GA GUARDIAN

USDT0

Tether Gold Deployment

Security Assessment

May 16th, 2025

Summary

Audit Firm Guardian

Prepared By Roberto Reigada, Daniel Gelfand

Client Firm USDT0

Final Report Date May 16, 2025

Audit Summary

USDT0 engaged Guardian to review the security of their Tether Gold deployment. From the 14th of May to the 15th of May, a team of 2 auditors reviewed the source code in scope. All findings have been recorded in the following report.

Confidence Ranking

Given the lack of critical issues detected and the minimal code changes following the main review, Guardian assigns a Confidence Ranking of 5 to the protocol. Guardian advises the protocol to consider periodic review with future changes.

For detailed understanding of the Guardian Confidence Ranking, please see the rubric on the following page.

✅ Verify the authenticity of this report on Guardian's GitHub: https://github.com/guardianaudits

Guardian Confidence Ranking

Confidence Ranking	Definition and Recommendation	Risk Profile
5: Very High Confidence	Codebase is mature, clean, and secure. No High or Critical vulnerabilities were found. Follows modern best practices with high test coverage and thoughtful design. **Recommendation:** Code is highly secure at time of audit. Low risk of latent critical issues.	0 High/Critical findings and few Low/Medium severity findings.
4: High Confidence	Code is clean, well-structured, and adheres to best practices. Only Low or Medium-severity issues were discovered. Design patterns are sound, and test coverage is reasonable. Small changes, such as modifying rounding logic, may introduce new vulnerabilities and should be carefully reviewed. **Recommendation:** Suitable for deployment after remediations; consider periodic review with changes.	0 High/Critical findings. Varied Low/Medium severity findings.
3: Moderate Confidence	Medium-severity and occasional High-severity issues found. Code is functional, but there are concerning areas (e.g., weak modularity, risky patterns). No critical design flaws, though some patterns could lead to issues in edge cases. **Recommendation:** Address issues thoroughly and consider a targeted follow-up audit depending on code changes.	1 High finding and ≥ 3 Medium. Varied Low severity findings.
2: Low Confidence	Code shows frequent emergence of Critical/High vulnerabilities (~2/week). Audit revealed recurring anti-patterns, weak test coverage, or unclear logic. These characteristics suggest a high likelihood of latent issues. **Recommendation:** Post-audit development and a second audit cycle are strongly advised.	2-4 High/Critical findings per engagement week.
1: Very Low Confidence	Code has systemic issues. Multiple High/Critical findings (≥5/week), poor security posture, and design flaws that introduce compounding risks. Safety cannot be assured. **Recommendation:** Halt deployment and seek a comprehensive re-audit after substantial refactoring.	≥5 High/Critical findings and overall systemic flaws.

Table of Contents

Project Overview

Project Summary

Project Name	USDT0
Language	Solidity
Codebase	https://github.com/Everdawn-Labs/usdt0-tether-contracts-hardhat https://github.com/Everdawn-Labs/usdt0-oft-contracts
Commit(s)	usdt0-tether commit: ffd78fc1f275fcb403c3f65a2e7e8bded713b2c1 usdt0-oft commit: 528bd5f508ff4e21f08365ad666c7fa71ab320c6

Audit Summary

Delivery Date	May 16, 2025
Audit Methodology	Static Analysis, Manual Review, Test Suite

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
High	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Low	0	0	0	0	0	0
Info	3	0	0	1	0	2

Project Overview

Project Summary

Network	Addresses
Ethereum Mainnet	OFT Proxy: 0xb9c2321BB7D0Db468f570D10A424d1Cc8EFd696C OFT Implementation: 0x77E277ea59a49EE2c9c6D06EF708B4BB8Edc4af3 OFT Proxy Admin: 0x4de7096B2131E84Fd6b2042AD8cd9B4E43F728Fc XAUt Proxy: 0x68749665FF8D2d112Fa859AA293F07A622782F38 XAUt Implementation: 0x4c0d2c74a8d26f1e4f5653021c521f5471f9e566 XAUt Proxy Admin: 0x856fcc085290ac1e40392442211e6a333afb873e
Arbitrum	OFT Proxy: 0xf40542a7B66AD7C68C459EE3679635D2fDB6dF39 OFT Implementation: 0xa2B4fA529eaF8465036e1E7363DE4f1cbe6BB8E8 OFT Proxy Admin: 0xfc061c6b31a03e84c741e6a41ba07fd7094519ad XAUt Proxy: 0x40461291347e1eCbb09499F3371D3f17f10d7159 XAUt Implementation: 0x9001dbe4d68d36ab87923a2a9dfb0c745fd25001 XAUt Proxy Admin: 0x553ec478a66be27ba25a6bc5db20aec2ed6a1b4a
HyperEVM	OFT Proxy: 0x904861a24F30EC96ea7CFC3bE9EA4B476d237e98 OFT Implementation: 0xcDd68D15372378b04300820c1d3d0237886d283f OFT Proxy Admin: 0xa882c21C9df00958A958cde96f2B2Ae8FB4315B1 XAUt Proxy: 0xb8ce59fc3717ada4c02eadf9682a9e934f625ebb XAUt Implementation: 0xf555a12bffaef20cc201a74ae6513cb4aadb34b9 XAUt Proxy Admin: 0x779ded0c9e1022225f8e0630b35a9b54be713736
Avalanche	OFT Proxy: 0x7E7866bc840aFf9f517a49AfDbfC9e7C7Aba9a68 OFT Implementation: 0x57142977Ba9826793398fbDec436284065187f49 OFT Proxy Admin: 0xfc061c6B31A03E84c741e6a41bA07fd7094519aD XAUt Proxy: 0x2775d5105276781b4b85ba6ea6a6653beed1dd32 XAUt Implementation: 0xc6bc407706b7140ee8eef2f86f9504651b63e7f9 XAUt Proxy Admin: 0xf8b07fc6924b80e4792aca834309e03caf36cd80
Polygon	OFT Proxy: 0x5421Cf4288d8007D3c43AC4246eaFCe5b049e352 OFT Implementation: 0x75FEB87F8494bEcbE0634c414c15c8200A4A5770 OFT Proxy Admin: 0xfc061c6B31A03E84c741e6a41bA07fd7094519aD XAUt Proxy: 0xf1815bd50389c46847f0bda824ec8da914045d14 XAUt Implementation: 0x6d205337f45d6850c3c3006e28d5b52c8a432c35 XAUt Proxy Admin: 0xd9492653457a69e9f4987db43d7fa0112e620cb4

Audit Scope & Methodology

Vulnerability Classifications

Severity	Impact: *High*	Impact: *Medium*	Impact: *Low*
Likelihood: *High*	🔴 Critical	🟠 High	🟡 Medium
Likelihood: *Medium*	🟠 High	🟡 Medium	🟢 Low
Likelihood: *Low*	🟡 Medium	🟢 Low	🟢 Low

Impact

High Significant loss of assets in the protocol, significant harm to a group of users, or a core functionality of the protocol is disrupted.

Medium A small amount of funds can be lost or ancillary functionality of the protocol is affected. The user or protocol may experience reduced or delayed receipt of intended funds.

Low Can lead to any unexpected behavior with some of the protocol's functionalities that is notable but does not meet the criteria for a higher severity.

Likelihood

High The attack is possible with reasonable assumptions that mimic on-chain conditions, and the cost of the attack is relatively low compared to the amount gained or the disruption to the protocol.

Medium An attack vector that is only possible in uncommon cases or requires a large amount of capital to exercise relative to the amount gained or the disruption to the protocol.

Low Unlikely to ever occur in production.

Audit Scope & Methodology

Methodology

Guardian is the ultimate standard for Smart Contract security. An engagement with Guardian entails the following:

- Two competing teams of Guardian security researchers performing an independent review.
- A dedicated fuzzing engineer to construct a comprehensive stateful fuzzing suite for the project.
- An engagement lead security researcher coordinating the 2 teams, performing their own analysis, relaying findings to the client, and orchestrating the testing/verification efforts.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts. Comprehensive written tests as a part of a code coverage testing suite.
- Contract fuzzing for increased attack resilience.

Findings & Resolutions

ID	Title	Category	Severity	Status
I-01	OApp Owner And Delegate Address	Configuration	Info	Resolved
I-02	Inaccurate Block Confirmations	Configuration	Info	Resolved
I-03	Missing setTrusted Call In HyperliquidExtension	Configuration	Info	Acknowledged

I-01 | OApp Owner And Delegate Address

Category	Severity	Location	Status
Configuration	Info	Global	Resolved

Description

The current `owner` and `delegate` address for all the `OApps` deployed across the different chains is set to the externally owned address `0x565786AbE5BA0f9D307AdfA681379F0788bEdEf7`.

This configuration introduces a single point of control and potential security risks across all blockchains where it is deployed. EOA-controlled addresses can be more vulnerable to key compromise or misuse by a single actor.

Recommendation

Migrate the address to a multisignature wallet to distribute control and reduce the risk of unauthorized transactions. This ensures that multiple parties approve critical operations, thereby enhancing the overall protocol security.

Resolution

USDT0 Team: Resolved.

I-02 | Inaccurate Block Confirmations

Category	Severity	Location	Status
Configuration	Info	Global	Resolved

Description

The current LayerZero configuration sets block confirmations to 60 for any HyperEVM communication, which does not align with the actual block time requirements and risks finality issues.

The desired interval for messages with this chain is 24 hours, equivalent to a setting of 43,200 blocks.

Recommendation

Update the block confirmation value for messages sent from HyperEVM to 43,200. This adjustment ensures adequate certainty for finalizing messages.

Resolution

USDT0 Team: Resolved.

I-03 | Missing setTrusted Call In HyperliquidExtension

Category	Severity	Location	Status
Configuration	Info	contract	Acknowledged

Description

The current HyperliquidExtension deployed is missing a `setTrusted` call to the `HyperLiquidComposer` contract.

Recommendation

Similarly as was performed during the USDT deployment in this transaction, consider calling `setTrusted(<HyperLiquidComposer address>)` in the `XAUt0 HyperliquidExtension`.

Resolution

USDT0 Team: Composer will be deployed later.

Disclaimer

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Guardian to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Guardian’s position is that each company and individual are responsible for their own due diligence and continuous security. Guardian’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by Guardian is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

Notice that smart contracts deployed on the blockchain are not resistant from internal/external exploit. Notice that active smart contract owner privileges constitute an elevated impact to any smart contract’s safety and security. Therefore, Guardian does not guarantee the explicit security of the audited smart contract, regardless of the verdict.

About Guardian Audits

Founded in 2022 by DeFi experts, Guardian Audits is a leading audit firm in the DeFi smart contract space. With every audit report, Guardian Audits upholds best-in-class security while achieving our mission to relentlessly secure DeFi.

To learn more, visit https://guardianaudits.com

To view our audit portfolio, visit https://github.com/guardianaudits

To book an audit, message https://t.me/guardianaudits