X AUDITR

SMART CONTRACT SECURITY AUDIT REPORT

OED Smart Contract Audit Report

- ☐ **Contract Address:** 0x5bf28FC94f1Ad269dbAC0aA2A205c5C0A5eEfe0C
- ☐ **Contract name :** OneEveryDecade
- ☐ **Token Name:** One Every Decade
- ☐ **Token Symbol:** OED
- ☐ **Token Decimals:** 8
- ☐ **Total SUPPLY:** 21 OED
- ☐ **Minting Mechanism:** New tokens are minted every 10 years until the total supply reaches 21 OED.
- ☐ **Liquidity Management:** Auto-liquidity feature via Uniswap V2.
- ☐ **Fee Structure:** Various fees for transactions, including reflections and buyback mechanisms.
- ☐ **Security Measures:** Implements OpenZeppelin's Ownable and ReentrancyGuard to secure ownership and prevent reentrancy attacks.

Libraries & Dependencies

The contract imports the following external libraries

OpenZeppelin Contracts

- `ERC20` Standard ERC20 token functionality.
- `Ownable` Restricts sensitive functions to the contract owner.
- `ReentrancyGuard` Prevents reentrancy attacks.

Uniswap V2 Interfaces

- `IUniswapV2Router02` Handles token swaps and liquidity additions.
- `IUniswapV2Factory` Creates the liquidity pair for OED and WETH.

Tokenomics & Minting Mechanism

- **Initial Supply** 10 OED tokens are minted upon deployment.
- **Max Supply**: 21 OED (21 * 10^8 units).

Minting Schedule

- Tokens are minted every 10 years (`MINT_INTERVAL = 10 years`).
- Each minting event adds 1 OED (10^8 units) to the supply.
- The contract ensures that minting stops once the total supply reaches 21 OED.
- Minting occurs via the `mint()` function, which is protected by `nonReentrant`.

Transaction Fee Structure

The contract applies fees on transfers unless the sender or recipient is exempt.

Fee Breakdown

- **BTEG Buy-Burn Fee**: 50% of the collected fees (used to buy back and burn BTEG tokens).
- **Holder Reflection Fee** 50% of the collected fees (distributed among OED holders).

Final Fee Distribution (Total = 2%)

Fee Type	Calculation	Final % of Transaction Amount	Where It Goes
Liquidity Fee	`50% of 2%`	**1%**	Sent to contract (for liquidity)
BTEG Buy & Burn Fee	`50% of 2%`	**1%**	Used for `_buyBackBTEG()`
Total Deducted	`2%` of amount	**2%**	Distributed among liquidity & buyback

Liquidity & Trading Mechanisms

Liquidity Addition

- The contract maintains liquidity via _addLiquidity(), which pairs OED with WETH and adds liquidity to Uniswap.
- The function ensures that at least half of the minted tokens are used for liquidity.

Buyback Mechanism

- `_buyBackBTEG()` swaps OED for WETH and then buys BTEG tokens to be burned.
- This ensures a deflationary mechanism for BTEG while supporting OED's ecosystem.

Reflection Mechanism

- The `_distributeReflections()` function rewards OED holders who hold more than **1,000,000 OED units**.
- Excludes the liquidity pool (`lpPair`) from reflections.
- Tokens are proportionally distributed based on holdings.

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.	Arithmatic accuracy	✅ passed
15.	Design Logic	✅ passed
16.	Cross-function race conditions	✅ passed
17.	Safe Openzeppelin contracts implementation and usege	✅ passed

OVARAL RATING 8.8/10 **Passed ✅**