

TBILL

Multi-Chain Public-Deployment Security Assessment

OpenEden TBILL
Evidence-bound review of the Ethereum, Arbitrum One and BNB Smart Chain deployments

REPORT	B3-TBILL-2026-001
ISSUED	1 October 2026
BASELINE	Technical evidence through 29 September 2026; public product/RWA evidence through 30 September 2026
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 and Coverage 7

6 Findings and Control Observations 8

7 RWA Linkage and Public Verifiability 10

8 Limitations and Conclusion 11

A Deployment and Configuration Inventory 12

B Evidence and Source Index 12

Assessment of identified public TBILL Vault V5 deployments, supporting controls and recorded validation. Exact observation points, methods and exclusions are defined in Section 2.

1 Executive Summary

bench3.ai assessed the public OpenEden TBILL Vault V5 deployments on Ethereum, Arbitrum One and BNB Smart Chain. The review covered deployment and source identity, initialization and upgrade boundaries, KYC-gated subscriptions, queued and instant redemption paths, price freshness, fees and configured limits, and the distinction between on-chain TBILL accounting and the fund's private valuation, register and custody records. [E01-E07]

Assessment conclusion

No reportable implementation vulnerability or confirmed ordinary-investor loss was established at the recorded configurations. The contracts accept a price almost seven days old, but every inspected production price increase was below the approximately 10.0075 bps weekday round-trip break-even, ordinary redemption is queued and operator processed, and the governing repricing/equalization/cancellation policy is private. The stale-NAV question is therefore a material business-invariant limitation, not a confirmed exploit. [E02, E04, E07-E08]

Classification	Recorded result
Confirmed vulnerabilities	Critical 0 High 0 Medium 0 Low 0
Control observations	3; stale-NAV policy boundary, unused FeeManager maxima, dormant Ethereum instant-redemption mismatch
Material limitation	The controlling stale-NAV and oracle-outage dealing rules were not publicly available.

Material residual risk

A whitelisted investor can subscribe while the latest oracle value remains younger than the contract's seven-day threshold. If a later upward NAV correction exceeds fees, and if the resulting allocation is final rather than repriced, equalized, cancelled or clawed back, the stale mint can dilute prior holders. Those conditions were not established together: the actor cannot cause the price delay or update, no inspected update crossed break-even, and the current PPM or signed dealing policy was unavailable. The report does not convert this absent business invariant into a confirmed loss. [E02, E04, E07-E08; B3-TBILL-O01; L01]

TBILL remains administratively controlled. The operator processes queued redemptions; the maintainer can cancel queue entries and burn tokens; KYC administrators can revoke eligibility; and contract owners control upgrades and configuration. These powers can contain or correct incidents but are trust dependencies, not automatic proof that every economically adverse subscription would be reversed. [E02-E03]

2 Scope and Assessment Basis

2.1 Deployment baseline

Network	Vault proxy / implementation	Recorded observation
Ethereum (1)	0xdd50C053C096CB04A3e3362E2b622529EC5f2e8a 0xc4545bf80f935894cbe138d86b506923dab7c048	Block 26,077,383; rechecked 26,077,515. Exact Sourcify V5 implementation match.
Arbitrum One (42161)	0xF84D28A8D28292842dD73D1c5F99476A80b6666A 0x78365404fc5edabef6eca2f6b2f1ba1471727a07	Block 509,772,263; rechecked 509,778,452. Source/runtime identity recorded.
BNB Smart Chain (56)	0x5b4681F0d7A01B817675F25892D3Ad73572FD1D9 0xf3c7bbd9f91de0664a3e2ec5063e45872da472d9	Block 124,563,075; rechecked 124,566,623. Normalized runtime matches official V5 source.

The latest issuer-controlled source baseline retained by the workpapers is OpenEdenHQ/openeden.vault.audit commit 4410d1b495deea7c484582fd67aab6df5ec4a77a, authored 15 July 2026. Ethereum and Arbitrum use exact or recorded source correspondence; BNB Vault and KYC runtimes were normalized for UUPS immutable references and matched to the same official source family. [E03; S02]

2.2 Included components and methods

Scope element	Extent of assessment
Vault V5 and dependencies	Proxy/implementation identity; FeeManager, Controller, KYC Manager, price oracle, Partnership and redemption dependency relevant to subscriptions and redemptions.
Production configuration	Read-only fixed-block and fresh-tip observations of initialization, owners, pause state, fees, limits, supply caps, supply, price age and redemption configuration.
Behavioral validation	Archived local fork tests for maximum-limit behavior and the Ethereum instant-redemption ABI mismatch; historical price-update analysis. No production transaction was signed or broadcast.
Business boundary	Current public product, subscription, redemption, price, governance and user-agreement materials. Private PPM, investor register, administrator records and settlement operations were unavailable.

Methods comprised retained source review, exact/normalized runtime correspondence, read-only RPC and event-history analysis, archived fixed-block fork tests and public-policy review. Tests described in Section 5 were inherited workpapers; report preparation did not rerun them or add assessment coverage. [E02-E08]

2.3 Exclusions

Excluded are the current private PPM and Subscription Agreement, investor and legal ownership registers, fund administrator calculations, complete portfolio and custody records, off-chain onboarding decisions, operator runbooks, payment rails, signer custody and organizational approvals. This report is not a financial audit, reserve attestation or opinion that every public or private TBILL operation was tested. [E07, E09]

3 System and Threat Model

TBILL Vault V5 accepts an underlying settlement token from approved investors, deducts the applicable fee and mints TBILL using an externally maintained TBILL/underlying rate. Ordinary redemption escrows a holder's shares in a FIFO queue and is completed by an authorized operator using the rate and fee effective at processing. On-chain supply represents tokenized claims in the product model; it does not itself prove the fund's securities, liabilities, legal register or cash settlement. [E02-E04; S03-S05]

Actor / layer	Authority	Security boundary
Approved investor	Deposit, transfer among eligible accounts and request redemption of owned TBILL.	Cannot update NAV, administer KYC, process the queue or move another holder's units through ordinary functions.
Price operator / administrator	Publish close NAV and on-chain price subject to configured deviation controls.	Price timeliness and accuracy are trusted operational inputs; the ordinary investor does not control them.
Operator / maintainer	Process or cancel queued redemptions; maintain operational state; burn balances through authorized paths.	Containment and correction depend on authorized private operations and policy.
Owner / upgrade authority	Change implementations and supporting configuration.	Integrity of ownership, key custody and deployment approvals was not independently verified.
Fund and service providers	Calculate NAV, hold portfolio assets, maintain legal records and settle cash.	Private records remain outside the public-contract assessment.

3.1 Security objectives

The examined objectives were: only initialized, authorized contracts and roles may change supply or configuration; subscriptions remain paid and KYC-gated; redemptions cannot exceed the caller's owned position or force unavailable liquidity; price-age handling does not silently imply an unsupported economic entitlement; and configuration fields are not credited as controls unless the active execution path consumes them.

4 Technical Assessment

4.1 Deployment, initialization and authorization

All three Vault proxies were initialized, had nonzero owners and selected the V5 implementations listed in Section 2. Read-only initializer calls reverted as already initialized. The BNB KYC proxy likewise matched the official KycManager source after normalization, was initialized, had strict mode enabled and required UPGRADE_ROLE for implementation changes. The reviewed public-takeover conditions were therefore not substantiated at the recorded blocks. [E02-E03]

4.2 Per-chain operating configuration

Network	FeeManager / Controller	Recorded admission and liquidity controls
Ethereum	0x99C913B3cBDdCFC7eD49Ff19B00704286a4B3b6B 0x377de6729507Bb0E56E0AAC666bd8522E4A3fe41	Deposit/redeem 5/5 bps on workdays and 10/10 bps on holidays; min fee 0; deposit and withdrawal unpaused; minimum 1 USDC; configured maximum 25,000,000 USDC; unlimited supply cap.
Arbitrum One	0x965738d072F2a37fEE9DFf572Bf517068cFFEa39 0xC6773ba1Ff30Cc9b14972225924a21FF7fDCd01F	Same fee and pause state; minimum 1 USDC; configured maximum 25,000,000 USDC; unlimited supply cap.
BNB Smart Chain	0xAa311E05f20B5e3D28B56f012B4560f1e405f4d7 0xDAe70F90620Bcbb7D7B3b536683bB2BA257e0fc9	Same fee and pause state; minimum 1 underlying unit; configured maximum 10,000,000 underlying units; unlimited supply cap. Underlying uses 18 decimals.

Vault V5 reads the configured minimum deposit and withdrawal values but discards both maximum values. Archived three-chain fork tests demonstrated that above-maximum deposits remain fully paid and KYC-gated and that above-maximum queued redemptions escrow only the caller's shares. Public subscription and redemption materials publish minimums and permit full-investment redemption but do not publish these maxima. The fields are therefore treated as stale/dead configuration or an unverified product-policy discrepancy, not as a confirmed loss-prevention control. [E02, E05; B3-TBILL-O02]

4.3 Price freshness and subscription economics

Vault V5 rejects the oracle value only after its age exceeds seven days. An eligible investor can therefore subscribe at a stale-but-contract-valid price. The investor cannot publish or choose the subsequent NAV. A profitable weekday round trip requires an upward correction greater than approximately 10.0075 bps before gas, capital cost and operational intervention; the threshold is greater than approximately 20.0300 bps under 10/10 bps holiday fees. [E02-E04]

$$\text{net return} = (1 - \text{deposit fee}) \times (\text{new NAV} / \text{old NAV}) \times (1 - \text{redemption fee}) - 1$$

5 bps + 5 bps break-even: NAV increase > approximately 10.0075 bps

The retained Ethereum history contained 123 price updates through 25 September 2026 and the retained Arbitrum history contained 51. The largest positive move on either chain was 7.9536 bps; no inspected increase exceeded the minimum round-trip fee. A modeled 15 bps correction produced measurable dilution, while a 9.5 bps control remained unprofitable. Those models establish the mechanism and threshold, not a realized or currently reproducible loss. [E04, E08]

Public User Agreements reserve broad power to delay or decline issuance/redemption and incorporate non-public PPMs and Subscription Agreements. They do not define the maximum permitted NAV age or mandatory pause, repricing, equalization, cancellation/refund, cutoff or clawback treatment. This missing business invariant prevents the report from deciding whether a threshold-crossing stale subscription would be final or corrected. [E07; B3-TBILL-O01; L01]

4.4 Redemption paths and atomicity

Ordinary redemption is a queued process. The investor escrows owned TBILL, and the operator later values and settles requests against available on-chain assets. Queue processing stops when liquidity is insufficient; the maintainer can cancel requests and return shares. This does not force an unfunded settlement and does not provide atomic stale-NAV extraction. [E02-E05; S05]

Only Ethereum has a nonzero instant-redemption dependency: Circle Redemption at 0x31D3F59Ad4aAC0eeE2247c65EBE8Bf6E9E470a53. Vault V5 expects redeem(uint256) to return uint256, while the configured Circle implementation returns no data. Archived exact-runtime validation showed that, once other dormant prerequisites were locally supplied, the typed call reverted on zero-length return decoding and rolled back every token movement. At the pinned production state, the Vault also held no required BUIDL, had no allowance, Circle Settlement was paused and liquidity was zero. The path is a dormant Informational configuration defect, not a fund-loss path. [E06; B3-TBILL-O03]

5 Recorded Validation and Coverage

The following results are recorded in retained workpapers. They are differentiated as read-only observation, local-model/fork validation or business-policy review; none was newly executed for this report.

ID	Recorded check	Outcome and limit
V01 read-only	Vault/KYC initialization, owner and implementation state on all three chains	Initialized and nonzero authorized ownership recorded; no public initializer or unprivileged upgrade takeover established.
V02 history	Ethereum and Arbitrum oracle-update series	Largest positive update 7.9536 bps, below 10.0075 bps weekday break-even. This does not prove future threshold-crossing moves impossible.
V03 local validation	Deposits and queued redemptions above configured FeeManager maxima	Operations remained paid, KYC-gated and backed; no third-party value extraction was observed.
V04 dependency validation	Ethereum redeemIns with current Circle dependency	Current state stops before settlement; the retained dependency validation showed atomic rollback on incompatible return decoding.
V05 economic and control assessment	Seven-day stale-NAV model and production economics	Mechanism real; 15 bps model profitable, 9.5 bps control unprofitable; no qualifying production event and no governing finality/remedy policy established.
V06 policy review	Current public User Agreements and product documentation	Broad discretion and daily NAV expectation recorded, but no objective stale-NAV handling rule.

5.1 Interpretation of negative and local tests

Initializer reverts support the recorded initialization boundary but do not test every authorized upgrade. Fork tests prove the active Vault predicates under their documented overrides; they do not establish private-policy acceptance or end-to-end fund settlement. Price history is a bounded historical sample, not a guarantee about future NAV movement. Atomic rollback of redeemIns refutes persistent asset loss on that path but does not make a dormant product feature available.

6 Findings and Control Observations

No implementation vulnerability with confirmed ordinary-actor loss was identified. The following observations are excluded from vulnerability severity totals. No issuer response or remediation verification was provided to bench3.ai.

ID	Title	Classification / status
B3-TBILL-001	Stale-NAV acceptance cannot be classified without the governing dealing policy	Business-invariant control observation; unresolved scope limitation
B3-TBILL-002	Vault V5 does not consume configured maximum deposit and withdrawal values	Informational configuration observation; applicable at snapshot
B3-TBILL-003	Ethereum instant redemption is configured to an incompatible no-return dependency	Informational operational observation; dormant at snapshot

001 | Stale-NAV acceptance cannot be classified without the governing dealing policy

Attribute	Record
Affected components	Vault V5 price-age check; price oracle; subscription and queued-redemption processes
Classification	Control observation and material limitation; no implementation-vulnerability severity assigned
Evidence	E02-E04, E07-E08; S03-S06

Description. Vault V5 may mint against a price almost seven days old. A threshold-crossing upward correction can transfer value to the stale-price subscriber in a model. Current public terms neither establish that outcome as an intended final allocation nor define a mandatory correction. The decisive PPM or signed dealing rule was unavailable.

Impact and preconditions. Potential dilution requires an already approved investor, an externally caused delay, an upward NAV correction exceeding all fees and costs, sufficient capacity, later settlement, and a policy that lets the investor retain the allocation. No inspected production update met the economic threshold, and the finality/remedy condition is unproven. No confirmed exploitable loss is assigned.

Recommendation. The fund operator should define and enforce a maximum NAV age aligned with weekends and holidays and publish or provide a privacy-safe policy excerpt specifying pause, cutoff, repricing/equalization, cancellation/refund and clawback treatment. The contract operator should automatically pause subscriptions when that age is exceeded or when required price publication fails.

Status. Unresolved scope limitation; no issuer response or remediation evidence recorded.

O02 | Vault V5 does not consume configured maximum deposit and withdrawal values

Attribute	Record
Affected components	OpenEdenVaultV5Impl.deposit, redeem and redeemIns; FeeManager maxima
Classification	Informational configuration/interface observation; no vulnerability severity assigned
Evidence	E02, E05

Description. FeeManager retains finite, owner-managed maximum values, but Vault V5 reads only the minima. Above-maximum subscriptions and queued redemptions succeeded in the archived three-chain fork suite. Public product terms do not publish the maxima, and all live supply caps were unlimited.

Impact and preconditions. An approved investor can exceed the displayed configuration. The tested deposits remained fully paid and the redemptions used only the caller's shares; no unbacked mint, forced payout, KYC bypass or third-party loss was demonstrated. Impact would depend on a separate binding policy that treats these fields as mandatory controls.

Recommendation. The contract operator should either remove and deprecate the unused maximum fields or restore checks with explicit per-transaction, per-address or rolling-flow semantics. Deployment monitoring should reject finite maxima when the selected Vault implementation does not consume them.

Status. Applicable at the recorded snapshots; no issuer confirmation of policy intent recorded.

O03 | Ethereum instant redemption is configured to an incompatible no-return dependency

Attribute	Record
Affected components	Ethereum Vault V5 redeemIns; Circle Redemption 0x31D3...0a53
Classification	Informational operational/configuration observation; no asset-loss severity assigned
Evidence	E02-E03, E06

Description. Vault V5 expects a uint256 return, while the configured Circle Redemption function returns no data. At the pinned state, independent prerequisites also made instant redemption inactive. Exact-runtime validation isolated the mismatch and showed deterministic atomic rollback once those prerequisites were supplied.

Impact and preconditions. Current impact is dormant feature unavailability and caller gas loss; queued redemption remains active. No share burn or settlement movement persists after the revert. A future reactivation without replacing the dependency would make the function deterministically unavailable, not create a demonstrated fund-loss path.

Recommendation. The contract operator should keep instant redemption disabled until a returning adapter is configured and migration tests verify returndata, allowance, compliance and liquidity prerequisites. If instant redemption is retired, the exposed configuration and user interface should be removed or clearly deprecated.

Status. Dormant at the recorded Ethereum snapshot; no remediation verification recorded.

Classification criteria

Severity is assigned only when the evidence establishes an implementation defect, realistic reachability and supported impact. Business-policy gaps, privileged powers and inactive operational defects are reported separately and do not increase the confirmed-vulnerability count.

7 RWA Linkage and Public Verifiability

TBILL represents a proportional contractual claim linked to the net redemption value of an OpenEden professional fund. Public materials describe token price as fund NAV, less accrued fees, divided by outstanding TBILL. Settlement USDC held by a Vault is not the fund's Treasury, repo, money-market-fund or other portfolio inventory. [E09; S03, S07-S09]

Assertion	Available public evidence	Assurance boundary
Product and deployment identity	Issuer documentation and repository identify three production Vaults and supporting components. [S01-S02]	Public attribution applies to listed addresses and recorded versions only.
Price mechanism	Oracle-fed NAV-per-token calculation and on-chain price history are public. [S03]	The fund administrator's inputs, liabilities and same-cutoff calculations were not independently audited.
On-chain quantity	Vault supply and settlement balances were observed at fixed blocks. [E03-E05]	Supply is not a same-time legal-register or custody reconciliation.
Fund/legal structure	BVI regulated-entity record and product documents describe the professional-fund structure and service-provider model. [S07-S09]	Private PPM, holder register, portfolio and signed administrator/custodian reports were unavailable.

Public evidence supports the described linkage mechanism but cannot close, at one cutoff, the chain from aggregate token supply to legal investor records and underlying assets and liabilities. This report does not assign a reserve-coverage percentage or treat on-chain settlement liquidity as proof of fund assets.

8 Limitations and Conclusion

ID	Limitation	Effect on conclusions
L01	The current PPM or signed stale-NAV/oracle-outage dealing policy was unavailable.	The report cannot decide whether a threshold-crossing stale subscription is final, repriced, equalized, cancelled, refunded or clawed back; O01 is not classified as a confirmed loss.
L02	Private fund, legal-register, custody, NAV-input and settlement records were outside scope.	No assurance is provided over legal ownership, portfolio existence, NAV correctness, payment completion or reserve sufficiency.
L03	Signer custody, organizational approvals and operator runbooks were not independently verified.	Observed role restrictions do not establish the effectiveness of off-chain governance, incident response or key security.
L04	Behavioral validation was targeted and inherited; historical price analysis was bounded.	The workpapers do not establish complete path coverage or guarantee that future fees, prices, liquidity and configurations remain within recorded bounds.

Conclusion

The reviewed deployments were initialized and source-bound as described, and the recorded subscription and redemption tests did not establish unbacked minting, unauthorized asset movement or a current profitable stale-NAV extraction. No reportable vulnerability was confirmed. The unresolved stale-NAV business invariant remains material and must not be represented as a verified safety property.

The conclusions apply only to the listed deployments, configurations and observation dates. A change to Vault implementation, FeeManager semantics, oracle policy, fees, eligibility, redemption adapter or fund dealing rules requires reassessment.

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

A Deployment and Configuration Inventory

Network	Component	Address
Ethereum	Vault / Price Oracle / KYC Manager	0xdd50C053C096CB04A3e3362E2b622529EC5f2e8a 0xCe9a6626Eb99eaeA829D7fA613d5D0A2eaE45F40 0x51Be497AcEd1a2C19f6151064301e356B020D947
Ethereum	FeeManager / Controller / instant Redemption	0x99C913B3cBDdCFC7eD49Ff19B00704286a4B3b6B 0x377de6729507Bb0E56E0AAC666bd8522E4A3fe41 0x31D3F59Ad4aAC0eeE2247c65EBE8Bf6E9E470a53
Arbitrum One	Vault / Price Oracle / KYC Manager	0xF84D28A8D28292842dD73D1c5F99476A80b6666A 0xc0952c8ba068c887B675B4182F3A65420D045F46 0x0d7690bAa1008c8d3C5dae9D5033FF846738BAfB
Arbitrum One	FeeManager / Controller	0x965738d072F2a37fEE9DFf572Bf517068cFFEa39 0xC6773ba1Ff30Cc9b14972225924a21FF7fDCd01F
BNB Smart Chain	Vault / Price Oracle / KYC Manager	0x5b4681F0d7A01B817675F25892D3Ad73572FD1D9 0x3347d0C6e2Bd23b1148Fbb7fEF5f0fED281612A8 0xd9cf8C5bB16422d992595f3e3342De25fE7F5cf9
BNB Smart Chain	FeeManager / Controller	0xAa311E05f20B5e3D28B56f012B4560f1e405f4d7 0xDAe70F90620Bcbb7D7B3b536683bB2BA257e0fC9

Addresses are issuer-listed or recursively resolved components retained in the workpapers. Inventory inclusion does not imply that every function of every component received equal review depth. [E03, E10]

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	Tokenized Treasury production assessment summary
E02	TBILL deployment and control assessment
E03	TBILL public deployment, source and configuration assessment
E04	TBILL production-state and oracle-history evidence
E05	TBILL FeeManager maximum-limit recheck
E06	TBILL Ethereum instant-redemption independent validation
E07	TBILL public stale-NAV policy refresh
E08	TBILL stale-NAV economic and business-policy assessment
E09	Tokenized Treasury RWA anchor and public-verifiability assessment
E10	Original Tokenized Treasury asset scope registry

Primary public sources

S01 | OpenEden TBILL smart-contract addresses

Issuer deployment attribution retained in the assessment evidence.

S02 | OpenEden Vault audit repository at assessed commit

Official source baseline observed for the 2026-09-29 assessment.

S03 | OpenEden TBILL token price

NAV-per-token and oracle-publication model; accessed in the 2026-09-29 policy review.

S04 | OpenEden TBILL subscriptions

KYC subscription and prevailing-price description; accessed in the 2026-09-29 policy review.

S05 | OpenEden TBILL redemptions

Queued processing, pricing and timing description; accessed in the 2026-09-29 policy review.

S06 | OpenEden TBILL user agreements

Public US and non-US agreements reviewed on 2026-09-29; incorporated PPMs were not publicly linked.

S07 | OpenEden TBILL product structuring

Product, fund-interest and service-provider context retained in the evidence.

S08 | BVI FSC - Treasury Bills Institutional Liquidity Limited

Public regulated-entity record used for the RWA linkage assessment.

S09 | OpenEden trust and transparency

Public description of fund administration, custody and reporting; not a same-cutoff reserve attestation.

Scope attachment

tbill-scope-manifest-en.json

SHA-256: 61a4d3384c18dc2dab4f29ec3f44ee9e0114e5cca80cc6b31d2d60901c3dde26