

thBILL

Smart Contract and Cross-Chain Configuration Assessment

Theo thBILL
Public-evidence review of the Ethereum canonical wrapper, tULTRA backing, mint Router and four-chain OFT mesh

REPORT	B3-THBILL-2026-001
ISSUED	1 October 2026
BASELINE	28 September 2026: separate eligibility checks and synchronized four-chain configuration observations
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 10

8 Limitations and Conclusion 11

A Deployment and Authority Inventory 12

B Evidence and Source Index 13

Assessment of the identified public contracts, fixed-height configuration, role history, canonical custody and LayerZero peer graph. Scope, methods and exclusions are defined in Section 2.

1 Executive Summary

bench3.ai assessed the public thBILL smart-contract system across four networks. The system separates four materially different layers: the canonical Ethereum thBILL proxy and IToken implementation; tULTRA as the canonical wrapper's configured asset; TTokenRouterV2 and its privileged mint-service account; and a LayerZero OFT mesh comprising an Ethereum lock/unlock adapter plus native burn/mint OFTs on Arbitrum, Base and HyperEVM. [E01-E05; S01-S05]

The synchronized fixed-height review confirmed the canonical proxy implementation and initialized state, reconstructed the Router's sole surviving MINTER_ROLE holder, distinguished the Ethereum adapter from the three direct OFTs, verified all 12 directional remote peer edges, and reconciled adapter custody against aggregate sidechain supply at the recorded blocks. [E01-E03]

Assessment conclusion

No reportable implementation vulnerability was confirmed in the examined canonical-token, Router authorization, OFT peer, adapter-custody or holder-eligibility paths. Three material control observations are reported. The conclusion does not cover the private production mint service or establish legal or custodial backing beyond the public on-chain layers.

Classification	Recorded result
Confirmed vulnerabilities	Critical 0 High 0 Medium 0 Low 0
Control observations	3; private-service trust, cross-chain governance and RWA wrapper boundaries
Unresolved technical issues	No ordinary-caller defect was established; private mint-service behavior remains outside the assessed boundary

Material residual risk

TTokenRouterV2.depositOptimistic is restricted to MINTER_ROLE but accepts economically coupled fields—including assetIn, amountAssetIn, assetReceiver, tTokenAssets, iToken and to—from that privileged caller without an on-chain signed quote binding them together. The sole current role holder was an authenticated EIP-7702 account rather than a public forwarder. No ordinary-caller exploit was established, but the private service that authenticates users and constructs these calls was not reviewed. [E01; O01; L01]

The public on-chain backing chain is layered rather than a direct claim on Treasury securities. Canonical thBILL was configured against tULTRA; the Ethereum OFT adapter held canonical thBILL against sidechain OFT supply; and tULTRA's pending/optimistic quantities must ultimately reconcile to formal ULTRA shares, legal records and custody assets outside the public contract boundary. [E01, E06; O03; L02]

2 Scope and Assessment Basis

2.1 Recorded state points

Network	Observation point	Principal component
Ethereum / eligibility	Block 26,074,031 2026-09-28 06:02:59 UTC	Canonical wrapper and underlying tULTRA eligibility behavior; separate earlier observation
Ethereum	Block 26,077,438 2026-09-28 17:26:59 UTC	Later configuration/custody snapshot: canonical thBILL, tULTRA asset binding, Router and Ethereum OFTAdapter
Arbitrum	Block 509,774,894 2026-09-28 17:27:05 UTC	Native thBILL OFT
Base	Block 51,913,540 2026-09-28 17:27:07 UTC	Native thBILL OFT
HyperEVM	Block 47,132,570 2026-09-28 17:27:07 UTC	Native thBILL OFT

The four configuration/custody observations at 17:26:59-17:27:07 UTC were synchronized within eight seconds. The eligibility calls at Ethereum block 26,074,031 were earlier and are not part of that synchronized baseline. Full hashes and component identities are recorded in Appendix A and the attached scope manifest. [E01-E02]

2.2 Included components and methods

The assessment reviewed exact-matched public source for the canonical IToken implementation, TTokenRouterV2, the Ethereum ThBillOFTAdapter and the three ThBillOFT deployments; resolved the canonical EIP-1967 implementation; recorded initialization, role and ownership history; used fixed-height read-only calls for configuration and authorization boundaries; reconstructed LayerZero peers and endpoints; and compared canonical adapter custody with synchronized sidechain supplies. [E01-E05]

Canonical holder-eligibility calls were recorded at Ethereum block 26,074,031 (28 September 2026, 06:02:59 UTC), separate from the later configuration snapshot. Their interpretation also considered the restricted tULTRA recipient boundary, exact sidechain OFT implementations and Theo's public product/terms materials. Selected read-only calls used ordinary balance or allowance state overrides; they were not completed production transactions. The behavior is consistent with the documented direct-mint/redeem and self-custody model, not a legal-compliance opinion. [E02-E04; S06-S10]

2.3 Exclusions

The production mint-service source, deployment build, API, request and quote schemas, user-authentication controls, replay store, decimals normalization, transaction-construction logic, monitoring and reconciliation were not available and were not validated. No inference about those controls is made from the Router's on-chain access check. [L01]

Also excluded are private tULTRA-to-ULTRA settlement and share conversion records, legal ownership registers, offering/private fund documents not in the public corpus, underlying portfolio and custody records, cash settlement, sanctions operations, organization-level key custody and full message-by-message LayerZero reconciliation. [L02-L05]

3 System and Threat Model

thBILL is a layered wrapper and cross-chain representation. The Ethereum canonical proxy issues thBILL shares against supported assets and was configured with tULTRA as its sole asset. The Router supports issuer-operated minting flows. The Ethereum OFTAdapter locks canonical thBILL for outbound transfers and releases it for inbound transfers; the Arbitrum, Base and HyperEVM OFTs burn on send and mint on receive. [E01-E05]

Layer	Security-relevant state	Boundary considered
Canonical thBILL	Share supply, supported asset, pause state and upgrade/admin roles	Proxy identity, initialization and public wrapper operations reviewed.
tULTRA	Restricted underlying-token eligibility and conversion into canonical wrapper assets	Address and recipient restriction observed; private tULTRA/ULTRA lifecycle excluded.
TTokenRouterV2	Privileged deposit parameters and MINTER_ROLE authorization	On-chain role and code reviewed; private service behavior excluded.
Ethereum OFTAdapter	Canonical token custody, LayerZero peers and lock/unlock accounting	Implementation, peers, endpoint and fixed-height custody reviewed.
Sidechain OFTs	Local supply, burn/mint bridge accounting and trusted peers	Three exact-matched deployments and 12 remote edges reviewed.
Legal and fund layers	Formal ULTRA shares, investor records, assets, liabilities and custody	Public linkage described; no legal, reserve or financial attestation provided.

3.1 Threat model

The threat model includes ordinary external addresses, canonical and sidechain token holders, allowance spenders and LayerZero messages from untrusted source identities. It distinguishes those actors from the canonical administrator, the Router's MINTER_ROLE account, the OFT owner/delegate and authorized LayerZero endpoints/peers.

Security objectives were to prevent first-caller initialization takeover; enforce Router role authorization; preserve trusted-peer source authentication; avoid sidechain issuance exceeding canonical adapter custody at the snapshot; and maintain the documented boundary between transferable thBILL ownership and restricted receipt of tULTRA. Compromise or misuse of legitimate administrators and the private mint service remains a trust dependency.

4 Technical Assessment

4.1 Canonical Ethereum proxy and initialization

At Ethereum block 26,077,438, canonical proxy 0x5FA487BCa6158c64046B2813623e20755091DA0b resolved through EIP-1967 to implementation 0x325478a069b0dbbdfbee909fa3741f84259ba519. The implementation had exact creation/runtime correspondence, compiler 0.8.28+commit.7893614a and runtime Keccak-256 0x5b0645110549d0d5e52b855323423d224b908c03836adaf90e4ca482f4a3b126. [E01, E05; S02]

The proxy emitted Initialized(1) at block 22,976,986. A fixed-block initialize retry returned OpenZeppelin InvalidInitialization(), and the configured production state was populated and unpaused. Complete DEFAULT_ADMIN_ROLE history left only timelock 0x2bB4b7E6E83FA6b77d0143dad631843cB73DCA02. The recorded deployment was initialized, and a public first-caller initialization takeover was not established. [E01]

4.2 tULTRA backing layer and canonical wrapper behavior

The canonical proxy's sole configured asset was tULTRA at 0x82b840b6eDf77f90C92a70b99f0B5d50E7967330. The IToken implementation exposes multi-asset ERC-4626-style conversion and deposit/redeem behavior; its recorded production configuration uses tULTRA as the on-chain asset for canonical thBILL. tULTRA was in ONLY_WHITELISTED transfer mode at the separate eligibility-check block 26,074,031, not established by this statement at the later synchronized snapshot. [E01-E04]

At Ethereum block 26,074,031, the recorded read-only calls showed canonical thBILL transferring independently of tULTRA recipient eligibility: the underlying token rejected the sampled ineligible recipient, while canonical redemption delivered tULTRA only to an eligible recipient. The calls' funding/allowance prerequisites are described in section 2.2. Exact sidechain contracts are plain transferable OFTs. This behavior is consistent with Theo's public description of KYC/KYB for direct mint and redeem access, self-custody and DeFi/bridge use; no continuous holder-level allowlist invariant was established. [E02-E04; S06-S10]

4.3 Router authorization and private mint-service boundary

TTokenRouterV2 at 0x8a2c307D1462Ff4fA98c9c119D3A3457AD505Eb1 had exact creation/runtime correspondence and runtime Keccak-256 0x4196bb916cde2a9dbe7843a12342f720b7f69222eff576cc14cd05aa7468c450. The source describes the Router as a helper for Theo's minting service and restricts depositOptimistic and bulkCompletePending to MINTER_ROLE. [E01, E05]

Complete role history through block 26,077,438 left one current minter: 0x0f21ee679e40123dea03cc64983035ce24bffc3. Its account code was an EIP-7702 delegation designator to the verified Simple7702Account implementation at 0xe6cae83bde06e4c305530e199d7217f42808555b. An unrelated-caller execute sample reverted with not from self or EntryPoint, supporting the account-authentication boundary. [E01]

The Router does not bind assetIn, amountAssetIn, assetReceiver, tTokenAssets, iToken and to to a single on-chain quote object. That design makes the private service's authentication, quotation, normalization, replay protection and final-beneficiary binding security-critical. No ordinary actor was shown able to invoke the Router path directly or cause the service to alter those fields, and the private implementation was unavailable. The report therefore reaches no conclusion on the correctness of private request construction; no on-chain ordinary-caller vulnerability was established. [O01; L01]

4.4 LayerZero OFT identity and peer graph

Ethereum 0xfDD22Ce6D1F66bc0Ec89b20BF16CcB6670F55A5a was a verified ThBillOFTAdapter immutably bound to canonical thBILL and LayerZero Endpoint V2 0x1a44076050125825900e736c501f859c50fE728c. token() returned the canonical token and approvalRequired() returned true. The same address on Arbitrum, Base and HyperEVM was an exact-matched ThBillOFT; on those chains token() returned the OFT itself and approvalRequired() returned false. [E01, E05; S04-S05]

The owner on all four deployments was operator Safe 0x94877640dD9E6F1e3Cb56Bf7b5665b7152601295, identified publicly as a 4-of-6 Safe. Endpoint EIDs were 30101 (Ethereum), 30110 (Arbitrum), 30184 (Base) and 30367 (HyperEVM). Every non-self peers(eid) entry resolved to bytes32 address 0x0000000000000000000000000000000000000000000000000000000000000000, while each self slot was zero.

The 12 directional remote edges were therefore complete and symmetric at the fixed blocks. [E01; S01, S05]

4.5 Canonical custody and sidechain supply

At Ethereum block 26,077,438, the adapter held 1,645,778,535,678 raw canonical units. Synchronized sidechain supplies were 346,146,556,781 raw units on Arbitrum, 215,960,991 on Base and 1,299,167,905,976 on HyperEVM. Their sum was 1,645,530,423,748, leaving canonical custody 248,111,930 raw units higher than aggregate sidechain issuance. With six decimals, the difference was 248.111930 thBILL. [E01]

Adapter canonical custody: 1,645,778.535678 thBILL

Sidechain OFT supply: 346,146.556781 + 215.960991 + 1,299,167.905976 = 1,645,530.423748 thBILL

Snapshot surplus: 248.111930 thBILL

The positive difference does not support an unbacked sidechain-mint claim. It may reflect in-flight bridge state or direct transfers to the adapter and was not attributed message by message. This reconciliation addresses the OFT layer only; it does not prove that all canonical thBILL is matched to finalized ULTRA legal shares or underlying custodial assets. [E01, E06; L02-L03]

4.6 Shared-decimal boundary

All four OFT contracts used six shared and local decimals with decimalConversionRate equal to 1. The LayerZero source converts a local amount to uint64 shared units. The first lossy value is above 18,446,744,073,709.551615 thBILL, while canonical supply at the synchronized Ethereum block was 36,252,237.545115 thBILL—approximately 508,844 times lower. Because the direct OFTs burn only the caller's balance and the adapter pulls only caller-approved canonical units, no realistic current third-party-loss path was established. [E01; S05]

5 Recorded Validation

The table records the principal fixed-height and source-correspondence checks retained in the assessment evidence. It does not imply that private services or every success/failure path were tested. [E01-E05]

ID	Recorded check	Outcome and evidentiary limit
V01	Resolve canonical proxy and retry initialize	Implementation matched; Initialized(1) recorded; retry returned InvalidInitialization(). Does not assess every privileged upgrade path.
V02	Reconstruct DEFAULT_ADMIN_ROLE	Only Ethereum timelock 0x2bB4...CA02 survived at the fixed block. Private timelock governance procedures were not assessed.
V03	Reconstruct Router MINTER_ROLE and sample account execution	Unique minter 0x0f21...fcf3; unrelated execute reverted at the Simple7702Account boundary. Private service requests were not tested.
V04	Read four-chain OFT owner, endpoint, EID and peer matrix	All 12 remote edges pointed to the official same-address deployment; self edges were zero. Point-in-time result only.
V05	Compare adapter canonical custody with synchronized sidechain supply	Custody exceeded aggregate sidechain issuance by 248.111930 thBILL; the surplus was not reconciled message by message.

ID	Recorded check	Outcome and evidentiary limit
V06	Canonical versus tULTRA eligibility behavior	At Ethereum block 26,074,031 (06:02:59 UTC), canonical transfer to an ineligible recipient succeeded in the recorded read-only call; tULTRA rejected that recipient. Redemption delivered tULTRA to an eligible recipient. Selected calls used balance/allowance overrides; this is separate from the later synchronized state snapshot.
V07	Compare current supply with uint64 shared-decimal boundary	Canonical supply was approximately 508,844 times below the first truncating amount; no current reachable third-party-loss path established.

All negative execution samples were read-only eth_call simulations. No transaction was signed or sent, and no private mint-service endpoint or credential was available or used. [E01-E04]

6 Findings and Control Observations

No implementation vulnerability was confirmed. The three observations below identify material trust and integration boundaries; they are not included in vulnerability severity totals. No issuer response or remediation verification was supplied.

ID	Title	Category / status
B3-THBILL-O01	Private mint-service controls are decisive to optimistic mint integrity	Service/control observation and material scope limitation
B3-THBILL-O02	A 4-of-6 operator Safe controls the mutable OFT trust graph	Privileged cross-chain control observation; applicable at snapshot
B3-THBILL-O03	thBILL, tULTRA, ULTRA shares and fund custody are distinct assurance layers	RWA integration observation; applicable to disclosed model

O01 | Private mint-service controls are decisive to optimistic mint integrity

Attribute	Record
Affected components	TTokenRouterV2.depositOptimistic; unique MINTER_ROLE holder; production mint service
Classification	Service/control observation and material scope limitation. No implementation-vulnerability severity assigned.
Evidence	E01, E05; L01

Description. The Router restricts optimistic minting to MINTER_ROLE, and the sole role holder was an authenticated EIP-7702 account. Once authorized, that caller supplies asset, amount, receiver, tToken, iToken and final-beneficiary fields that are not coupled by an on-chain quote signature. Integrity therefore depends on the private service that authenticates users and constructs the privileged call.

Impact and preconditions. A defect or compromise in the private service could cause a mismatch between received assets, minted thBILL-related quantities and the intended beneficiary. Exploitation would require influence over, or compromise of, the privileged service/account; no ordinary actor was shown able to call the

Router directly or induce altered parameters. The service was not validated, so neither exploitability nor safety is established.

Recommendation. The mint-service operator should bind authenticated user identity, quote identifier, expiry, nonce, chain, assetIn, amountAssetIn, actual received amount, decimals, assetReceiver, tToken, tTokenAssets, iToken and final beneficiary in one tamper-evident request; enforce one-time execution and explicit rounding rules; and reconcile each privileged call to settled balances. The issuer should retain deployable build identity, request/response records and exception handling sufficient for independent review.

Status. Applicable design boundary; private service implementation and controls not assessed.

O02 | A 4-of-6 operator Safe controls the mutable OFT trust graph

Attribute	Record
Affected components	Ethereum ThBillOFTAdapter; Arbitrum, Base and HyperEVM ThBillOFT; peers, owners and LayerZero delegates
Classification	Privileged cross-chain control observation. No implementation-vulnerability severity assigned.
Evidence	E01; S01, S04-S05

Description. All four OFT deployments were owned by operator Safe 0x94877640dD9E6F1e3Cb56Bf7b5665b7152601295, publicly identified as 4-of-6. The fixed-height peer matrix was complete and symmetric, but owner-authorized peer, delegate or configuration changes can alter the trusted message graph after the observation point.

Impact and preconditions. Compromise, collusion or erroneous authorization at the OFT owner could redirect trusted peers, disrupt bridging or admit an unintended remote source. The risk requires valid owner authority; no ordinary-caller path to setPeer or owner functions was established. Safe signer custody and approval procedures were not assessed.

Recommendation. The OFT operator should maintain a signed deployment/EID/peer manifest, require independent review for every setPeer, delegate or endpoint change, monitor configuration events on all supported chains, and reconcile canonical custody, in-flight messages and every sidechain supply before and after changes. Emergency removal procedures should preserve pending-message and recovery records.

Status. Peer graph correctly configured at the assessed blocks; later changes and organizational controls not verified.

003 | thBILL, tULTRA, ULTRA shares and fund custody are distinct assurance layers

Attribute	Record
Affected components	Canonical thBILL, tULTRA, Router/backing wallet, OFT representations and off-chain fund records
Classification	RWA integration/control observation; not a demonstrated contract defect
Evidence	E01, E06; S06-S09

Description. Canonical thBILL is an on-chain wrapper configured against tULTRA. OFT units are bridged representations backed by canonical tokens locked in the Ethereum adapter. Those relationships are publicly observable. The further conversion of tULTRA pending/optimistic positions into formal ULTRA shares, the legal holder register, fund assets/liabilities and custody records are not publicly closed at the same cutoff. The official backing wallet is an operational address, not by itself proof of reserves.

Impact and preconditions. An integrator that treats an OFT balance, adapter custody balance, canonical total supply or tULTRA conversion view as a complete legal-ownership or reserve attestation may overstate redeemability and settlement finality. No undercollateralized OFT condition was observed at the synchronized snapshot, but that result does not establish the deeper fund-level backing chain.

Recommendation. The issuer and fund operator should publish reconciliations that separately identify canonical thBILL supply, adapter custody, each OFT supply, tULTRA assets, pending/optimistic amounts, finalized ULTRA shares and the authoritative legal/custody records at aligned cutoffs. Integrators should distinguish bridge completion, wrapper redemption, underlying-token eligibility and final cash or fund settlement.

Status. Applicable to the disclosed architecture; private fund and settlement records not assessed.

Classification criteria

Where an implementation vulnerability is established, severity considers supported impact, realistic preconditions and reachability. Control observations describe material trust or integration dependencies without establishing a contract defect. Scope limitations identify claims the available evidence cannot support. Neither observations nor limitations are included in vulnerability totals.

7 RWA Linkage and Public Verifiability

thBILL is not presented in the retained public evidence as direct ownership of an underlying Treasury security. It is a NAV-accumulating wrapper within Theo's mint/redeem arrangement. At the assessed Ethereum block, the canonical contract was configured against tULTRA; the cross-chain layer then represented canonical thBILL through lock/unlock and burn/mint OFT accounting. [E01, E06; S06-S09]

Layer / assertion	Available public evidence	Assurance boundary
Canonical wrapper	Ethereum proxy, exact-matched IToken implementation, supply and sole tULTRA asset were recorded. [E01-E02]	Establishes current on-chain configuration, not fund-level reserve coverage.

Layer / assertion	Available public evidence	Assurance boundary
tULTRA conversion	Public wrapper interfaces expose conversion/accounting behavior; tULTRA recipient restrictions remained effective. [E01-E04]	Pending/optimistic tULTRA amounts to finalized ULTRA shares were not privately reconciled.
Cross-chain representation	Four-chain peers, adapter custody and sidechain supplies reconciled at synchronized blocks. [E01]	Point-in-time OFT conservation; surplus not attributed message by message.
Operational backing wallet	Theo's public address manifest identifies 0xAE Cc546baFB16735b273702632C8Cbb83509d 8F. [S01]	An EOA balance or label is not a reserve attestation or custody proof.
Legal fund rights and custody	Theo product pages describe yield, mint and redeem arrangements. [S06-S09]	Legal register, investor priority, fund assets/liabilities and custodian records were not independently obtained.

The public evidence supports the canonical-to-tULTRA and canonical-to-OFT mechanics at the recorded snapshots. It does not close a same-cutoff chain from tULTRA to formal ULTRA legal shares and the underlying fund portfolio/custody. This report therefore does not assign a reserve-coverage percentage, opine on insolvency priority or treat the backing-wallet label as proof of assets.

8 Limitations and Conclusion

ID	Limitation	Effect on conclusions
L01	The private production mint service controlling MINTER_ROLE was unavailable, including its build, authentication, quote, replay, decimal, amount and beneficiary-binding logic.	The report confirms Router authorization and parameter flexibility but provides no assurance that private service requests are correctly authenticated, bound or reconciled.
L02	Private tULTRA/ULTRA settlement, legal register, portfolio, liabilities, custody and cash-settlement records were not obtained.	No legal-share, reserve, solvency, custody, completed-redemption or financial-statement assurance is provided.
L03	The peer graph and custody/supply reconciliation are fixed-height observations; the 248.111930 thBILL adapter surplus was not attributed message by message.	The report supports the absence of aggregate undercollateralized sidechain issuance at the snapshot, not continuous or transaction-level conservation.
L04	Validation was targeted and read-only; no production write, full regression/property suite, formal verification or privileged end-to-end operation was performed.	Sampled guards and states do not establish complete behavior across every caller, message order, failure mode or future version.
L05	Public terms support transferable thBILL and gate direct mint/redeem access, but private fund documents may contain additional eligibility obligations.	The report concludes that no public continuous-holder invariant was established; it does not provide a legal-compliance opinion or foreclose reassessment on new authoritative requirements.

Conclusion

The retained source correspondence, synchronized configuration/custody observations, separately anchored eligibility checks, role-history reconstruction and peer matrix support the stated conclusions for the canonical Ethereum wrapper, Router authorization boundary and four-chain OFT system. No reportable implementation vulnerability was confirmed in the examined paths.

The result must not be extended to the private mint service or to the complete RWA backing chain. Material changes to the canonical implementation, supported assets, Router roles/account delegation, OFT owner/delegate, endpoints, peers, supported chains, supply or public/legal product requirements require reassessment.

This public-evidence assessment was not commissioned by the issuer. It does not guarantee the absence of undiscovered vulnerabilities and does not constitute a financial audit, reserve attestation, legal opinion, regulatory-compliance opinion or investment recommendation.

A Deployment and Authority Inventory

Ethereum canonical and minting components

Component	Address / identity	Recorded state
Canonical thBILL proxy	0x5FA487BCa6158c64046B2813623e20755091DA0b	Implementation 0x325478a069b0dbbdfbee909fa3741f84259ba519; unpaused; 6 decimals
Canonical IToken implementation	0x325478a069b0dbbdfbee909fa3741f84259ba519	Runtime Keccak-256 0x5b0645110549d0d5e52b855323423d224b908c03836adaf90e4ca482f4a3b126
Configured tULTRA asset	0x82b840b6eDf77f90C92a70b99f0B5d50E7967330	Sole supported canonical asset; ONLY_WHITELISTED observed at the separate eligibility-check block 26,074,031
TTOKENRouterV2	0x8a2c307D1462Ff4fA98c9c119D3A3457AD505Eb1	Runtime Keccak-256 0x4196bb916cde2a9dbe7843a12342f720b7f69222eff576cc14cd05aa7468c450
Current MINTER_ROLE holder	0x0f21ee679e40123dea03cc64983035ce24bffc3	EIP-7702 delegation to Simple7702Account 0xe6cae83bde06e4c305530e199d7217f42808555b
Canonical administrator	0x2bB4b7E6E83FA6b77d0143dad631843cB73DCA02	Sole surviving DEFAULT_ADMIN_ROLE; official Ethereum timelock
Official backing wallet	0xAECCa546baFB16735b273702632C8Cbb83509d8F	EOA/control-surface address; not treated as reserve proof

Ethereum configuration/custody snapshot: block 26,077,438; 28 September 2026, 17:26:59 UTC.

Hash: 0x1fa48d3bca0b9f6071a4c67f57c39803280c423d3321e60e67e8163ebc13a8b6

Separate eligibility checks: block 26,074,031; 28 September 2026, 06:02:59 UTC.

Hash: 0x41426f085bdd1ac9335b71842622b35b9ab0900c396063501dac564902d8df6d [E01-E02]

Four-chain OFT mesh

Network / EID	Contract / type	Endpoint / observation
Ethereum / 30101	0xfDD22Ce6D1F66bc0Ec89b20BF16CcB6670F55A5a ThBillOFTAdapter	0x1a44076050125825900e736c501f859c50fE728c block 26,077,438
Arbitrum / 30110	0xfdd22ce6d1f66bc0ec89b20bf16ccb6670f55a5a ThBillOFT	0x1a44076050125825900e736c501f859c50fE728c block 509,774,894
Base / 30184	0xfdd22ce6d1f66bc0ec89b20bf16ccb6670f55a5a ThBillOFT	0x1a44076050125825900e736c501f859c50fE728c block 51,913,540
HyperEVM / 30367	0xfdd22ce6d1f66bc0ec89b20bf16ccb6670f55a5a ThBillOFT	0x3A73033C0b1407574C76BdBAC67f126f6b4a9AA9 block 47,132,570

All four contracts were owned by 4-of-6 operator Safe 0x94877640dD9E6F1e3Cb56Bf7b5665b7152601295. The Ethereum adapter constructor delegate was 0x22Cf1b8B3Ee6be94082aedadAc9596036163F568. Each non-self peer resolved to the bytes32 form of 0xfdd22ce6d1f66bc0ec89b20bf16ccb6670f55a5a. [E01]

Arbitrum block hash: 0xe24134fd91159f9434d2674d53f012a448e4917389cb299f789db884422ddfca

Base block hash: 0x04cc774414550dbf40b7ffc0434eebbd25bda35e9dfc7e749e0f74d42b34df7d

HyperEVM block hash: 0xcb5e48bf042c5a1bad4e6284ebdae4608c572a2f586a6fcfeb50e9961af655d7

B 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	thBILL deployed-contract and cross-chain configuration assessment
E02	Canonical IToken fixed-block behavior record
E03	Canonical IToken and tULTRA eligibility assessment
E04	Public thBILL holder and redemption model assessment
E05	thBILL deployment and source registry
E06	Tokenized Treasury RWA anchor and public-verifiability assessment
E07	Tokenized Treasury asset-scope and limitation summary

Primary public sources

S01 | Theo deployed addresses

Observed 29 September 2026; current canonical, Router, backing-wallet, OFT, Safe and timelock identities.

S02 | Etherscan canonical thBILL proxy

Canonical proxy and implementation identity used by the retained fixed-block review.

S03 | Sourcify TTokenRouterV2 source record

Exact production Router source and compilation record retained in the deployment registry.

S04 | Etherscan ThBillOFTAdapter source

Exact Ethereum adapter source and decoded constructor binding.

S05 | LayerZero OFT technical reference

Official lock-or-burn and mint-or-unlock model, peer semantics and shared-decimal boundary observed 29 September 2026.

S06 | Theo thBILL product description

Public product and wrapper description retained in the business and RWA assessments.

S07 | How thBILL generates yield

Public NAV/yield and layered backing description retained in the RWA assessment.

S08 | Theo thBILL mint and redeem

Public direct mint/redeem eligibility and process description.

S09 | Theo legal terms

Observed 29 September 2026; public self-custody, Platform/Services compliance, bridge and Dapp boundary.

S10 | Theo documentation overview

Public description of token holding, wallet/application integration and DeFi use retained in the eligibility assessment.

Scope attachment**thbill-scope-manifest-en.json**

SHA-256: a4220546af8e4e33952bb79c66044d9fec982a956ddd9f5117fcd13b4417faf