INDEPENDENT SMART CONTRACT REVIEW / 01

TAOT

Smart Contract Audit

A focused review of the verified TAOT ERC-20 contract deployed on Base.

REVIEW DATE	NETWORK	VERSION	SCOPE
September 13, 2026	**Base**	**1.0**	**TAOT.sol + inherited ERC-20 / AccessControl paths**

CONTRACT
0x7f2f00e54dcaa8b248bdfd75da2ae859d4d8ff3e

---

01 / EXECUTIVE SUMMARY

Clear design, bounded supply

The reviewed TAOT contract is a compact ERC-20 implementation with a 250,000,000-token maximum supply on Base. The full 250,000,000 tokens were issued at deployment, and the observed Base supply remained at that ceiling when checked for this report. The contract's bridge functions are reserved for a possible future cross-chain flow; they are not open minting or burning functions.

Within this focused source review, we identified **no high-, medium-, or low-severity code findings**. The bridge role and administrator remain important operational trust points, explained below in plain language. This conclusion applies to the reviewed Base token contract, not to any future bridge implementation, other-chain contract, or investment outcome.

0	0	0	2
High	Medium	Low	Operational notes

---

02 / SCOPE & METHOD

What was checked

We reviewed the explorer-verified `TAOT.sol` source, its use of OpenZeppelin ERC-20 and AccessControl, constructor supply and role assignment, external mint/burn and role-management entry points, and the publicly reported token supply. Explorer metadata identifies Solidity 0.8.34, optimization enabled with 200 runs, and no proxy implementation. This was a manual source and public-data review; it did not include a formal proof, full transaction-history reconstruction, deployed bridge system, multisignature configuration, or economic analysis.

Source verification was observed on both BaseScan (verified exact match) and Base Blockscout (verified). These are the two explorers checked; this report does not claim

verification on every explorer.

03 / CONTRACT MECHANICS

How the protections work

01

Maximum supply

`MAX_SUPPLY` is a constant of 250,000,000 tokens (18 decimals). The constructor rejects an initial supply above it, and `bridgeMint` rejects any mint that would make Base `totalSupply()` exceed it.

02

Bridge-only minting

`bridgeMint` is protected by `BRIDGE_ROLE`. Since the full supply was initially issued, it cannot mint more while Base supply remains at the cap. If tokens are burned and supply falls below the cap, a bridge-role account can reissue only within the newly available room.

03

Holder-approved burning

`bridgeBurnFrom` also requires `BRIDGE_ROLE`, and it spends the holder's ERC-20 allowance before burning. A bridge-role account cannot use this function to burn an unapproved holder balance.

04

Role management

`DEFAULT_ADMIN_ROLE` can add or revoke bridge-role accounts, including through inherited `grantRole` and `revokeRole`. This does not bypass the Base supply cap, but it makes administrator key security important.

04 / OPERATIONAL NOTES

What to understand about bridging

Bridge intent versus enforcement

The stated purpose is to burn tokens during cross-chain transfers and reissue them on a destination chain while respecting the supply ceiling. This Base contract enforces a *Base-chain* cap and role restrictions. It does not itself verify a burn on another chain, match a mint to a particular burn, or prove a global supply cap across chains. Those guarantees would depend on a future bridge's separate design and operations.

Privileged-key stewardship

An administrator can grant `BRIDGE_ROLE` to another address. A bridge-role account can mint into any available Base supply headroom, whether or not this contract can see a corresponding cross-chain event. Secure key custody and monitored role changes matter if bridging is activated. These are transparent trust assumptions, not high-, medium-, or low-severity code defects found in this scoped review.

05 / REVIEW TEAM & DISCLOSURE

Human-led, AI-assisted

JustinVforVendetta (sunerok) provided the independent third-party review and findings. His public contribution record includes Bitcoin Core, Dogecoin Core, and Verge Core. These links document experience; those projects did not sponsor or endorse this report.

AI-assisted analysis: Codex, using GPT-5.6 Sol as designated for this review. OpenAI Docs lists a **February 16, 2026 knowledge cutoff** for GPT-5.6 Sol. That is a knowledge-cutoff date, *not* a verified last model-update or release date. No public last-update date for this session's model snapshot was established. AI assistance is not a professional credential, independent auditor, or substitute for human judgment.

---

06 / EVIDENCE & LIMITATIONS

Source trail

1. BaseScan verified contract source and constructor arguments.
2. Base Blockscout verified contract source and token supply data.
3. OpenZeppelin AccessControl documentation and ERC-20 documentation.
4. OpenAI Docs: GPT-5.6 Sol model information.

> This report records a point-in-time, scoped assessment, not a guarantee that software, operators, bridges, or token markets are risk-free. The future cross-chain bridge was not in scope. Anyone integrating or buying a token should review the live contract, privileges, and their own risk exposure.

SUNEROK.DEV / TAOT / 2026-09-13 End of report