

X AUDITR




**SMART CONTRACT SECURITY
AUDIT REPORT**

X AUDITR

Audit Summary

This audit report provides a comprehensive review of the OEDNFTMarketplace smart contract. The primary goal of this audit is to evaluate the contract's security, functionality, and adherence to best practices in Solidity development. The contract implements an ERC-721-based NFT marketplace with a unique minting mechanism and pricing structure

- 
- ☐ **Contract name :** OEDNFTMarketplace
 - ☐ **Blockchain Platform :** Base network
 - ☐ **Solidity Version :** 0.8.20
 - ☐ **Libraries Used :** OpenZeppelin (ERC721Enumerable, Ownable, ReentrancyGuard)
 - ☐ **Functionality :** NFT minting, listing, purchasing, and resale
 - ☐ **Audit Areas :** Security, functionality, efficiency, and best practices

Smart Contract Overview

The contract consists of the following key components

- **NFT Minting System** only owner to mint NFTs based on a year-based pricing model.
- **NFT Metadata Storage** Each NFT has associated metadata (name, description, image, listing status)
- **Marketplace Mechanism** NFTs can be resold
- **Ownership & Access Control** The contract uses OpenZeppelin's Ownable module for admin privileges
- **Security Measures:** Implements ReentrancyGuard to prevent reentrancy attacks

The logo features a stylized 'X' composed of four overlapping, semi-transparent shapes in green, blue, and purple. Below the 'X' is the word 'AUDITR' in a bold, green, sans-serif font.

X AUDITR

Smart Contract Analysis

1 Minting Mechanism

✓ Minting Conditions

- Minting is only allowed from **2025 to 2135**.
- A maximum of **21 NFTs** can be minted.
- The minting price follows a structured increase over time.

✓ Pricing System

- **2025 - 2034** Price starts at **0.5 ETH** and increases by **0.5 ETH per year**.
- **2035** Fixed price of **6 ETH**
- **2045 - 2125** Increases by **1 ETH** per decade.
- **2135** Final price of **21.5 ETH**.

2 Marketplace Mechanism

✓ Resale System

- NFT owners can list their NFTs with a custom price
- The contract updates the metadata and marks the NFT as listed

✓ Purchase System

- Buyers must send the exact ETH amount to purchase an NFT.
- The NFT is transferred to the new owner
- OED Market owner receives the ETH payment.
- The event NFTResold is emitted

Security Analysis

✓ Common Vulnerability Checks

- | | |
|--|----------|
| 1. Compiler errors | ✓ passed |
| 2. Race conditions and Reentrancy (Cross-function race conditions) | ✓ passed |
| 3. Possible delays in data delivery | ✓ passed |
| 4. Oracle calls | ✓ passed |
| 5. Front running | ✓ passed |
| 6. Timestamp dependence | ✓ passed |
| 7. Integer Overflow and Underflow | ✓ passed |
| 8. DoS with Revert | ✓ passed |
| 9. DoS with block gas limit | ✓ passed |
| 10. Methods execution permissions | ✓ passed |
| 11. Economy model of the contract | ✓ passed |
| 12. Malicious Event log | ✓ passed |
| 13. Scoping and Declarations | ✓ passed |
| 14. Arithmetic accuracy | ✓ passed |
| 15. Design Logic | ✓ passed |
| 16. Cross-function race conditions | ✓ passed |
| 17. Safe Openzeppelin contracts implementation and usege | ✓ passed |

OVERALL RATING 9/10

Passed ✓