

USTBL

Multi-Chain Public-Contract Security Assessment

Spiko US T-Bills Money Market Fund USD Share
Eight-network public-production and source-correspondence assessment

REPORT	B3-USTBL-2026-001
ISSUED	1 October 2026
BASELINE	Fixed observations on 28-29 September 2026; chain-specific points are listed in scope
AUTHOR	bench3.ai

Contents

1 Executive Summary 3

2 Scope and Assessment Basis 4

3 System and Threat Model 5

4 Technical Assessment 5

5 Recorded Validation 7

6 Findings and Control Observations 8

7 RWA Linkage and Public Verifiability 9

8 Limitations and Conclusion 10

A Evidence and Source Index 10

Assessment of official USTBL deployments, retained source/build records, fixed-state read-only observations, assessment conclusions and cross-network supply reconciliation over a non-atomic observation window of approximately 41 minutes.

1 Executive Summary

bench3.ai assessed the official USTBL deployments on Ethereum, Polygon, Base, Arbitrum, Etherlink, Starknet, Stellar and Solana. The assessment addressed proxy and implementation identity, meta-transaction authorization, mint/burn and eligibility controls, redemption state transitions, upgrade authority, non-EVM source correspondence, and cross-network supply reconciliation using non-atomic observations collected over approximately 41 minutes. [E01-E07]

Assessment conclusion

No reportable vulnerability was confirmed in the examined public-production scope. The conclusion is qualified by materially different non-EVM evidence: all three Starknet production classes and ABIs matched the pinned source build; the live Stellar token executable did not match a public repository artifact; and the Solana minter and Gate had strong correspondence while the deployed Token ACL remained source-unresolved and its shared upgrade controller was not publicly identified.

Classification	Recorded result
Confirmed vulnerabilities	Critical 0 High 0 Medium 0 Low 0
Control observations	3; privileged control concentration, Solana eligibility lifecycle and Stellar emergency-pause configuration
Supply reconciliation	154,448,726.41002 USTBL across eight networks; zero base-unit difference from the issuer totals API over a non-atomic observation window from 18:27:04 to 19:08:06 UTC

The supply match is strong bounded accounting evidence across the approximately 41-minute observation window, not an atomic snapshot or proof of continuous cross-network conservation, legal-register equality, asset custody or completed cash settlement. Private KYC, legal-register, NAV, signer-custody, bank and redemption-reconciliation records were not available. [E03-E07]

2 Scope and Assessment Basis

2.1 Assessment identity

Parameter	Assessment basis
Assessment type	Multi-chain public-contract, source-correspondence and public-evidence assessment
Evidence cutoff	Technical production evidence through 29 September 2026; RWA linkage evidence through 30 September 2026
Networks	Ethereum, Polygon, Base, Arbitrum, Etherlink, Starknet, Stellar and Solana
Methods	Official-inventory review, proxy and dependency resolution, source/build comparison, fixed-block/ledger/slot calls, retained event-history analysis, read-only negative calls and non-atomic cross-network supply reconciliation

2.2 Deployment inventory

Network	Primary identifier	Recorded identity
Ethereum	0xe4880249745eac5f1ed9d8f7df844792d560e750	Token proxy to 0x15ea0ec460a0e6847ec0aa8d50a84b3a51b95f74; fixed authorization snapshot at block 26,077,416
Polygon	0xe4880249745eac5f1ed9d8f7df844792d560e750	Token proxy to 0x15ea0ec460a0e6847ec0aa8d50a84b3a51b95f74; fixed authorization snapshot at block 94,607,175
Base	0xe4880249745eac5f1ed9d8f7df844792d560e750	Token proxy to 0x15ea0ec460a0e6847ec0aa8d50a84b3a51b95f74; fixed authorization snapshot at block 51,913,411
Arbitrum	0x021289588cd81dc1ac87ea91e91607eef68303f5	Token proxy to chain-specific implementation 0xa0769f7a8fc65e47de93797b4e21c073c117fc80; block 509,773,919
Etherlink	0xe4880249745eac5f1ed9d8f7df844792d560e750	Token proxy to 0x15ea0ec460a0e6847ec0aa8d50a84b3a51b95f74; block 54,441,224
Starknet	0x020ff2f6021ada9edbceaf31b96f9f67b746662a6e6b2bc9d30c0d3e290a71f6	Token, PermissionManager and Redemption classes matched pinned Scarb 2.8.2 builds at block 15,589,081
Stellar	CARUUX2FZNP6DGJOEUF5IUQWYHNL5AVD V7PMVSHWL7OBYIBFC76F4TO	Custom Soroban token at ledger 64,667,341; live token WASM lacked an exact public-repository artifact match
Solana	Mint 3E2qphMMBQtH3HZH2ZSg7CkbF8gSLePuo y7yVpkDxHGn	Token-2022 mint with verified minter, exact Gate v0.2.0 and source-unresolved Token ACL; finalized anchor slot 451,406,890

The attached scope manifest records component identities and source/build limits; listing or common branding does not imply equal assurance or full test coverage. [E01-E05; S01-S05]

2.3 Exclusions

Excluded were private key custody, signer independence, production approval workflows, monitoring and incident response, KYC/AML decisions, the legal shareholder register, NAV calculation inputs, underlying portfolio and custody records, bank and cash settlement, complete per-chain mint/burn reconciliation, and end-to-end redemption operations. No production transaction was signed or broadcast.

3 System and Threat Model

USTBL is a DLT-registered variable-NAV share class issued natively on multiple networks. The assessed public architecture does not expose a common on-chain canonical bridge or global cap; each deployment maintains local supply and relies on issuer-level authorization and reconciliation. EVM networks use upgradeable token proxies, PermissionManager authorization and ERC2771Forwarder meta-transactions. Starknet and Stellar pair tokens with permission and redemption contracts. Solana uses Token-2022 extensions, a minter, Token ACL and Gate. [E01-E05]

Actor or layer	Relevant capability	Security objective
Ordinary or whitelisted holder	Transfer, request redemption and use permitted meta-transaction paths	Cannot mint, burn third-party balances, change eligibility, pause or upgrade
Issuer operators	Mint/burn, whitelist, freeze/thaw, pause, execute redemption and administer roles	Actions must follow authorized procedures; custody and approvals remain trust dependencies
Upgrade controllers	Replace EVM, Starknet, Stellar or Solana execution logic	Source correspondence and operational governance determine continuing report applicability
Issuer accounting and legal register	Reconcile eight native supplies to legal shares and cash settlement	Public supply equality over the approximately 41-minute non-atomic observation window does not prove continuous conservation or backing

4 Technical Assessment

4.1 EVM deployments and meta-transaction authority

All five EVM token proxies were initialized through constructor delegatecalls and resolved to the recorded implementations. The Arbitrum runtime difference was attributable to its chain-specific PermissionManager and forwarder constructor values and matched the official deployment artifacts. The deployed OpenZeppelin forwarder signs sender, target, value, gas, nonce, deadline and calldata under an EIP-712 domain bound to chain ID and verifying contract, so the examined cross-chain replay condition was not established for the reviewed version. [E01-E02; S02-S03]

At one fixed block per chain, two independent RPC endpoints agreed that the production forwarder held only PUBLIC. That group did not intersect requirements for mint, burn, pause, unpause, ownership change or upgrade, and every direct PermissionManager.canCall query returned false. The forwarder lacked those six powers at the five observations; later role, requirement or upgrade changes fall outside this conclusion. [E02]

4.2 Starknet source and state

The production Token, PermissionManager and Redemption class hashes and ABIs were reproduced from issuer repository commit 487823179d75dfd7a9702f7f8adf3d1e24d52423 using the pinned Scarb 2.8.2 toolchain after semantic canonicalization. Mint required MINTER and a whitelisted recipient; transfers required both parties to be whitelisted; Redemption escrowed tokens before privileged execution or cancellation; and upgrade/role paths remained privileged. No ordinary path to bypass those controls was established. Historical event enumeration was incomplete because public RPCs constrained broad range queries, but the current class and role state was fixed. [E03-E04; S04]

4.3 Stellar source limitation and controls

The official Stellar deployment is a custom Soroban token, not a Stellar Asset Contract. PermissionManager matched the issuer repository exactly and Redemption's executable sections matched after excluding custom specification sections. The live token executable, however, did not match any token artifact in the complete public repository history. Its exposed methods and state aligned with the documented architecture, but mint, burn, transfer-authentication, upgrade and replay conclusions cannot be elevated to exact source-binary proof. [E03-E04; L01]

The token was unpaused and had three minters, two burners, two whitelisters, 25,893 whitelisted accounts, two redemption executors and no PAUSER member. The owner was a single-signer Stellar account. No ordinary route to roles, mint, privileged burn, dependency replacement, upgrade or unescrowed redemption was established, subject to the binary-provenance limitation. [E03; O01; O03]

4.4 Solana program correspondence and eligibility lifecycle

The Solana mint had zero supply, default-frozen accounts and configured permanent-delegate, freeze, pause, mint-close and permissioned-burn authorities. The minter executable matched issuer commit afdab14fb1a59bf3abe2f263870023349a560e2e through public build verification, and the Gate program matched the public v0.2.0 fixture. The Token ACL executable matched no artifact in the complete public repository history, and the controller/threshold behind shared ACL/Gate upgrade authority DXtFpBPjcn2hxPnw79x1Pfoj35vXh5AsWBkS37YnXMVv was unresolved. [E03-E04; S05]

Eligibility lists gate thaw rather than each Token-2022 transfer. Removing an account from the allow list or adding it to the block list does not retroactively freeze an already-thawed account while permissionless freeze is disabled; the issuer must actively freeze that account. Strict list modes derived entries from actual token-account owner data, and no permissionless thaw bypass was established despite the deployed Token ACL predating public hardening changes. The zero-supply state prevented review of funded-holder history. [E03; O02; L02-L03]

4.5 Non-atomic cross-network supply reconciliation

Network	Recorded supply
Ethereum	72,604,691.39473
Polygon	12,368,401.85452
Base	1,833,300.01515
Arbitrum	23,891,114.36001
Etherlink	2,868,905.70200
Starknet	10,007,011.61704
Stellar	30,875,301.46657
Solana	0.00000
Total	154,448,726.41002; equal to issuer API totalShares across observations from 18:27:04 to 19:08:06 UTC

5 Recorded Validation

Validation record	Recorded result and limit
EVM fixed authorization	Dual-RPC same-block calls on five networks denied the trusted forwarder for six sensitive selectors; conclusion is snapshot-specific.
EVM initialization and replay	Constructor initialization and EIP-712 domain separation were established from official artifacts, source and representative production history.
Starknet build comparison	Three production Sierra classes and ABIs matched pinned Scarb 2.8.2 builds after semantic canonicalization.
Stellar binary comparison	PermissionManager matched exactly and Redemption executable sections matched; the live token executable did not match any public token artifact.
Solana build comparison	Minter matched the issuer commit and Gate matched v0.2.0; Token ACL remained source-unresolved.
Supply reconciliation	Eight network supplies matched the issuer total to the base unit at non-atomic observations spanning approximately 41 minutes.

6 Findings and Control Observations

Zero confirmed vulnerabilities

No reportable implementation vulnerability was confirmed in the assessed public-production scope. O01-O03 are control observations and are not included in vulnerability severity totals.

O01 — Privileged authority is concentrated across non-EVM deployments

Field	Assessment
Classification	Control observation - applicable at snapshot; no vulnerability severity assigned
Affected components	Stellar owner; Starknet emergency pauser; Solana issuer vaults, minter upgrade and operational mint/burn authorities
Condition	Compromise, misuse or procedural error within authorized control paths
Status	No ordinary-attacker route established; custody and approval controls unavailable

Stellar administration was held by a single-signer account; Starknet emergency pause was controlled by a 1-of-5 account; and observed Solana vaults used threshold one with no timelock, while the minter upgrade and operational mint/burn paths also depended on direct authorities. These are authorized governance choices with material operational consequences. [E03-E04]

Recommendation: Spiko should require independent approval for upgrades, issuance, burn, eligibility and emergency controls; document actual signer custody and rotation; and use on-chain thresholds or timelocks proportionate to each action's impact where rapid emergency response does not require a narrower control.

O02 — Solana eligibility revocation requires an active freeze

Field	Assessment
Classification	Control observation - operational compliance dependency; no vulnerability severity assigned
Affected component	Solana Token-2022 mint and Token ACL configuration
Precondition	A token account was previously thawed and its owner later loses eligibility
Status	No authorization bypass established; current supply was zero

Allow/block lists govern permissionless thaw. They do not automatically refreeze a previously thawed account when eligibility changes, and permissionless freeze was disabled. Compliance therefore depends on an authorized issuer operation that freezes the account promptly after revocation. [E03]

Recommendation: Spiko should bind every eligibility revocation to a monitored, idempotent freeze workflow with defined completion time, retry and reconciliation behavior before enabling funded Solana issuance.

O03 — The Stellar token had no active PAUSER member

Field	Assessment
Classification	Control observation - applicable at snapshot; no vulnerability severity assigned
Affected component	Stellar PermissionManager and token pause capability
Configuration	Zero PAUSER members while pause/unpause methods existed
Status	Operational availability issue; administrator could grant the role

At the observation point, no account could exercise the exposed PAUSER-gated emergency function without a preceding administrative role grant. This does not grant an attacker authority, but it adds a role-change step to emergency response and leaves that step dependent on the single-signer owner. [E03]

Recommendation: Spiko should assign emergency pause authority to a controlled account under a tested runbook, or explicitly document why pause remains intentionally dormant and how equivalent containment is achieved.

7 RWA Linkage and Public Verifiability

USTBL is a DLT-registered USD share class of Spiko SICAV with daily variable NAV, not a token designed to remain at a fixed one-dollar price. The prospectus describes the legal structure and service providers, while Spiko's public APIs expose the share class, NAV, totalShares, total assets and portfolio data. [E06; S01; S06-S08]

The exact eight-network supply-to-totalShares match materially supports the recorded accounting relationship across the approximately 41-minute observation window. Because the reads were not atomic, it does not replace an issuer-signed continuous conservation record, the legal shareholder register, or a same-cutoff administrator/custodian attestation of assets and liabilities. Public code review is not a reserve, solvency, NAV or legal-title opinion.

8 Limitations and Conclusion

ID	Limitation	Effect on conclusions
L01	Stellar live token executable did not match a public repository artifact	Method and architecture review cannot be represented as exact source-binary assurance for token mint, burn, transfer, replay or upgrade behavior.
L02	Solana Token ACL source/build match and shared upgrade-controller identity unresolved	Token ACL binary-specific defects or governance changes cannot be conclusively excluded; the verified minter and exact Gate do not remove this dependency.
L03	Solana supply was zero	No funded live-holder transfer, freeze, thaw, forced-transfer or permissioned-burn history was available for observation.
L04	Broad historical Starknet event enumeration was RPC-constrained	Current class, role and state conclusions are fixed, but the report does not claim a complete historical control-change ledger.
L05	Private operating, signer, KYC, legal-register, NAV, bank and redemption records unavailable	No full operational, key-custody, legal-title, NAV, cash-settlement or continuous multi-chain control opinion is provided.
L06	Eight-network supply equality was observed non-atomically over approximately 41 minutes	The result does not represent one atomic snapshot and does not prove continuous global conservation or backing.

Qualified conclusion

No reportable vulnerability was confirmed in the examined public deployments and recorded validation. Assurance is strongest for the fixed EVM authorization state and the matched Starknet classes, materially qualified for the Stellar token and Solana Token ACL, and bounded to the zero-supply Solana configuration observed. Any implementation, role, ACL, signer or supply-state change may require reassessment.

A Evidence and Source Index

Assessment workpapers are retained separately and are not attached. The scope manifest identifies each record by SHA-256 and includes deployment and source references. Checksums identify records; they do not attest to their contents.

ID	Assessment record
E01	USTBL public deployment and control assessment
E02	USTBL EVM authorization conclusions and issue classification
E03	USTBL non-EVM public-production review
E04	USTBL non-EVM assessment conclusions and issue classification
E05	USTBL official deployment registry snapshot
E06	Tokenized-treasury RWA anchor and public-verifiability assessment
E07	Portfolio-wide assessment basis and limitations

Primary public sources

S01 | Spiko USTBL official share-class API

Primary issuer deployment inventory retained at the technical evidence cutoff.

S02 | Spiko EVM contracts repository

Primary source, deployment-cache and configuration basis for EVM review; referenced commits and fixed deployment state control the conclusions.

S03 | OpenZeppelin ERC2771Forwarder v5.0.1

Pinned forwarder source used to assess signed request contents and EIP-712 replay domains.

S04 | Spiko Starknet contracts at reviewed commit

Pinned issuer source reproduced with Scarb 2.8.2 and matched to all three production classes after semantic canonicalization.

S05 | Spiko Solana contracts at reviewed commit

Pinned issuer source corresponding to the verified minter; it did not resolve the deployed Token ACL binary.

S06 | Spiko 2026 prospectus

Primary legal and variable-NAV product context retained in the RWA workpaper.

S07 | USTBL latest NAV API

Issuer-published NAV source; not an independent same-cutoff attestation.

S08 | USTBL totals API

Issuer totalShares response used for cross-network reconciliation against non-atomic observations collected over approximately 41 minutes.

Scope attachment

ustbl-scope-manifest-en.json

SHA-256: a13184cb9f219b816838d1907625a9e013ac47d371120c7aa585ed9fae79b62f