

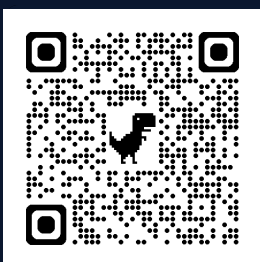


SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Kohenoor
\$KEN

21/11/2025



AUDIT REPORT

TOKEN OVERVIEW

Fees

- Buy fees: 0%
- Sell fees: 0%

Fees privileges

- Can't change fees

Ownership

- Owned

Minting

- Mint function not detected

Max Tx Amount / Max Wallet Amount

- Can't change max tx amount and / or max wallet amount

Blacklist

- Blacklist function not detected

Other privileges

- N/A
-

TABLE OF CONTENTS

1

DISCLAIMER

2

INTRODUCTION

3

WEBSITE + SOCIALS

4-5

AUDIT OVERVIEW

6-7

OWNER PRIVILEGES & FINDINGS

8

CONCLUSION AND ANALYSIS

9

TOKEN DETAILS

10

KEN TOKEN ANALYTICS &
TOP 10 TOKEN HOLDERS

11

TECHNICAL DISCLAIMER



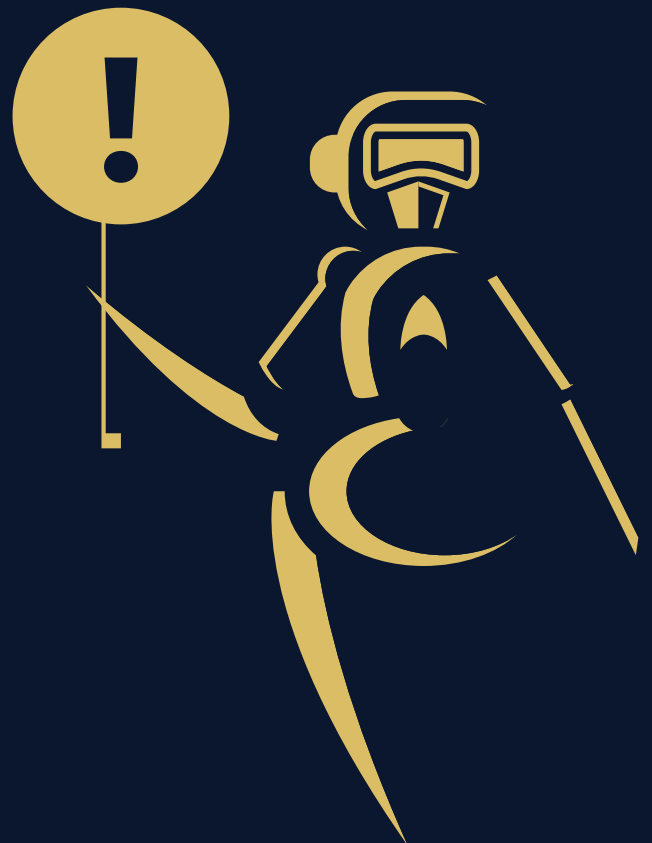
DISCLAIMER

The information provided on this analysis document is only for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results of this audit.

The score and the result will stay on this project page information on our website <https://freshcoins.io>

FreshCoins Team does not guarantees that a project will not sell off team supply, or any other scam strategy (RUG or Honeypot etc)



INTRODUCTION

FreshCoins (Consultant) was contracted by **Kohenoor** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x5f602133653237f362eb69826ba8237f4f7ab0c3

Network: **Ethereum (ETH)**

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on **21/11/2025**



WEBSITE DIAGNOSTIC

<https://www.kohenoor.tech/>



0-49



50-89



90-100



Performance



Accessibility



Best
Practices



SEO



Progressive
Web App

Socials



X (Twitter)

<https://x.com/kohenoortoken>



Telegram

<https://t.me/kohenoortech>

AUDIT OVERVIEW



Security Score



Static Scan

Automatic scanning for common vulnerabilities



ERC Scan

Automatic checks for ERC's conformance



High



Medium



Low



Optimizations



Informational



No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Low
3	Front running	Low
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Passed
8	Methods execution permissions	Passed
9	Exchange rate impact	Passed
10	Malicious Event	Passed
11	Scoping and Declarations	Passed
12	Uninitialized storage pointers	Passed
13	Design Logic	Passed
14	Safe Zeppelin module	Passed

OWNER PRIVILEGES & FINDINGS

- **Constructor Option B is commented but still present in source**

Having two constructors (one active, one commented) can confuse auditors and tools. Some verification pipelines will flag the commented code.

Remove the commented Option B entirely before verification and final deployment.

- **SafeERC20 is imported and used but OpenZeppelin 5.x already makes ERC20 operations safe**

In OZ 5.x, `ERC20.transfer` / `transferFrom` revert on failure, so `SafeERC20` is redundant overhead (~few hundred gas).

You can remove using `SafeERC20` for `IERC20`; and the import, and just use `IERC20(token).transfer(to, amount);`. Keeps bytecode slightly smaller.

Recommendation:

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. The risk can be prevented by temporarily locking the contract or renouncing ownership.



CONCLUSION AND ANALYSIS



Smart Contracts within the scope were manually reviewed and analyzed with static tools.



Audit report overview contains all found security vulnerabilities and other issues in the reviewed code.



Found no HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	0%
Sell fees:	0%
Max TX:	N/A
Max Sell:	N/A

Honeypot Risk

Ownership:	Owned
Blacklist:	Not detected
Modify Max TX:	Not detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

Rug Pull Risk

Liquidity:	N/A
Holders:	Clean



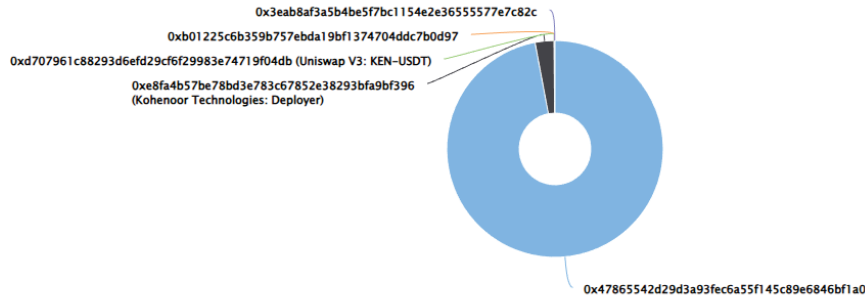
KEN TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (101,964.69 Tokens) of Kohenoor

Token Total Supply: 101,966.00 Token | Total Token Holders: 14

Kohenoor Top 10 Token Holders

Source: Etherscan.io



(A total of 101,964.69 tokens held by the top 10 accounts from the total supply of 101,966.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x47865542...6846Bf1A0	98,962.1	97.0540%
2	Kohenoor Technologies: Deployer	2,872.116242734491857542	2.8167%
3	Uniswap V3: KEN-USDT	42.358017721594309569	0.0415%
4	0xB01225C6...dDC7b0d97	39.734307894605442714	0.0390%
5	0x3eaB8aF3...577e7c82C	16	0.0157%
6	0x40c70213...5Cb27d1A4	15.000000000000000015	0.0147%
7	0xA78816D6...2176c2ffC	9.3	0.0091%
8	0xD6af3984...918b83085	5	0.0049%
9	Uniswap V4: Pool Manager	1.584071416187690684	0.0016%
10	0x587c3c75...13833F60f	1.5	0.0015%

TECHNICAL DISCLAIMER

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. The audit can't guarantee the explicit security of the audited project / smart contract.

