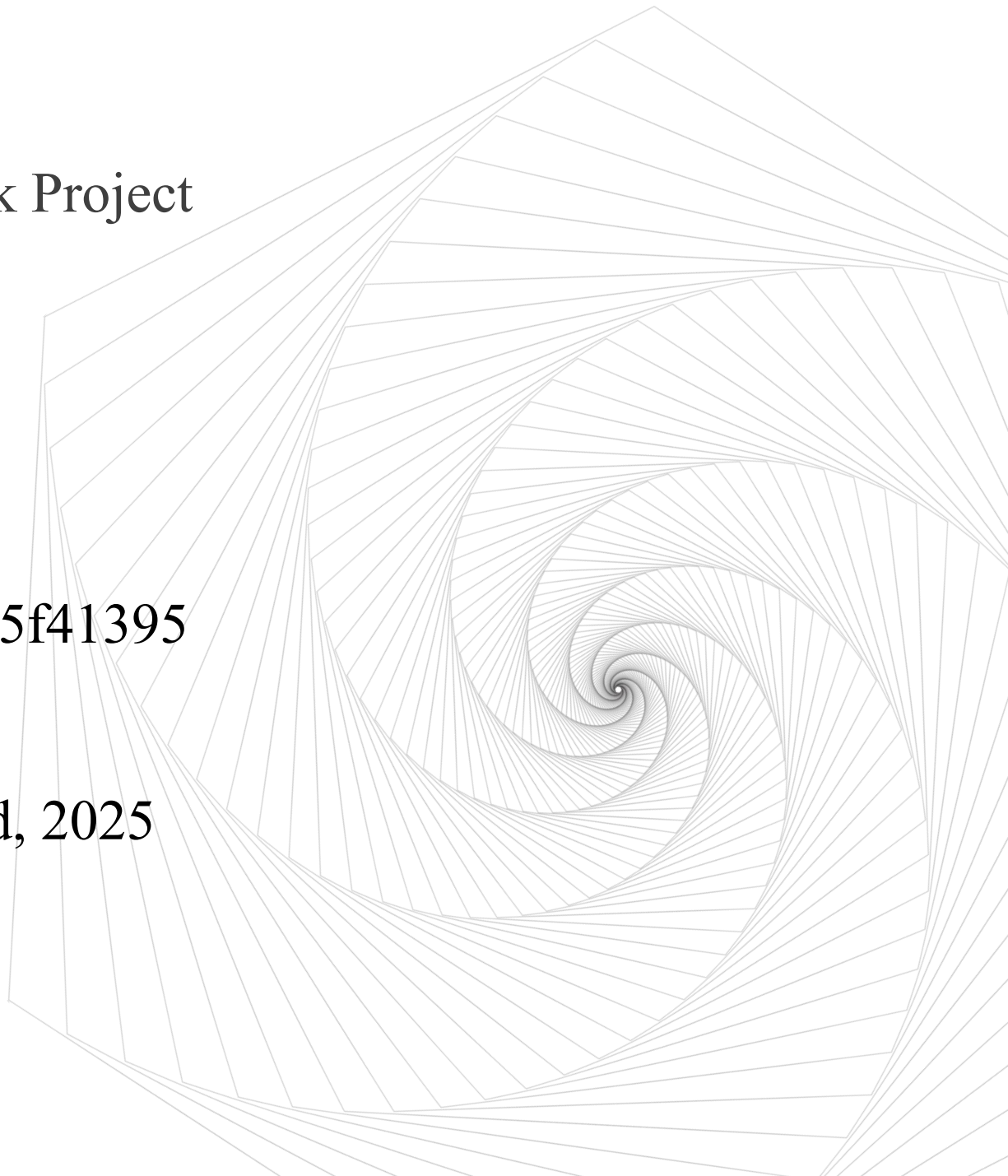


Table Of Content

1 Report Overview	- 2 -
2 Asset Management Security Assessment	- 3 -
3 Audit Overview	- 4 -
3.1 Project Information	- 4 -
3.2 Audit Information	- 4 -
3.3 External Visibility Analysis	- 4 -
3.4 Audit Process	- 5 -
4 Audit Categories	- 6 -
5 Security Finding Details	- 8 -
5.1 <i>Approve Function</i>	- 8 -
5.2 <i>Transfer Function</i>	- 8 -
5.3 <i>TransferFrom Function</i>	- 9 -
6 Explanation of Vulnerability Rating	- 10 -
7 Statement	- 12 -
8 About Binenet	- 13 -



1 Report Overview

Binenet security audit has identified 0 significant security issues across the TronBank smart contracts.

Contract Code	Function	Security Level	Status	Fix Result
---	---	---	---	---

***Risk Description:** No obvious security issues found based on business logic.



2 Asset Management Security Assessment

Asset Type	Function	Security Level
User Mortgage Token Assets	---	---
Users Mortgage Platform Currency Assets	---	---

***Description:** Check the management security of digital currency assets transferred by users in the contract business logic. Observe whether there are security risks that may cause the loss of customer funds, such as the digital currency assets transferred into the contract are incorrectly recorded or transferred out by mistake.

3 Audit Overview

3.1 Project Information

TronBank is a decentralized financial platform built on the TRON blockchain, featuring its native TBK (TronBank Token) as the core utility token. The project leverages the robust infrastructure of the TRON network to provide users with efficient, low-cost, and transparent financial services.

TronBank aims to revolutionize decentralized banking services on the TRON network by combining the benefits of blockchain technology with user-friendly financial solutions. The platform provides a foundation for various financial services including lending, staking, yield farming, and cross-chain operations, all powered by the TBK ecosystem. With its commitment to transparency, security, and innovation, TronBank represents a significant step forward in making decentralized finance more accessible and efficient for users worldwide, while contributing to the growth and maturation of the TRON blockchain ecosystem.

3.2 Audit Information

Project Name	TronBank
Platform	TRON
Audit Scope	TBK https://tronscan.io/#/token20/TR84L8oj3zt6NEZknUPerxZJyAALE8XNSH/code
Website	https://tronbank.pro/

3.3 External Visibility Analysis

Function	Visibility	State Change	Modifier	Payable	Description
approve	external	true	---	---	---

transfer	external	true	---	---	---
transferFrom	external	true	---	---	---

3.4 Audit Process

Audit time: November 22, 2025 - November 23 2025

Audit methods: Static Analysis, Dynamic Testing, Typical Case Testing and Manual Review.

Audit team: Binenet Security Team.



4 Audit Categories

Categories	Subitems	Status	Description
Business Security	Transfer token function	Pass	---
	Mint token and burn token vulnerability	Pass	---
	Contract logic function	Pass	---
	Mining pool deposit and withdrawal function	Pass	---
	Reasonableness of agreement amendment	Pass	---
	Functional design	Pass	---
	Dos caused by time	Pass	---
	Insecure oracles and their design	Pass	---
	Deployer private key leak hazard	Pass	---
General Vulnerability	Compiler version security	Pass	---
	Redundant code	Pass	---
	Use of safemath library	Pass	---
	Not recommended encoding	Pass	---
	Use require/assert mistakenly	Pass	---
	Fallback function safety	Pass	---
	tx.origin authentication	Pass	---
	Owner permission control	Pass	---
	Gas consumption detection	Pass	---
	Call injection attack	Pass	---
	Low-level function safety	Pass	---
	Additional token vulnerabilities	Pass	---
	Access control	Pass	---
	Numeric overflow detection	Pass	---

	Arithmetic precision error	Pass	---
	Misuse of random number detection	Pass	---
	Unsafe external call	Pass	---
	Variable override	Pass	---
	Uninitialized storage pointer	Pass	---
	Return value call validation	Pass	---
	Transaction order dependent detection	Pass	---
	Timestamp dependent attack	Pass	---
	Denial of service attack detection	Pass	---
	Fake recharge vulnerability detection	Pass	---
	Reentrancy Attack Detection	Pass	---
	Replay attack detection	Pass	---
	Reordering attack detection	Pass	---

5 Security Finding Details

5.1 Approve Function

Severity Level : Safe

Lines : TBK.sol#L58-L61

Description:

The approve() function allows a token owner to authorize a spender address to transfer tokens on their behalf up to a specified amount. The function sets the allowance mapping that tracks how many tokens the spender can transfer from the owner's balance. This enables delegated token transfers, which is essential for DeFi protocols, DEXs, and other smart contracts that need to move tokens on behalf of users. The function emits an Approval event for transparency and follows the ERC20 standard implementation.

Recommendations: ---

Status : Audited.

Fix Result: Known.

5.2 Transfer Function

Severity Level : Safe

Lines : TBK.sol#L53-L56

Description:

The transfer() function enables direct token transfers from the caller's address to a specified recipient address. It internally calls _transfer() which validates that the sender has sufficient balance, updates the balances mapping, and emits a Transfer event. This is the primary method for users to send TBK tokens to other addresses without requiring any third-party authorization. The function implements standard ERC20 transfer functionality with balance checks and event emissions for blockchain transparency.

Recommendations: ---

Status : Audited.

Fix Result: ---

5.3 TransferFrom Function

Severity Level : Safe

Lines : TBK.sol#L63-L67

Description:

The transferFrom() function allows a spender (typically a smart contract or approved address) to transfer tokens from an owner's address to a recipient address, provided that the spender has been granted sufficient allowance by the owner. The function first calls _spendAllowance() to verify and deduct the allowance, then executes the transfer. This mechanism enables automated token movements by DeFi protocols, exchanges, and other contracts that have been pre-approved by token holders, facilitating complex financial operations while maintaining user control through the allowance system.

Recommendations: ---

Status : Audited.

Fix Result: ---

6 Explanation of Vulnerability Rating

Vulnerability Rating	Rating Description
High Risk Vulnerability	Vulnerabilities that can directly cause the loss of token contracts or user funds, such as: overflow 、 reentrancy 、 false recharge , which can cause the value of tokens to be zeroed, or causing false exchanges to lose tokens, or causing losing ETH or tokens, etc; Vulnerabilities that can cause loss of ownership of token contracts, such as: access control flaws of key functions, call injection leading to access control bypass of key functions, etc; Vulnerabilities that can cause token contracts to fail to work properly, such as: denial of service vulnerabilities caused by sending ETH to malicious addresses, and denial of service vulnerabilities caused by gas exhaustion;
Medium Risk Vulnerability	High-risk vulnerabilities that require specific addresses to be triggered, such as overflow that can only be triggered by token contract owners; access control flaws of non-critical functions, logic design flaws that cannot cause direct financial losses, etc;
Low Risk Vulnerability	Vulnerabilities that are difficult to be triggered, vulnerabilities that cause limited harm after triggering, such as overflow vulnerabilities that require a large amount of ETH or tokens to be triggered, vulnerabilities that the attacker cannot directly profit after triggering overflow, and transaction sequence-dependent risks

	triggered by specifying high gas wait;
--	--



7 Statement

Binenet only issues this report based on the facts that have occurred or existed before the issue of this report, and assumes corresponding responsibilities for it. For the facts that occurred or existed after the issuance, we cannot judge the security status of the smart contract , and we will not be responsible for it.

This report does not include external contract calls , new types of attacks that may appear in the future, and contract upgrades or tampered codes (with the development of the project side, smart contracts may add new pools, new functional modules, new external contract calls, etc.), does not include front-end security and server security.

The documents and materials provided to us by the information provider as of the date of this report.

Binenet assumes that there is no missing, tampered, deleted or concealed information provided. If the information provided is missing, tampered, deleted, concealed or reflected inconsistent with the actual situation, Binenet shall not be liable for any losses and adverse effects resulting therefrom.

8 About Binenet

Founded in June 2021, Binenet is a dedicated and pure blockchain security company, focusing on accurate, efficient and intelligent blockchain threat detection and response. Committed to providing users with professional products and dedicated services in the field of blockchain security. Business functions cover penetration testing, code auditing, emergency response, on-chain data monitoring, AML anti-money laundering, etc., covering all aspects of blockchain ecosystem security.





Official Website

<https://binenet.com>

Telegram

<https://t.me/binenetxyz>

Twitter

<https://twitter.com/binenetxyz>

E-mail

team@binenet.com