Bitlayer: Security Audit Report

DogScan Security Team

DogScan

July 16th, 2025

Contents

DogScan Security Audit Report

Project	Bitlayer
Chain	Bitlayer (ID 200901)
Smart Contract	ERC1967Proxy
Implementation	YBTCB
Audit Date	July 16th, 2025
Report Version	1.0
Overall Risk	**Low**

1. Executive Summary

We conducted a comprehensive security audit of the YBTC.B token contract system, which consists of an ERC-1967 upgradeable proxy and its implementation contract. The audit reveals that the overall security posture of the contract system is good.

The core token logic for depositing and withdrawing assets is sound and follows best practices like the Checks-Effects-Interactions pattern to prevent reentrancy. The system employs a UUPS upgradeable proxy pattern where the upgrade mechanism is controlled by a multi-signature wallet (Gnosis Safe). This provides better security assurance compared to single account control.

2. Audit Scope

The audit scope covers the YBTC.B token contract system deployed on Chain ID 200901. The system consists of:

- **Proxy Contract**: `0x2cd3cdb3bd68eea0d3be81da707bc0c8743d7335` (ERC-1967 Proxy)
- **Implementation Contract**: `0x699c4a6982425e4b6e5f747fcc581798326ab5d3` (YBTC token logic)

The following components were analyzed:

- OpenZeppelin proxy implementation and utilities
- YBTC token contract with UUPS upgradeability
- Access control mechanisms
- Token economics and minting/burning functions

- Deposit and withdrawal mechanisms

3. Audit Methodology

This audit employed a multi-agent AI security analysis framework. The process involved a team of specialized AI agents, each designed to detect specific vulnerability classes such as reentrancy, access control flaws, honeypot mechanisms, liquidity risks, and economic exploits. The findings from these specialist agents were then synthesized and validated by a lead security strategist AI to eliminate false positives, assess the true impact of vulnerabilities, and produce this comprehensive security report.

4. Findings Summary

ID	Title	Severity	Status
I-01	Multi-signature Wallet Governance Model	**Informational**	**For Consideration**

5. Detailed Findings

[I-01] Multi-signature Wallet Governance Model (Informational)

Severity: Informational

Description The token contract system utilizes a UUPS (Universal Upgradeable Proxy Standard) pattern, where the proxy's implementation can be changed. The authority to perform these upgrades is controlled by a multi-signature wallet (Gnosis Safe) (`0x79468a83e77423978e984E9799C51963B236F724`). This is a secure contract governance model that provides better security assurance compared to single account control.

Impact The use of a multi-signature wallet significantly reduces single point of failure risks, requiring consensus from multiple signers to execute upgrade operations. This design is technically secure and provides better decentralization assurance compared to single account control. No malicious functionality was found in the current contract code.

Code Evidence

```
contract YBTCB is UUPSUpgradeable, ... {

    function _authorizeUpgrade(
        address newImplementation
    ) internal override onlyOwner {}

}
```

Recommendation The current multi-signature wallet governance model already provides good security assurance. To further enhance decentralization, consider: 1) Publicly disclosing multi-sig signer information and threshold settings; 2) Consider adding timelock mechanisms in the future to provide transparency and reaction time for proposed changes; 3) Long-term consideration of migrating to a decentralized governance system (DAO).

6. Architecture and Design Analysis

The contract architecture is generally clean, leveraging well-audited OpenZeppelin libraries for core ERC20, ownership, and upgradeability functionalities. The choice of UUPS for upgradeability is a modern and gas-efficient approach. The core logic for depositing and withdrawing assets is straightforward and secure against common attacks like reentrancy.

Points for consideration:

1. **Hardcoded Conversion Ratio**: The `getCovertRatio()` function returns a constant value (`10**10`). This is safe and simple but offers no flexibility. The team might consider if a governance-updatable ratio would be beneficial in the future, with appropriate security measures (e.g., Timelock).

7. Systemic Risk Assessment

After comprehensive analysis, the contract system's overall security status is good:

- **Governance Features**: Multi-signature wallet control over upgrade authority provides good security assurance
- **Core Function Security**: Deposit and withdrawal logic is well-designed and follows security best practices
- **Token Economics**: Simple model based on fixed conversion rate with no complex economic vulnerabilities

- **Reentrancy Protection**: Correctly implements the Checks-Effects-Interactions pattern

Overall, the technical implementation is secure, and the governance structure employs a secure multi-signature model.

8. Conclusion

The YBTCB contract system provides a functional and secure implementation for a wrapped asset token. Its logic is sound, and it is protected against common vulnerabilities like reentrancy. The project employs a standard upgradeable proxy pattern managed by a multi-signature wallet (Gnosis Safe).

The contract's technical implementation follows industry best practices, and core functions have been thoroughly considered for security. The use of a multi-signature wallet provides better security assurance compared to single account control, which is a positive governance feature.

Summary: The contract system is technically secure and employs a secure governance model. The use of a multi-signature wallet reduces single point of failure risks and provides better security assurance for users.

9. Disclaimer