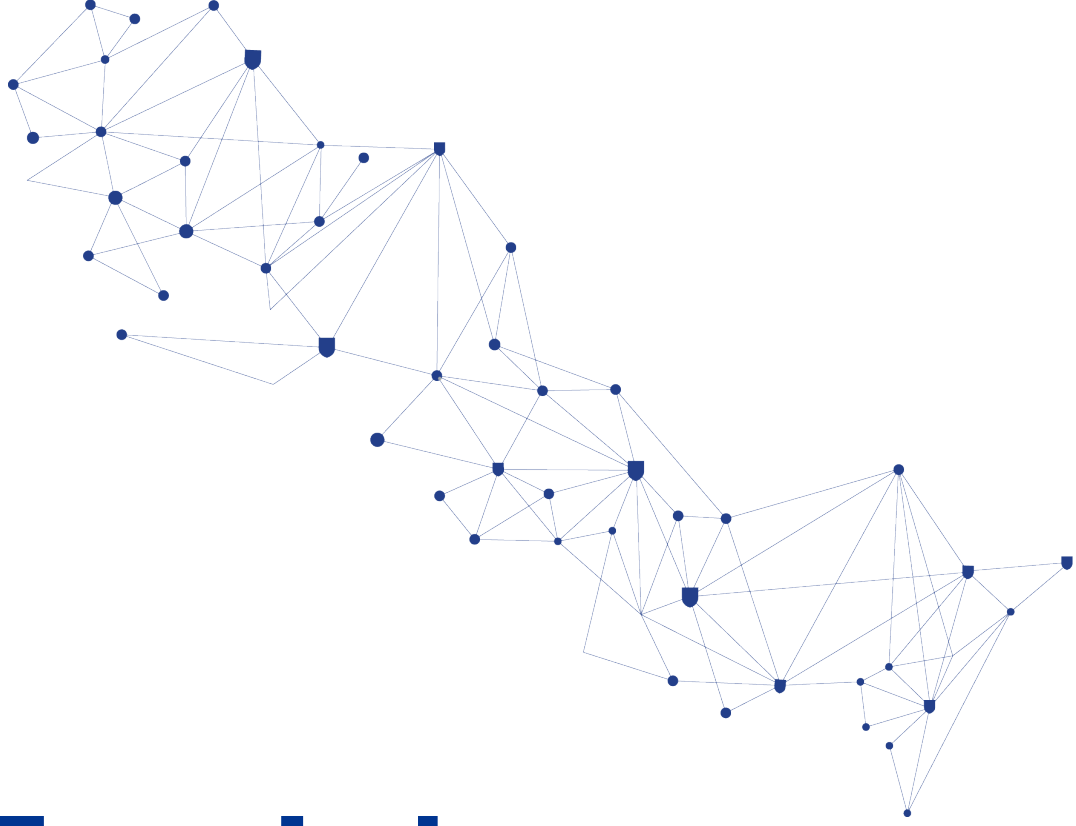


LayerZero Labs Security Audit

wXRPToken Audit for Hex Trust

Released November 3, 2025

Performed By

Carter Snay csnay@iol.unh.edu
James Kahn jkahn@iol.unh.edu
Oliver Willis owillis@iol.unh.edu

University of New Hampshire
Interoperability Labs

+1-603-862-0090 | www.iol.unh.edu

Table of Contents

1 Legal Notice 2

2 Executive Summary 3

2.1 About LayerZero Labs and wXRPToken

2.2 Review Timeline

2.3 Scope

2.3.1 Files in Scope

3 Audit Details 5

3.1 Methodology

3.1.1 Phase I: Initial Scoping

3.1.2 Phase II: Codebase Review

3.1.3 Phase III: Local Testing

3.1.4 Proof of Vulnerability

3.2 Risk Classification

4 Vulnerabilities 7

4.1 Findings Summary

4.2 Detailed Findings

4.2.1 Gas

5 The Interoperability Labs 9

1 Legal Notice

The Interoperability Labs Blockchain team makes every effort to identify as many vulnerabilities in the code as possible within the given time period but assumes no responsibility for the findings presented in this document. A security audit by the team does not constitute an endorsement of the underlying business or product. The audit was time-boxed, and the review focused solely on the security aspects of the Solidity implementation of the contracts.

2 Executive Summary

The UNH Interoperability Labs conducted a security assessment for wXRPToken from October 10, 2025 to October 14, 2025. During this assessment, the UNH Interoperability Labs reviewed the wXRPToken code for security vulnerabilities, design issues and general weaknesses.

During the assessment, no critical, high, or medium-severity vulnerabilities were identified in the analyzed smart contracts. One gas optimization is being suggested and has been acknowledged.

2.1 About LayerZero Labs and wXRPToken

LayerZero is an omnichain interoperability protocol designed to facilitate seamless messaging of arbitrary data between blockchains. It achieves this by leveraging a combination of on-chain endpoints, a decentralized network of verifiers, and executors to securely transmit messages across chains. The protocol enables cross-chain applications to maintain atomicity and composability across multiple networks.

The wXRPToken project involves the development and deployment of an upgradeable ERC-20 token with cross-chain capabilities, designed to operate within the LayerZero ecosystem. The audit scope includes three smart contracts.

The wXRPToken supports minting and burning via role-based permissions, and includes features such as pausability, blacklisting, and upgradeability through the Transparent Upgradeable Proxy (TUP) pattern. The WXRPMintBurnOFTAdapter contract enables omnichain interoperability by facilitating cross-chain token transfers using LayerZero's OFT standard. It performs mint and burn operations across chains to maintain supply consistency.

All privileged functions are strictly controlled through defined roles (e.g., Minter, Burner, Pause Admin, Blacklist Admin), ensuring secure and controlled access to sensitive operations.

2.2 Review Timeline

- **October 3, 2025**: Audit scoping document delivered; review process initiated.
- **October 9, 2025**: Security researchers accessed the GitHub repository.
- **October 10, 2025**: Manual review of the smart contracts conducted.
- **October 13, 2025**: First audit report draft delivered.
- **October 14, 2025**: Final audit report delivered.
- **November 3, 2025**: Updated repo url.

2.3 Scope

Project Name	wXRPToken for Hex Trust		
URL	`https://www.hextrust.com/`		
Language	Solidity		
Scope	Repo	`https://github.com/hextrust/wrapped-xrp`	
	Hash	~~403467905db4e377c7547eb3e2631c5ef8c0248f~~	Oct 1, 2025
		2837ed36cacda1eb9413e00795a19b8e75271267	Oct 10, 2025

2.3.1 Files in Scope

```
contracts/
├── interfaces/
│   └── IWXRPToken.sol
├── WXRPMintBurnOFTAdapter.sol
└── WXRPToken.sol
```

3 Audit Details

3.1 Methodology

The Interoperability Labs audit team follows a comprehensive methodology in ensuring the security and reliability of smart contracts and Web3 protocols. While the specific testing procedures performed vary between the project and protocol, the tooling and manual review process remains the same to ensure thorough analysis has been completed on all items within the defined scope of the audit. Throughout the security review, the audit team maintains communication with the development team, providing feedback on identified vulnerabilities and optimizations. The following sections provide an overview of our systematic audit process and methodology.

3.1.1 Phase I: Initial Scoping

- Independent review of project documentation to understand the business logic of the project.
- Identification of critical components and key areas of focus and possible areas of exploitation.
- Ensure that the project's documentation is accurate, complete, understandable, and there is alignment between the code and the documentation.
- Discussion with the development team to clarify objectives, expectations, and known issues.

3.1.2 Phase II: Codebase Review

- **Static Analysis**: Automated tools to scan for common vulnerabilities with Slither and Aderyn.
- **Manual Review**: In-depth inspection of the code by the audit team to identify issues, including unsafe coding practices from known previous exploits.
- **Function State Machine Diagramming**: Generate a flow diagram illustrating the intended transaction paths, as well as unintended and potentially exploitable paths.

3.1.3 Phase III: Local Testing

Methods:

- **Unit Testing**: Validate individual functions for correctness.
- **Integration Testing**: Ensure that different components interact as expected.

Techniques Used in This Audit:

- **Unit Testing**
- **Manual Review**
- **Function State Machine Diagramming**

3.1.4 Proof of Vulnerability

Objective: Prove how a found exploit can be executed.

Activities:

- Perform controlled attacks on a local fork of the protocol to show how an exploit can be executed.
- Test edge cases and unexpected scenarios discovered in the diagramming phase.

By following a structured and comprehensive methodology, we aim to provide actionable insights to strengthen the security and reliability of the protocol. This ensures security, resilience, and long-term success for the protocol.

3.2 Risk Classification

Impact →

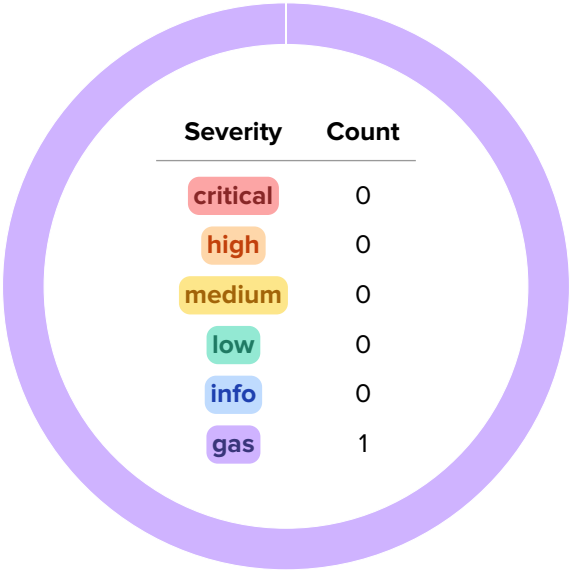
Likelihood ↓

	Informational	Low	Medium	High	Critical
Very Unlikely	Info	Low	Low	Medium	Critical
Unlikely	Info	Low	Low	Medium	Critical
Possible	Info	Low	Medium	High	Critical
Likely	Info	Low	Medium	High	Critical
Very Likely	Low	Medium	High	Critical	Critical

We use the PricewaterhouseCoopers-style matrix to provide comprehensive risk assessment. See the documentation for more details.

4 Vulnerabilities

In summary, we did not discover vulnerabilities with the files in scope, and we are communicating 1 gas suggestion.



Severity	Count
critical	0
high	0
medium	0
low	0
info	0
gas	1

4.1 Findings Summary

ID	Severity	Title	Status
G-01	gas	Change `WXRPToken.sol` constant role variables to private	ACKNOWLEDGED

4.2 Detailed Findings

4.2.1 Gas

[G-01] Change `WXRPToken.sol` constant role variables to private

Category	Target
Gas-Optimization	`WXRPToken.sol`

Description

The contract `WXRPToken.sol` contains the following role variables:

WXRPToken.sol **solidity**

```
contract WXRPToken is IWXRPToken, ERC20Upgradeable, AccessControlUpgradeable, PausableUpgradeable {
    bytes32 public constant BLACKLISTER_ROLE = keccak256("BLACKLISTER_ROLE");
    bytes32 public constant PAUSER_ROLE = keccak256("PAUSER_ROLE");
    bytes32 public constant MINTER_ROLE = keccak256("MINTER_ROLE");
    bytes32 public constant BURNER_ROLE = keccak256("BURNER_ROLE");

    ...
}
```

On deployment, the compiler will create non-payable getter functions for each of these variables. To save deployment gas, the visibility of these variables can be changed to private. Furthermore, the values themselves can be read from the contract's verified source code.

Resolution

LayerZero has acknowledged this, but has decided that publicly accessible role bytes are a feature.

5 The Interoperability Labs

The University of New Hampshire Interoperability Labs (UNH-IOL) is the foremost independent testing facility for data networking companies worldwide.

We accelerate the launch of innovative products by providing standards and compliance testing to ensure that devices meet industry standards. Whether it's traditional Ethernet or advanced technologies like 5G, blockchain, and autonomous vehicles, our services provide comprehensive testing for device interoperability, conformance, and certification.

Our state-of-the-art laboratory and 36 years of extensive experience make it a strategic resource for industry startups and Fortune 500 companies needing collaboration, innovation, and standards development to help them shape the future of networking.

Join us and become a part of a community driving the next generation of networking technology. Together, we can shape the future of networking.

https://www.iol.unh.edu/membership

University of New Hampshire Interoperability Laboratory

21 Madbury Rd., Ste 100 Durham, NH 03824-4716

+1-603-862-0090 | www.iol.unh.edu

Contact our Blockchain Team: `blockchain@iol.unh.edu`