

# OUSG

## Multi-Ledger Public-Contract and RWA-Linkage Assessment

Ondo Short-Term US Government Bond Fund  
Fixed-ledger and public-evidence assessment of Ethereum, Polygon, Solana and XRP Ledger

|          |                                             |
|----------|---------------------------------------------|
| REPORT   | B3-OUSG-2026-001                            |
| ISSUED   | 1 October 2026                              |
| BASELINE | Ledger observations dated 28 September 2026 |
| AUTHOR   | bench3.ai                                   |

# Contents

1 Executive Summary . . . . . 3

2 Scope and Methods . . . . . 4

3 System and Threat Model . . . . . 5

4 Technical Assessment . . . . . 6

5 Recorded Validation . . . . . 7

6 Findings and Control Observations . . . . . 8

7 RWA Linkage and Public Verifiability . . . . . 10

8 Limitations and Conclusion . . . . . 11

A Code and Observation Identities . . . . . 11

B Evidence and Source Index . . . . . 12

Assessment of identified public deployments, retained source-review records, fixed-ledger observations, recorded bounded validation and current primary published documentation. Private fund, transfer-agent, custody, dealing and legal-register records were outside the assessed boundary.

# 1 Executive Summary

bench3.ai assessed the identified OUSG public execution surfaces on Ethereum, Polygon, Solana and XRP Ledger. The work addressed deployment identity, permissioned transfers, privileged issuance and redemption, NAV consumption, dormant-network posture, non-EVM issuer controls, cross-ledger reconciliation evidence, and the public relationship between token balances and interests in Ondo I LP. [E01-E06; S01-S08; S10; S11]

**Assessment conclusion**

OUSG-KR-01 is an open known control risk: the reviewed TOKENIZED\_RWA price path exposes a timestamp but does not enforce a maximum age before use. The technical condition is established. Authoritative NAV-validity rules, the effectiveness of compensating operating controls and realistic economic exposure were not sufficiently evidenced to assign a risk rating. No investor-loss vulnerability was substantiated; that evidence limit is not a low-risk conclusion. Four additional control observations remain applicable to the assessed deployments.

| Classification                    | Recorded result                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Severity-assigned vulnerabilities | Critical 0   High 0   Medium 0   Low 0                                                                                                                |
| Known unresolved risks            | 1; OUSG-KR-01. Technical condition established; economic risk rating unassigned. This item is excluded from the severity totals above, not dismissed. |
| Control observations              | 4; privileged control, dormant-network reactivation, XRP Ledger operations and cross-ledger reconciliation                                            |
| Unconfirmed candidates            | 0                                                                                                                                                     |

## 2 Scope and Methods

### 2.1 Assessment basis

| Parameter       | Assessment basis                                                                                                                                                                                                                                                                       |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assessment type | Multi-ledger public-contract, recorded-state and RWA-linkage assessment; not a legal, financial-statement, reserve or full operational audit                                                                                                                                           |
| Evidence dates  | Ledger observations are archived at 28 September 2026, retained technical evidence runs through 29 September 2026, and primary documents were reviewed on 1 October 2026. The product page's portfolio snapshot is separately dated 30 September 2026 at 4:00 p.m. EDT. [E01-E06; S01] |
| Networks        | Ethereum, Polygon, Solana and XRP Ledger                                                                                                                                                                                                                                               |
| Methods         | Retained source correspondence review, fixed-block/slot/ledger observations, transaction-history analysis, bounded recorded local-model results, and current primary-document comparison                                                                                               |

### 2.2 Exact deployment inventory

Principal token and operational entrypoints are listed below. Appendix A records the retained EVM implementation and runtime-code identities. [E01-E03]

| Network  | Component and identifier                                        | Recorded identity or state point                                                                 |
|----------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Ethereum | OUSG token<br>0x1B19C19393e2d034D8F31ff34c81252FcBbee92         | Official issuer-listed proxy; fixed at block 26,077,885                                          |
| Ethereum | OUSGManager<br>0x93358db73B6cd4b98D89c8F5f230E81a95c2643a       | Retained source-matched manager; fixed at block 26,077,885                                       |
| Ethereum | Identity registry<br>0xc6958D69d535FD03BD6Df3F4fe6CDcd127D97df  | Official issuer-listed registry; fixed at block 26,077,885                                       |
| Ethereum | OndoOracle<br>0x9Cad45a8BF0Ed41Ff33074449B357C7a1fAb4094        | Official issuer-listed oracle; fixed at block 26,077,885                                         |
| Ethereum | OUSGOracleWrapper<br>0xADC4966E4F8CAAf12C777f07AA7A0Ae8D894cDf3 | Resolved live manager dependency in the archived observation                                     |
| Ethereum | Underlying oracle<br>0x0502c5ae08E7CD64fe1AEDA7D6e229413eCC6abe | Issuer-listed as Oracle (Legacy); resolved as the wrapper dependency in the archived observation |
| Polygon  | OUSG token<br>0xbA11C5effA33c4D6F8f593CFA394241CfE925811        | Official issuer-listed token; zero supply at block 94,611,786                                    |
| Polygon  | CashManager<br>0x6B7443808ACFCD48f1DE212C2557462fA86Ee945       | Official issuer-listed manager; paused at block 94,611,786                                       |

| Network    | Component and identifier                                                                            | Recorded identity or state point                                                           |
|------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Polygon    | Identity registry<br>0x7cD852c0D7613aA869e632929560f310D4059AC1                                     | Official issuer-listed registry; fixed at block 94,611,786                                 |
| Solana     | OUSG mint<br>i7u4r16TcsJTgq1kAG8opmVZyVnAKBwLKu6ZPMwzxNc                                            | Official issuer-listed legacy SPL Token mint; zero supply in slots 451,418,544-451,420,480 |
| Solana     | Circle recipient<br>EgFDCr2UmsoUvoJ5DcNZqVnkFzSDE9KyCYBHgcnrAd5G                                    | Official issuer-listed operational recipient; retained history reviewed                    |
| XRP Ledger | OUSG currency<br>4F55534700000000000000000000000000000000; issuer rHuiXXjHLpMP8ZE9sSQUsADQVWDww6h5p | Official issuer-listed issued currency; fixed at ledger 107,299,413                        |
| XRP Ledger | OUSG recipient rHPwrKvDexV5LF5tzKQmx7U7Ku2836DA1                                                    | Official issuer-listed operational recipient; fixed at ledger 107,299,413                  |
| XRP Ledger | RLUSD recipient rEZiJUjsputkS6VjPAwdRLESNpdYRC6ba;<br>destination tag 1                             | Official issuer-listed payment recipient; retained transaction history reviewed            |

The inventory identifies public entypoints, not legal ownership or reserve support. Appendix A and the attached scope record distinguish the primary Ethereum snapshot at block 26,077,885 from the independent price-path recheck at block 26,078,147; Polygon, Solana and XRP Ledger retain their own recorded state points. Source and code identities are recorded separately from public repository source. [E01-E03; S02]

## 2.3 Exclusions

Excluded were private offering and dealing documents, investor agreements, transfer-agent and limited-partner registers, fund-administrator workpapers, custody statements, signed NAV approvals, fiat and stablecoin settlement operations, internal sanctions and KYC systems, organization-level key custody, private incident records, and same-cutoff reconciliation across all ledgers.

### 3 System and Threat Model

### 3.1 Product and settlement model

Ondo describes OUSG as tokenized limited partnership interests in Ondo I LP, a Delaware limited partnership relying on Rule 506(c) and Investment Company Act section 3(c)(7). The public product model expresses fund performance through an increasing OUSG redemption price, while rOUSG provides a rebasing representation. Publicly described subscriptions and redemptions accept supported stablecoins around the clock, subject to eligibility, manager configuration, liquidity and off-chain fund operations. [S01; S10; S11]

| Actor or component | Trusted function                                                                           | Security relevance                                                                                         |
|--------------------|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Eligible investor  | Controls an approved address and submits subscription, redemption or transfer instructions | An ordinary eligible user is within the relevant state-price threat model; unauthorized users remain gated |
| Manager/operator   | Configures payment assets, limits, fees, pause state and transaction processing            | Misconfiguration or key compromise can affect issuance, liquidity access and incident response             |

| Actor or component                               | Trusted function                                                                         | Security relevance                                                                                          |
|--------------------------------------------------|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Oracle publisher and wrapper                     | Publishes NAV-derived prices and exposes the value consumed by manager paths             | Freshness, correctness and update continuity determine whether the on-chain dealing price is current        |
| Identity and compliance controls                 | Approve addresses and enforce transfer eligibility                                       | KYC gating narrows reachability but does not make an eligible user's economic path trusted                  |
| Fund administrator, transfer agent and custodian | Maintain the authoritative fund records, portfolio support and legal ownership processes | These private systems are necessary to establish NAV validity, beneficial ownership and final economic loss |
| Ledger-specific privileged controllers           | Control EVM roles, Solana mint/freeze authority and XRP Ledger issuer functions          | Compromise or inconsistent policy can affect supply, eligibility and recovery across networks               |

### 3.2 Principal trust boundaries

The principal public-code boundary is between a manager that can complete a token-for-stablecoin exchange and an oracle path whose `TOKENIZED_RWA` branch returns a price without enforcing the accompanying timestamp. Other material boundaries are the separation between token KYC and sanctions/blocklist operations, the reactivation of dormant deployments, native XRP Ledger issuer controls, and the absence of a public cryptographic conservation proof spanning Ethereum, Polygon, Solana and XRP Ledger. [E01-E03; S03-S05]

Price-age tolerance and economic impact are separate questions. The path does not enforce a maximum price age, but whether a value is invalid depends on the product's authoritative dealing calendar and NAV policy. Potential loss also depends on price divergence, available liquidity and limits, operational response and the treatment of completed instructions. The public website terms do not govern OUSG issuance and redemption economics, so repricing or recovery cannot be assumed to eliminate exposure. [E02; S08]

## 4 Technical Assessment

### 4.1 Ethereum and Polygon

At Ethereum block 26,077,885 on 28 September 2026, the retained review recorded an active OUSG deployment with total supply 1,075,264.489634584814798209 OUSG, an unpaused token and manager, KYC-gated transfer paths, zero default instant fees, minimum transaction settings around USD 5,000, and per-identity and global rolling limits. The resolved manager path used `OUSGOracleWrapper`, which in turn used the issuer-listed legacy underlying oracle. The recorded OUSG price was USD 116.684446 with a timestamp of 25 September 2026 at 21:27:35 UTC, approximately 69.48 hours before that fixed observation. [E01]

The reviewed deployed-source path for `TOKENIZED_RWA` obtains both a price and timestamp, but the wrapper and manager consume the price without a maximum-age check; the manager's `minimumRwaPrice` is a coarse lower bound rather than a freshness control. By contrast, the `AggregatorV3` path in the pinned published source contains a stale-data check. The Ethereum subscription and redemption operations reviewed in the workpapers were atomic at the EVM transaction layer, so a failed redemption does not leave a partial token burn; atomicity does not correct a successfully completed exchange at an old price. [E01; E02; S03-S05]

At Polygon block 94,611,786 on 28 September 2026, the OUSG token had zero supply, zero token minter and burner, and the listed manager was paused with instant minting disabled. That observation materially limits then-current public exposure, but it does not prove permanent retirement or define the controls required for later reactivation. [E01]

## 4.2 Solana and XRP Ledger

Across the retained Solana slot range 451,418,544-451,420,480, the legacy six-decimal SPL Token mint had zero supply and no positive-balance holders. Mint and freeze authority resolved to a Squads V3 vault controlled by a recorded 4-of-7 multisig with external execution disabled. The mint had remained at zero after the reviewed final burn of 624,604 OUSG on 20 April 2026. The legacy token had no transfer hook or destination allowlist; that is not a current exploit while supply is zero, but eligibility controls would require explicit review before reactivation. [E03]

At XRP Ledger 107,299,413 on 28 September 2026, the retained review recorded 1,605,617.725352341 OUSG of issued obligations, 29 trust lines, nine authorized lines, and five nonzero authorized lines. The issuer enabled RequireAuth and Clawback, retained an active master key and had no signer list. The RLUSD recipient used a 2-of-3 signer list with its master key disabled. Destination-tag enforcement required a tag for the recipient path, but public ledger rules did not prove that tag 1 alone was enforced. Issuance and redemption remained operationally staged rather than a single atomic cross-system action. [E03]

## 4.3 Cross-ledger consistency

The public evidence identifies official ledger entypoints and allows supply and history to be inspected at fixed points. It does not expose a cryptographic bridge or same-cutoff public proof that reconciles every ledger balance to a single legal limited-partner register. Historical burn and issuance timing can indicate a migration workflow, but timing alone is not proof of conservation or legal continuity. [E03; E06]

# 5 Recorded Validation

The retained workpapers record the following bounded validation results.

| Recorded check                                | Result                                                                                                                                                                                           | Boundary                                                                                                                     |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Ethereum deployment and source correspondence | The token proxy had exact Sourcify correspondence; the manager and oracle control flow was matched to retained Solidity 0.8.16 source. Current public 0.8.33 source preserved the material path. | Published repository source does not establish byte-for-byte correspondence with the deployed implementation. [E01; S03-S05] |
| Fixed Ethereum and Polygon state              | Roles, limits, pause state, supply, manager dependencies and oracle observations were recorded at exact blocks and hashes on 28 September 2026.                                                  | Point-in-time read-only evidence; not continuous monitoring. [E01]                                                           |
| Representative EVM transaction histories      | Retained histories showed completed subscription and redemption flows and supported the assessed atomic manager behavior.                                                                        | Representative transactions do not establish every operating path or legal finality. [E01]                                   |
| Stale-NAV control-flow model                  | Prior bounded local work established that the TOKENIZED_RWA path can use a price without a maximum-age rejection; independent review confirmed ordinary eligible-user reachability.              | The model did not prove a production incident, authoritative NAV divergence or retained third-party loss. [E02; E04]         |
| Solana and XRP Ledger assertions              | The retained read-only harness recorded 27 of 27 targeted assertions across mint, authority, trust-line, issuer-flag, signer and history checks.                                                 | A bounded assertion set is not a complete security proof; no transaction was submitted. [E03]                                |

| Recorded check                     | Result                                                                                                                                                                          | Boundary                                                                                                                                                             |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pinned published-source comparison | The pinned Ondo source omits a TOKENIZED_RWA age check. Issuer product, address and terms disclosures were compared with the retained evidence and historical audit disclosure. | The 0.8.33 published source was not bound to the 0.8.16 deployed code; deployed-source correspondence relies separately on the archived records. [E01; E02; S01-S08] |

## 6 Findings and Control Observations

### 6.1 OUSG-KR-01 — TOKENIZED\_RWA price freshness is not enforced

| Field                 | Assessment                                                                                                                                                                                                |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical status      | Known unresolved control gap; established in the reviewed path                                                                                                                                            |
| Risk rating           | Unassigned: authoritative NAV-validity rules, compensating controls and realistic economic exposure are not sufficiently evidenced. Absence of a recorded incident does not determine severity.           |
| Remediation status    | Open in the assessed implementation; no remediation verification or issuer response to this assessment is recorded.                                                                                       |
| Affected components   | Archived Ethereum OUSGManager, OUSGOracleWrapper and underlying TOKENIZED_RWA oracle path; pinned published OndoOracle, wrapper and BaseRWAManager source                                                 |
| Behavior established  | The price source returns a timestamp, but the reviewed wrapper and manager path use the price without enforcing a maximum age. minimumRwaPrice is not a substitute for freshness.                         |
| Impact qualification  | Economic consequences remain conditional and unquantified. The evidence does not establish an invalid dealing price, completed loss event or effectiveness of private correction and recovery procedures. |
| Historical disclosure | Code4rena L-01 described the missing staleness check in April 2024. Prior disclosure is background, not evidence of remediation or reduced audit significance. [S06; S07]                                 |

Description. A NAV-derived value can remain callable after its update timestamp becomes old because the relevant TOKENIZED\_RWA branch has no maximum-age rejection. The archived Ethereum observation demonstrated that the manager resolved through this path and recorded a roughly 69.48-hour-old value at its fixed block. The pinned official source retained the same control flow, but published source alone does not establish correspondence with the deployed implementation. [E01; E02; S03-S05]

Impact and preconditions. If an available dealing price is no longer valid under the fund's rules, subscriptions or redemptions can be priced on an outdated basis. The potential allocation of loss depends on the direction and size of the divergence, eligible-user access, liquidity, limits, operator intervention and enforceable correction procedures. The available record does not quantify that exposure. Eligibility and pause controls are relevant constraints, but their existence does not establish timely intervention or enforce NAV validity. [E02]

Assessment. The missing maximum-age check is established and remains a known control risk. A weekend-aged value is not, by age alone, an invalid NAV. The reviewed record does not supply an authoritative validity invariant or independently verify compensating procedures. A numerical or Informational severity would therefore imply unsupported precision. Neither prior disclosure nor absence of a historical loss establishes low

risk. The general website terms expressly exclude OUSG transaction economics and cannot substantiate a right to reprice, cancel, equalize or recover completed dealings. [E02; S06-S08]

Recommendation. Ondo, as issuer and system operator, should define an authoritative NAV-validity policy, including weekend and holiday dealing, and enforce it before subscription or redemption. The operator should pause the affected direction when that policy expires, alert operations before expiry, and publish the treatment of pending and completed instructions. The fund administrator and transfer agent should align signed NAV approval, repricing, equalization and recovery procedures with the on-chain control and test the combined process under delayed-update scenarios.

## 6.2 OUSG-CO-01 — Privileged control is material to safety and recovery

Status and affected components. Control observation affecting EVM upgrade, manager, oracle, mint/burn, pause, identity and compliance roles; Solana mint/freeze authority; and XRP Ledger issuer and recipient accounts. The retained Ethereum review identified multiple Safe-controlled roles, while Solana used a 4-of-7 Squads vault. The XRP Ledger issuer retained an active master key with no signer list. These are not ordinary-user vulnerabilities, but key compromise or governance failure can alter supply, eligibility, pricing or recovery assumptions. [E01; E03]

Recommendation. Ondo should maintain documented role ownership, hardware-backed key custody, independent change approval, time-bounded emergency procedures and periodic access recertification across every network. For the XRP Ledger issuer, Ondo should document why the active master-key posture is necessary and evaluate a signer-list and master-key-disable design consistent with recovery requirements.

## 6.3 OUSG-CO-02 — Dormant deployments need explicit reactivation gates

Status and affected components. Control observation affecting Polygon and Solana. Polygon was paused with zero supply and no token minter or burner at its fixed block. Solana had zero supply but retained mint and freeze authority, and the legacy SPL Token design did not itself enforce a transfer hook or destination allowlist. Those states limited exposure on 28 September 2026 but do not establish permanent retirement. [E01; E03]

Recommendation. Before reactivating either deployment, Ondo should require a documented launch gate covering source and binary correspondence, current eligibility enforcement, role ownership, NAV source and freshness, supply reconciliation, incident pause procedures and public status-page updates. Dormant or retired deployments should be labelled consistently in issuer documentation.

## 6.4 OUSG-CO-03 — XRP Ledger processing depends on issuer operations

Status and affected components. Control observation affecting the OUSG issuer, OUSG recipient and RLUSD recipient on XRP Ledger. RequireAuth and Clawback provide native eligibility and recovery controls, while issuance and redemption are staged through operational accounts and off-chain processing. Destination-tag enforcement required a tag but did not publicly prove that the documented tag 1 was the only acceptable value. [E03]

Recommendation. Ondo should enforce the expected asset, issuer, destination account and destination tag in its processing service; reconcile every accepted payment to one authorized issuance or redemption record; quarantine duplicates and malformed instructions; and retain independently reviewable approvals and exception logs.

## 6.5 OUSG-CO-04 — Public evidence does not close cross-ledger conservation

Status and affected components. Control observation spanning all four networks and the private legal register. Public supply, burns, issuances and official addresses can be inspected, but the reviewed record did not provide a same-cutoff, independently signed reconciliation of aggregate ledger obligations to the authoritative limited-partner register and fund-administrator records. [E03; E06]

Recommendation. Ondo, the transfer agent and fund administrator should publish or provide to assurance reviewers a periodic same-cutoff reconciliation that identifies every ledger, explains pending migrations and settlement items, ties aggregate token obligations to the legal register, and is signed or otherwise independently attested.

## 7 RWA Linkage and Public Verifiability

OUSG has meaningful public legal-product and deployment anchors, but public verifiability remains incomplete. The SEC filing identifies Ondo I LP as a Delaware pooled investment fund offering under Rule 506(c) and section 3(c)(7); the issuer describes OUSG tokens as limited partnership interests and lists the relevant network identifiers. The product page displayed a portfolio snapshot expressly dated 30 September 2026 at 4:00 p.m. EDT. These sources support product identity and disclosure context, not a chain-level proof of title or reserves. [E06; S01; S02; S10]

| Linkage layer                 | Publicly established                                                                              | Not established by the reviewed public record                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Legal vehicle and offering    | Ondo I LP, Delaware limited partnership; Rule 506(c) and section 3(c)(7) filing context           | Complete governing partnership, subscription, dealing, repricing and recovery terms                               |
| Token identity                | Issuer-listed Ethereum, Polygon, Solana and XRP Ledger identifiers                                | That every token holder and amount matches the authoritative limited-partner or transfer-agent register           |
| NAV mechanism                 | Public product description, on-chain price interfaces and a dated product-page portfolio snapshot | Signed same-cutoff administrator NAV workpapers, source holdings, valuation adjustments and stale-event decisions |
| Underlying assets and custody | Issuer description of the product mandate and a dated public portfolio allocation                 | Independent contemporaneous custody statements and asset-by-asset ownership reconciliation                        |
| Multi-ledger obligations      | Fixed-point public supplies and representative migration or dealing histories                     | A complete same-cutoff conservation proof across all ledgers, pending items and the legal register                |
| Transaction finality          | On-chain execution and ledger finality for recorded public transactions                           | Economic finality against private rights to cancel, reprice, equalize, reject or recover a dealing instruction    |

### Verifiability conclusion

The public record identifies the legal vehicle, offering exemption, issuer statements, addresses, supplies and oracle interfaces. It does not independently reconcile legal ownership, custody, administrator-approved NAV or multi-ledger obligations. Those gaps prevent this report from asserting full backing, reserve sufficiency or realized economic loss from a stale-price event.

## 8 Limitations and Conclusion

### 8.1 Material limitations

| ID          | Limitation                                                                                                                                                                | Effect on conclusion                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| OUSG-LIM-01 | The latest ledger state in scope is the archived fixed observations dated 28 September 2026.                                                                              | Later deployment state, oracle age and configuration cannot be asserted.                                           |
| OUSG-LIM-02 | Private offering, subscription, redemption, repricing, equalization, cancellation and recovery terms were unavailable.                                                    | Economic finality and retained loss from a completed stale-price transaction cannot be established.                |
| OUSG-LIM-03 | Transfer-agent, limited-partner, fund-administrator, custody and signed NAV records were unavailable.                                                                     | Token balances cannot be fully reconciled to legal ownership, underlying assets or authoritative same-cutoff NAV.  |
| OUSG-LIM-04 | Organization-level key custody, approval evidence and incident records were unavailable.                                                                                  | The effectiveness of privileged-role governance and actual response to delayed pricing cannot be verified.         |
| OUSG-LIM-05 | No authenticated end-to-end live subscription, redemption or cross-ledger migration was performed.                                                                        | Private payment processing, exception handling and operational reconciliation remain outside assurance.            |
| OUSG-LIM-06 | The pinned published source was not established as byte-for-byte correspondence with the deployed implementation, and non-EVM source/build correspondence was incomplete. | Published source supports continuity of the stale-NAV behavior but not complete deployed-implementation assurance. |

### 8.2 Conclusion

OUSG-KR-01 remains an open known control risk: the reviewed price path does not enforce a maximum age. Its economic risk rating is unassigned because authoritative NAV-validity rules, operational effectiveness and exposure are not sufficiently established. No investor-loss vulnerability was substantiated, but that evidence limit and the historical disclosure do not support a low-risk or remediated conclusion. This opinion applies to the recorded code and state points, not subsequent changes. [E01; E02; S03-S08]

The archived observations also identify material trust dependencies in privileged control, dormant-network reactivation, XRP Ledger processing and cross-ledger reconciliation. Public evidence does not close the private administrator, transfer-agent, custody and dealing records needed to establish NAV approval, legal ownership, transaction finality and any loss or recovery outcome.

## A Code and Observation Identities

The following runtime hashes and implementation identities identify the archived EVM scope. E01 records the primary Ethereum snapshot at block 26,077,885 (28 September 2026, 18:56:23 UTC) and Polygon at 94,611,786 (19:13:39 UTC). E02 separately records the Ethereum price-path recheck at block 26,078,147 (19:48:59 UTC). These observations are not a single atomic snapshot; the report date does not refresh them.

| Component / state point    | Recorded code identity                                                              |
|----------------------------|-------------------------------------------------------------------------------------|
| Ethereum token proxy / E01 | Runtime hash:<br>0xa23b20d4f9e75f4bf9bd74d8c1b7f0219547289c67a11dea65370c1810fc1387 |

| Component / state point                         | Recorded code identity                                                                                                                      |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Ethereum token implementation / E01             | 0x1ceb44b6e515abf009e0ccb6ddafd723886cf3ff<br>Runtime hash:<br>0xe3966d923815cfd861c8d73e35fa571de9439704c40ec2341f867ede467fbbdf           |
| Ethereum identity-registry implementation / E01 | 0x136f28d64b658460abdd418da5c156be74d05213<br>Matched implementation source; the registry proxy and ProxyAdmin source record is incomplete. |
| Ethereum manager / E01 and E02                  | Runtime hash:<br>0xbf946cbe7a882ed8390036e441e88b393215881521fa9c807b9f85aea2580c63                                                         |
| Ethereum OndoOracle / E01 and E02               | Runtime hash:<br>0xda013e72461dba0ac333f85d9c1aa207c9d58f83227beeea2daa0551414c08be                                                         |
| Ethereum wrapper / E02                          | Runtime hash:<br>0xbd03c3dfb562a2b6baba5f6d7930257bc0fa52c1b5178d0e2e3462efdc3a5f7                                                          |
| Ethereum underlying oracle / E02                | Runtime hash:<br>0x7b767b4be271c82c754a9545e4e69de7d5f08930b5537747e23343375c88434e                                                         |
| Polygon token implementation / E01              | 0xf0001671af432f7bb3c3172608265e49722fdbbb<br>Runtime hash:<br>0xe3966d923815cfd861c8d73e35fa571de9439704c40ec2341f867ede467fbbdf           |

E01 records the Ethereum block hash as 0x3a36339a5d75e737c117fa49d5a0747ec1dc7b1d34f0cb438f62b5f0717b94ff. E02 records 0x4ee13e8b66cf9a29a80df6730fab6238c7be9eae84d1de00fe3c34ec25db8137. Both recorded USD 116.684446 with the 25 September 2026, 21:27:35 UTC price timestamp; the respective ages were 250,128 and 253,284 seconds. The latter recheck is not the source for the supply and other primary-state figures in section 4.1. Full network state identifiers accompany the scope attachment.

The retained deployed-source records identify Solidity 0.8.16+commit.07a7930e. The separately reviewed published repository commit 046c5c58a2d2202e70d7c2c4f13f414f15de47f4 uses Solidity 0.8.33 for the relevant files. Similar control flow across those versions does not establish byte-for-byte deployment correspondence. [E01; E02; S03-S05]

## 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 | OUSG Ethereum and Polygon deployment assessment            |
| E02 | OUSG stale-NAV technical and impact assessment             |
| E03 | OUSG Solana and XRP Ledger deployment assessment           |
| E04 | OUSG stale-NAV technical assessment workpaper              |
| E05 | Tokenized-treasury cross-asset assurance memorandum        |
| E06 | Tokenized-treasury RWA anchor and verifiability assessment |

### Primary public sources

**S01** | Ondo OUSG product page

Primary issuer product description reviewed 1 October 2026; the page's displayed portfolio snapshot was expressly dated 30 September 2026 at 4:00 p.m. EDT.

**S02 | Ondo official addresses**

Primary issuer deployment catalogue reviewed 1 October 2026; no publication date was displayed on the page.

**S03 | Ondo OUSGOracleWrapper published source**

Official public repository source reviewed at pinned commit 046c5c58a2d2202e70d7c2c4f13f414f15de47f4, dated 16 September 2026; published source, not deployed-bytecode correspondence.

**S04 | Ondo OndoOracle published source**

Official public repository source at the pinned reviewed commit; the TOKENIZED\_RWA path returns the source price and timestamp to its caller.

**S05 | Ondo BaseRWAManager published source**

Official public repository source at the pinned reviewed commit; minimumRwaPrice is a price floor rather than a maximum-age control.

**S06 | Code4rena Ondo Finance audit report**

Public audit covering 29 March-3 April 2024, published in April 2024; L-01 records the missing oracle-price staleness check.

**S07 | Code4rena Ondo Finance contest repository**

Historical contest repository for 29 March-3 April 2024; its publicly known issues disclose price/rebasing arbitrage risk and describe off-chain agreements, fees and limits as mitigations.

**S08 | Ondo terms of service**

Primary public terms last updated 2 February 2026 and reviewed 1 October 2026; they state that the website terms do not govern OUSG issuance, sale, purchase, redemption or transaction economics.

**S10 | Ondo I LP SEC Form D/A**

Primary SEC filing dated 20 January 2026 identifying Ondo I LP, the Rule 506(c) offering and section 3(c)(7) pooled-investment-fund context.

**S11 | Ondo announcement of instant OUSG subscriptions and redemptions**

Primary issuer article dated 27 March 2024 describing the increasing OUSG redemption price and 24/7/365 instant subscription and redemption design.

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

SHA-256: ddec7b08f77914853f034c58ec21d0038fdbba3197d7726f1e791916e1914733