DORA: Security Audit Report

DogScan Security Team

August 1st, 2025

Contents

DogScan Security Audit Report

Project	DORA
Chain	Binance Smart Chain (ID 56)
Contract Address	0x23fe903be385832fd7bb82bf1fee93f696278888
Audit Date	August 1st, 2025
Report Version	1.0

1. Executive Summary

We conducted a comprehensive security audit of the `DORA` token contract deployed on the Binance Smart Chain network. This contract is a standard ERC20 token implementation built upon OpenZeppelin security libraries. The audit results show that the contract **maintains excellent overall security**, with only one informational-level risk identified.

Our analysis found that the contract contains a disabled transaction control mechanism, but since contract ownership has been renounced and this mechanism has been permanently disabled, it poses no actual security threat. The contract adopts good security practices and complies with industry standards.

Overall Risk Rating: Informational

This token contract is safe for user interaction.

2. Audit Scope

The audit scope encompasses the complete `DORA` token contract system deployed on Binance Smart Chain:

Contract Information:

- Address: `0x23fe903be385832fd7bb82bf1fee93f696278888`
- Token Name: DORA
- Token Symbol: DORA
- Decimals: 18
- Total Supply: 1,000,000,000 DORA
- Maximum Supply: 1,000,000,000 DORA

Key Audit Areas:

- ERC20 standard compliance
- Access control mechanisms and ownership management
- Token transfer restrictions and transaction controls
- Liquidity pool interaction security
- Supply management and minting/burning mechanisms
- Reentrancy attack protection
- Honeypot mechanism detection
- Mathematical operation security

3. Audit Methodology

This audit employed a comprehensive multi-agent AI security analysis workflow specifically designed for smart contract security assessment:

1. Specialized Analysis Modules:

- **Access Control Specialist**: Evaluated access control and ownership management
- **Core Logic Analyst**: Reviewed token transfer and business logic implementation
- **Honeypot Detection Expert**: Examined potential sell restriction mechanisms
- **Liquidity Risk Analyst**: Assessed liquidity manipulation risks
- **Reentrancy Specialist**: Analyzed external call patterns and state management
- **Economic Model Expert**: Evaluated token supply dynamics and economic model
- **User Rights Analyst**: Assessed restrictions on user token operations
- **DeFi Mathematics Expert**: Reviewed arithmetic operations and mathematical security

2. On-chain State Analysis:

- Current contract configuration verification
- Ownership status examination
- Transaction restriction status confirmation
- Liquidity pool configuration analysis

3. Comprehensive Analysis:

- Chief Security Strategist integrates all findings
- Risk prioritization and impact assessment
- Comprehensive reporting and recommendation development

4. Findings Summary

ID	Title	Severity	Status
I-01	TransferConstraints Transaction Control Mechanism	**Informational**	**Mitigated**

5. Detailed Findings

[I-01] TransferConstraints Transaction Control Mechanism (Informational)

Severity: Informational

Description The contract contains a mechanism that controls transfers to specified Uniswap pools through a `transferConstraints` boolean flag. This mechanism can restrict token trading with Uniswap V2 and V3 pools, effectively pausing trading functionality.

Impact

- Could theoretically prevent users from trading with DEX pools
- Potential disruption of token liquidity
- May cause confusion for new users understanding contract functionality

Technical Details The contract implements transaction restriction logic in the `_beforeTokenTransfer` function:

Important Finding: On-chain state analysis reveals: 1. `transferConstraints` flag is currently **`false`** (disabled) 2. Contract ownership has been renounced (owner is zero address `0x0000000000000000000000000000000000000000`) 3. Since ownership has been renounced, the `removeTransferConstraints` function can no longer be called 4. Therefore, this transaction restriction mechanism has been **permanently disabled** and cannot be re-enabled

Code Evidence

```
function _beforeTokenTransfer(address from, address to, uint256) internal view override {
    if (transferConstraints) {
        if (from == uniswapV2Pool || to == uniswapV2Pool) {
            revert("Token: transfer to/from uniswap v2 pool is not allowed");
        }

        if (from == uniswapV3Pool || to == uniswapV3Pool) {
            revert("Token: transfer to/from uniswap v3 pool is not allowed");
        }
    }
}

function removeTransferConstraints() external override onlyOwner {
    transferConstraints = false;
}
```

Current Status Assessment

- Transaction restrictions have been disabled
- Contract ownership has been renounced
- Restriction mechanism cannot be re-enabled
- Token can trade freely

Recommendations

- **For Users**: This mechanism has been permanently disabled and does not affect normal trading
- **For Developers**: Consider removing such dormant code in future versions to avoid confusion
- **Code Cleanup**: While it doesn't affect security, removing unused code can improve code readability

6. Architecture and Design Assessment

Design Strengths

1. **Standard Libraries**: Contract built upon battle-tested OpenZeppelin contracts
2. **ERC20 Compliance**: Fully compliant with ERC20 token standard, ensuring good interoperability
3. **Ownership Renouncement**: Contract ownership has been renounced, eliminating centralized control risks

4. **Secure Supply Management**: Fixed total supply with no additional minting risks
5. **Standardized Implementation**: Adopts industry best practices

Key Architectural Features

1. **Decentralized Design**: Ownership renounced, eliminating single point of control risks
2. **Trading Freedom**: All trading restrictions have been permanently removed
3. **Liquidity Friendly**: Can freely interact with DEX pools
4. **Stable Economic Model**: Fixed supply with no inflation or deflation mechanisms

Recommended Improvements

1. **Code Cleanup**: While not affecting security, consider removing disabled transaction restriction code
2. **Documentation Enhancement**: Recommend clearly documenting ownership renouncement and transaction restriction removal in project documentation

7. Conclusion

This security audit conducted a comprehensive security assessment of the `DORA` token contract. After in-depth analysis of all security dimensions of the contract, including access control, upgrade mechanisms, liquidity management, supply economics, reentrancy attacks, honeypot detection, and user permissions, **no actual security risks were identified**.

Key Findings Summary:

- **Access Management**: Contract ownership has been renounced, eliminating centralized control risks
- **Trading Freedom**: All trading restrictions have been permanently disabled, allowing free token trading
- **Code Quality**: Based on standard OpenZeppelin libraries with high code quality
- **Economic Model**: Fixed supply design with stable economic model

Overall Risk Rating: Informational

The contract adopts good security practices and complies with industry standards. The only finding is a permanently disabled transaction control mechanism that poses no actual risk.

Security Status:

The DORA token contract maintains **excellent** security status and can be safely used by users. The contract is well-designed, standardized in implementation, and has no known security vulnerabilities.

Final Recommendation:

This token contract can be safely used for various DeFi applications and trading activities. Users can interact with it confidently.

Disclaimer

This audit report is for reference only and does not constitute investment advice. The analysis is based on smart contract source code and on-chain state provided at a specific point in time, and is not an endorsement of the project or an absolute guarantee of its security. Smart contracts have inherent risks, and blockchain technology is still evolving. Users should conduct their own research and exercise caution when interacting with any smart contract. This report reflects the contract state at the time of audit, and subsequent contract modifications or network changes may affect security status.