



# Smart Contract Audit



**toolsblockchain**



**info@blockchainstools.com/**



**blockchainstools.com**

**PREPARED FOR**  
**IOTRADER Token**

# Introduction

<b>Auditing Firm</b>	BlockchainTools
<b>Client Firm</b>	IOTRADER
<b>Methodology</b>	Automated Analysis, Manual Code Review
<b>Contract</b>	0xFE4c3DFDD62B5C89D69a21b9864D47970E9bd9A5
<b>Blockchain</b>	BSC Blockchain
<b>Mutability</b>	Immutable
<b>Website</b>	<a href="https://iotrader.io">https://iotrader.io</a>
<b>Telegram</b>	<a href="https://t.me/iotradersio">https://t.me/iotradersio</a>
<b>X (Twitter)</b>	<a href="https://x.com/iotradersio">https://x.com/iotradersio</a>
<b>Gitbook</b>	<a href="https://github.com/iotraderofficial">https://github.com/iotraderofficial</a>
<b>Report Date</b>	19 Nov 2025

Verify the authenticity of this report on our website: <https://www.github.com/>



# EXECUTIVE SUMMARY

BlockchainTools has conducted both automated and manual analyses of the source code, reviewing it for common contract vulnerabilities and potential centralized exploits. Here's a brief audit summary:

Status	Critical	Major	Medium	Minor	Unknown
Open	0	0	0	0	0
Acknowledged	0	0	0	0	0
Resolved	0	0	1	1	0

Please be aware that smart contracts deployed on blockchains are not immune to exploits, vulnerabilities, or hacks. Blockchain and cryptographic assets rely on emerging technologies, which inherently carry significant risks.

- For a comprehensive understanding of risk severity, source code vulnerabilities, and audit limitations, we recommend reviewing the audit report thoroughly.

- Additionally, centralization privileges—regardless of their inherent risk level—can significantly impact the safety and security of smart contracts.



# TABLE OF CONTENTS

TABLE OF CONTENTS	0
SCOPE OF WORK	0
AUDIT METHODOLOGY	0
RISK CATEGORIES	0
METADATA ANALYSIS	0
MANUAL ANALYSIS	0
DISCLAIMERS	0
ABOUT US	0

BlockchainTools  BlockchainTools  BlockchainTools 



SMART CONTRACT AUDIT OF IOTRADER TOKEN CONTRACT

# SCOPE OF WORK

- BlockchainTools was consulted by IOTRADER to conduct the smart contract audit of their source codes. The audit scope of work is strictly limited to mentioned token only:
- 0xFE4c3DFDD62B5C89D69a21b9864D47970E9bd9A5
- If source codes are not deployed on the main net, they can be modified or altered before main-net deployment. Verify the contract's deployment status below:
- Token Link

<https://bscscan.com/address/0xFE4c3DFDD62B5C89D69a21b9864D47970E9bd9A5>

Token Name	<b>IOTRADER</b>
Owner Program	0xFE4c3DFDD62B5C89D69a21b9864D47970E9bd9A5
Current Supply	1B Token
Decimals	18
Token Extensions	False



# AUDIT METHODOLOGY

## Smart Contract Auditing Process on BSC Blockchain

Smart contract audits on the BSC blockchain follow a structured methodology to ensure security, efficiency, and compliance with best practices. Mutual collaboration is essential for an effective audit. Below is an overview of IOTRADER's auditing process and methodology for SOLIDITY-based smart contracts:

### CONNECT

- The onboarding team gathers SOLIDITY language source code and contract specifications to understand the scope and complexity of the audit.

### AUDIT

- *Automated Analysis:*
  - Performed using specialized tools to detect vulnerabilities in SOLIDITY-based smart contracts.
  - Common tools and frameworks include:
    - BSC SOLIDITY Analyzer (for contract structure and security checks)
    - SWC Vulnerabilities Registry (for identifying known smart contract weaknesses)
    - Formal Verification Tools (to ensure secure execution and prevent logical errors)
- **Simulation & Stress Testing:**
  - Transaction simulations are executed to detect centralization risks, reentrancy attacks, and state inconsistencies.
  - Testing is conducted to identify potential execution failures and trade lock risks on BSC object-based model.
- **Manual Code Review:**
  - A line-by-line inspection is performed to detect vulnerabilities related to object ownership, access control, and transaction dependencies.
  - The audit specifically reviews risks associated with:
    - SOLIDITY module permissions (ensuring no unauthorized access)
    - Object mutability risks (to prevent unintended changes)
    - Storage and gas optimization (to enhance efficiency and cost-effectiveness)



## **REPORT**

The auditing team prepares a preliminary report detailing all performed checks and identified findings.

The client's development team reviews the report and implements necessary amendments to the SOLIDITY source code.

After revisions, the auditing team delivers a final comprehensive report, highlighting any open or unresolved issues.

## **PUBLISH**

The client can choose to use the audit report internally or make it publicly available.

**Note:** Smart contract audits on the BSC blockchain do not have a pass or fail status. Instead, they serve as an objective assessment of the security and robustness of the source code.



# RISK CATEGORIES

Smart contracts are primarily designed to hold, approve, and transfer tokens, making them attractive targets for attackers.

**External Attacks:** A successful attack from an external entity may result in direct exploitation of the contract.

**Centralization Exploits:** If centralization risks exist, a privileged role may have the ability to manipulate the contract for personal gain.

All identified risks in the audit report are categorized below for reference and further review.

Risk Type	Definition
Critical	These risks could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away
Major	These risks are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to high-risk severity.
Medium	These risks should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. Low-risk re-entrancy-related vulnerabilities should be fixed to deter exploits.
Minor	These risks do not pose a considerable risk to the contract or those who interact with it. They are code-style violations and deviations from standard practices. They should be highlighted and fixed nonetheless.
Unknown	These risks pose uncertain severity to the contract or those who interact with it. They should be fixed immediately to mitigate the risk uncertainty.



# METADATA ANALYSIS

Metadata analysis on the BSC blockchain involves examining the SOLIDITY-based metadata structure of assets. Key attributes include object ownership, creator details, access controls, and linked multimedia files. This process ensures authenticity, integrity, and compliance with BSC decentralized standards. It helps detect unauthorized modifications or security risks in asset management. By verifying metadata, we enhance transparency and trust in BSC-based digital assets.

## Key Attributes Analyzed

*Object Ownership* – Tracks the ownership of assets.

*Creator Details* – Verifies the creator's identity.

*Access Controls* – Ensures appropriate permissions for asset modification and transactions.

*Multimedia Files* – Validates linked digital content (images, videos).

*Minting & Transaction Details* – Confirms compliance with minting and transaction rules.

## Conclusion

The analysis ensures that assets on the BSC blockchain are secure, comply with decentralization standards, and maintain transparency, enhancing trust and integrity within the ecosystem.



# DEFINITION

Record Type	Identifies the type of record within the BSC blockchain structure (e.g., asset, token, etc.).
UpdateAuthority	Account authorized to update the asset's metadata.
Mint	Represents the account responsible for creating this token or asset.
Data	Contains specific details and attributes about the asset or token.
Name	The name associated with this asset or token.
Symbol	Trading symbol of this asset or token.
URI	A link to external information related to the asset, typically hosted on IPFS or another decentralized storage solution
SellerFeeBasisPoints	The sales fee for this token or asset, measured in basis points.
PrimarySaleHappened	Indicates whether this asset or token has been sold for the first time.
IsMutable	Specifies if metadata can be modified after creation. Once set to False, metadata cannot be changed again.
EditionNonce	An optional field used to distinguish different editions of the token or asset.
TokenStandard	Defines the compliance standard of the token
Description	A textual description of the token or asset, often providing additional context or details.
Image	A link to an image or visual representation of the asset



# KEY INFORMATION

## **CreateAccount transaction**

<https://bscscan.com/address/0xFE4c3DFDD62B5C89D69a21b9864D47970E9bd9A5>

## **totalSupply**

1 Billion

## **New mintTokens authority**

NULL

## **New freezeAccount authority**

NULL

## **isMutable**

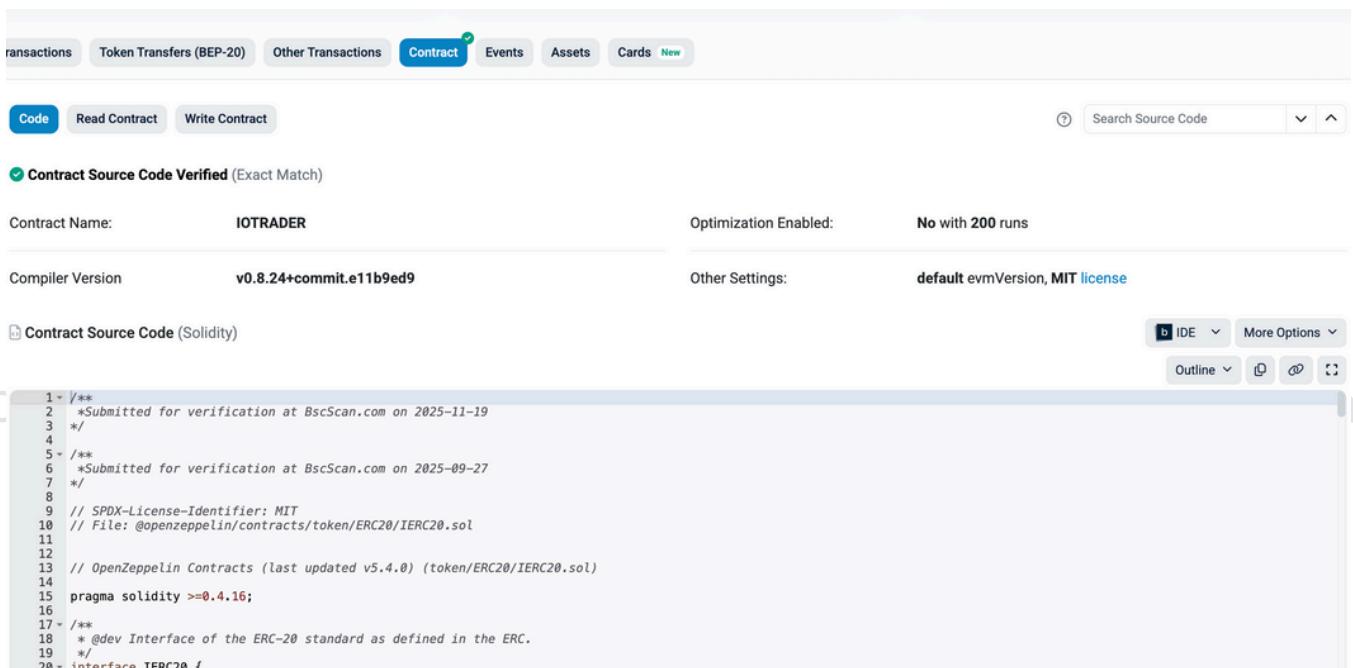
0



# MANUAL REVIEW

Identifier	Definition	Severity
CEN-02	Initial token distribution	Medium

Centralized role holds substantial portion of the circulating supply. Large number of tokens in one address raises significant concerns about centralization within the token's ecosystem.



The screenshot shows a smart contract audit interface. At the top, there are tabs for 'Transactions', 'Token Transfers (BEP-20)', 'Other Transactions', 'Contract' (which is selected), 'Events', 'Assets', 'Cards', and 'New'. Below the tabs, there are buttons for 'Code', 'Read Contract', and 'Write Contract'. A search bar says 'Search Source Code'. The main area displays contract details: 'Contract Name: IOTRADER', 'Optimization Enabled: No with 200 runs', 'Compiler Version: v0.8.24+commit.e11b9ed9', and 'Other Settings: default evmVersion, MIT license'. Below this, the 'Contract Source Code (Solidity)' tab is selected, showing the following Solidity code:

```
1 // SPDX-License-Identifier: MIT
2 // File: @openzeppelin/contracts/token/ERC20/IERC20.sol
3 
4 /**
5  *Submitted for verification at BscScan.com on 2025-11-19
6  */
7 
8 
9 // OpenZeppelin Contracts (last updated v5.4.0) (token/ERC20/IERC20.sol)
10 pragma solidity >=0.4.16;
11 
12 
13 /**
14  * @dev Interface of the ERC-20 standard as defined in the ERC.
15  */
16 
17 /**
18  * @dev Interface of the ERC-20 standard as defined in the ERC.
19  */
20 interface IERC20 {
```

## RECOMMENDATION

Project must communicate with stakeholders and obtain the community consensus while distributing tokens.

## RESOLUTION

IOTRADER team will distribute tokens as per their pre-determined tokenomics.



# DISCLAIMERS

BlockchainTools provides an easy-to-understand audit of blockchain source codes (commonly known as smart contracts). The smart contract for this particular audit was analyzed for common contract vulnerabilities and centralization exploits. This audit report makes no statements or warranties on the security of the code.

This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model, or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks.

Cryptographic tokens are emergent technologies, and they carry high levels of technical risks and uncertainty. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. This audit report could include false positives, false negatives, and other unpredictable results.

## CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer, and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without BlockchainTools' prior written consent.

## NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service, or any other assets. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice, and you should not treat any of the report's content as such. This audit report should not be used in any way.



To make decisions around investment or involvement, this report in no way provides investment advice, nor should it be leveraged as investment advice of any sort. FOR AVOIDANCE OF DOUBT, services, including any associated audit reports or materials, shall not be considered or relied upon as any form of financial, tax, legal, regulatory, or other advice.

## **TECHNICAL DISCLAIMER**

All services, audit reports, smart contract audits, other materials, or any products or results of the use thereof are provided "as is" and "as available" and with all faults and defects without warranty of any kind. To the maximum extent permitted under applicable law, BlockchainTools hereby disclaims all warranties, whether expressed, implied, statutory, or otherwise with respect to services, audit reports, or other materials. Without limiting the foregoing, BlockchainTools specifically disclaims all implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, and all warranties arising from the course of dealing, usage, or trade practice.

Without limiting the foregoing, BlockchainTools makes no warranty of any kind that all services, audit reports, smart contract audits, or other materials, or any products or results of the use thereof, will meet the client's or any other individual's requirements, achieve any intended result, be compatible or work with any software, system, or other services, or be secure, accurate, complete, free of harmful code, or error-free.

## **TIMELINESS OF CONTENT**

The content contained in this audit report is subject to change without any prior notice. BlockchainTools does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.



# About BlockchainTools

BlockchainTools provides intelligent blockchain solutions. We specialize in smart contract development, testing, and auditing services. With over 150+ solidity codes developed, 1000+ smart contracts audited, and over 500,000+ lines of code analyzed, we have extensive experience working on major public blockchains such as Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Velas, Oasis, and more.

BlockchainTools is built by engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 4 core members, along with 6+ casual contributors.





**toolsblockchain**



**info@blockchainstools.com/**



**blockchainstools.com**