

USYC

Multi-Network Public-Deployment Security Assessment

US Yield Coin
Evidence-bound review of the Ethereum, BNB Chain, Arc and Solana deployments

REPORT	B3-USYC-2026-001
ISSUED	1 October 2026
BASELINE	Technical evidence through 29 September 2026; public product/RWA evidence through 30 September 2026
AUTHOR	bench3.ai

B3-USYC-F01 is one confirmed deterministic Teller timestamp-conversion implementation defect. Its narrow DST-transition condition depends on a trusted-reporter timestamp, and supported realistic reachability and impact are insufficient for severity assignment. Two control observations and the stated evidence limitations remain.

Contents

1 Executive Summary 3

2 Scope and Assessment Basis 4

3 System and Threat Model 5

4 Technical Assessment 6

5 Recorded Validation and Coverage 9

6 Implementation Defect and Control Observations 10

7 RWA Linkage and Public Verifiability 12

8 Limitations and Conclusion 13

A Deployment and Authority Inventory 14

B Evidence and Source Index 14

Assessment of the official USYC deployment roster, identified token, Teller, oracle, permissions and cross-chain components, Solana production evidence and targeted control/economic assessments. Scope and exclusions are defined in Section 2.

1 Executive Summary

bench3.ai assessed the official USYC deployment surface on Ethereum, BNB Chain, Arc and Solana. The review covered proxy and runtime identity, initialization, role and capability configuration, mint/burn authority, Teller pricing and fee behavior, the Ethereum-BNB CCTP route, Solana Token-2022 extensions and control accounts, and the boundary between public token state and the private fund register and assets. [E01-E11]

Assessment conclusion

B3-USYC-F01 is a confirmed deterministic implementation defect: the Teller applies the current transaction's DST offset when converting a historical oracle timestamp. Its narrow DST-transition condition depends on a trusted-reporter timestamp, and all 520 reviewed rounds were weekday reports outside that condition. Supported realistic reachability and impact are insufficient for severity assignment. Six EVM control questions were otherwise resolved against fixed production state and source/configuration evidence, and three other targeted control and economic assessments did not establish an ordinary-actor path. The Solana production paths were corroborated, but the current Yieldcoin Manager binary lacks public exact source/build correspondence. [E02-E09]

Classification	Recorded result
Severity-assigned vulnerabilities	Critical 0 High 0 Medium 0 Low 0
Confirmed implementation defects	1; B3-USYC-F01, realistic reachability and impact insufficiently established for severity assignment
Control observations	2; Solana upgrade/management concentration and issuer-authorized balance-control powers
Material limitations	Solana source/build/IDL correspondence, private key governance, legal register, NAV/reserves and full cross-network reconciliation

Material residual risk

USYC is a permissioned asset. Configured issuers, minters, entitlement administrators and Solana program authorities can mint, burn, freeze, thaw, pause and change aspects of pricing or permissions. Those powers are part of the operating model, but compromise or misuse can have substantial effect. The recorded review did not establish an ordinary-caller authorization bypass; custody, quorum, rotation and monitoring of the controlling keys were not independently verified. [E02-E09; B3-USYC-O01-O02]

The Solana mint is active, and its nine enumerated token-account balances reconciled exactly to the recorded supply. Representative production subscription and redemption transactions moved USDC and minted/burned USYC as expected. The Yieldcoin Manager remains upgradeable by one direct on-curve key, and no issuer-published mainnet source, IDL or reproducible build matched the deployed binary. Public state therefore supports the specific observed routes, not an exhaustive source-code opinion over the Solana program. [E08-E09]

2 Scope and Assessment Basis

2.1 Official deployment baseline

Network	Primary identity	Recorded observation
Ethereum (1)	USYC 0x136471a34f6ef19fE571EFFC1CA711fdb8E49f2b Teller 0xeE35F963BFC71b51eC95147f26c030D674ea30e6	Block 26,077,212; 28 September 2026 16:41:11 UTC; hash 0x83cb93099505ad38e5782be4dad7674fa161ba61cb1087a4f8f89f4068db6a53.
BNB Chain (56)	USYC 0x8D0fA28f221eB5735BC71d3a0Da67EE5bC821311 CrossChainTeller 0xf38979E05650be7926EA07BB59C48Fb9b1DB3D08	Capability, initialization and CCTP observations at blocks 124,559,624; 124,559,805; and 124,561,256.
Arc (5042)	USYC 0x8a5D989Bbb96929F689B0200f435f53dA42bF490 Teller 0x51A8CE47dC08ba5CD19c7aa84EA6fD6664f60f9b	Block 23,228,513; 28 September 2026 16:42:43 UTC; hash 0xeac6d27733a2a6e42e1b027c65520e4f4191bd6a61c2c5607d63af8690928eea.
Solana mainnet-beta	Mint 7LWanZteUKtvFjv4MHYgKXXdAuCQYFPJysL9pxxdRQGn Yieldcoin Manager EMfvuBR8rre2f7sNqdDyPzQW7kgBUsVtxg7nX93YwAdm	Finalized snapshot slot 451,407,195; key deployment accounts rechecked at slot 451,408,537.

The current Circle deployment page retained by the workpapers had SHA-256 3e2228629d46d6e00f263a24fc58a74bb02680e9f0201150210736fc99bbfac5 and listed Ethereum, BNB Chain, Arc and Solana. The original local scope registry omitted Arc despite retaining the same source hash; the current official roster and fixed-block Arc observations therefore control this report's Arc scope. [E02-E03, E09, E11; S01]

2.2 Included components

Scope element	Extent of assessment
EVM tokens and permissions	USYC, Entitlements, Teller, oracle and CrossChainTeller components; EIP-1967 identities, runtime hashes, initialization, selected capability masks and minter configuration.
Cross-chain route	Ethereum domain 0 and BNB domain 17 CCTP V2 endpoints, redeemers, token pairs, finality, limits and allowances. Arc was confirmed absent from the advertised USYC CCTP route.
Pricing and fees	Teller current/next price behavior, permit ABI compatibility, FeeManager thresholds/rates and recorded split/order equivalence.
Solana	Token-2022 mint/extensions, Teller and fee state, ProgramData, permission records, supply/account reconciliation and representative subscription/redemption routes.
Business/RWA boundary	Public product, price and transfer-agent explanations and retained public financial evidence; not a private fund, legal-register or reserve audit.

2.3 Methods and exclusions

Methods comprised retained source/runtime analysis, EIP-1967 and Solana ProgramData resolution, fixed-block/finalized read-only calls, capability and event-history review, read-only selector probes, deterministic arithmetic checks, production transaction inspection and a Solana read-only completion review. No production transaction was signed or broadcast, and report preparation did not rerun the workpapers. [E02-E09]

Excluded are the private transfer-agent register, portfolio and custody records, NAV workpapers, all-chain supply reconciliation, key custody and organizational approvals, and private settlement operations. Canton and NEAR were not included because the retained official address page did not publish current identifiers for them. [E10-E11; S01]

3 System and Threat Model

USYC represents digital fund shares whose legal register is maintained by a transfer agent. Ethereum and Arc include Teller and oracle components for USDC subscription/redemption; BNB is a satellite representation connected to Ethereum through CCTP. Solana uses a custom Yieldcoin Manager and a Token-2022 mint, with permission accounts and privileged program-derived mint/freeze/burn powers. Public ledgers record token state but do not replace the private legal register, fund accounting or custody records. [E02-E10; S01-S05]

Actor / layer	Authority	Security boundary
Entitled investor	Subscribe, redeem and transfer within the configured permission model.	Cannot administer prices, roles, minter allowance or program upgrades through ordinary ownership.
Fund administrator / reporter	Publish current and next prices and administer operational state.	Price-input error or malicious reporting is a trusted-input risk unless an external actor can influence it.
EVM minters and CCTP	Mint/burn according to non-public capabilities, allowance and canonical CCTP authorization.	Current configuration and call graph determine whether a code primitive is externally reachable.
Solana Yieldcoin Manager and admin keys	Mint, freeze/thaw, permanent-delegate burn/transfer, price, pause, fee and permission administration.	Program-derived authorities cannot be ordinarily signed, but the program and direct keys remain trusted controls.
Transfer agent / fund / custodian	Maintain legal ownership, NAV, portfolio, liabilities and cash settlement.	Private records and controls are outside the public-deployment assessment.

3.1 Security objectives

The examined objectives were: initialized official deployments; role-consistent mint, burn and transfer permissions; correct cross-chain endpoint and peer binding; no replay or fee-tier bypass in the tested paths; supply/account reconciliation at recorded snapshots; and clear separation between authorized issuer powers, ordinary-user reachability and private financial/legal assurances.

4 Technical Assessment

4.1 EVM deployment and initialization

Network	Component proxies and implementations	Identity result
Ethereum	USYC 0x1364...9f2b -> 0xbf0f...4592 Teller 0xeE35...30e6 -> 0xb69e...ca72 Oracle 0x74f2...1f53 -> 0x6dea...1624 Entitlements 0x902D...808C -> 0xb59b...0c76	Fixed implementation hashes and initialized fields recorded; CrossChainTeller is direct at 0x5dbe...0c7d.
BNB Chain	USYC 0x8D0f...1311 -> 0x191f...45b Entitlements 0x6B7d...3692 -> 0x8cad...5acdb	Fixed implementation hashes and initialized fields recorded; CrossChainTeller is direct at 0xf389...3D08.
Arc	USYC 0x8a5D...F490 -> 0x7eb3...f948 Teller 0x51A8...f9b -> 0x7ff3...b1e6 Oracle 0x4BC8...537A -> 0x88bd...f65b Entitlements 0xb69e...ca72 -> 0x6b76...324	Fixed proxy slots, runtime hashes and initialized configuration recorded; Arc source matching remained incomplete.

Read-only second-initialization calls from an unrelated address reverted for Ethereum Entitlements, Oracle, Teller and USYC; the corresponding four Arc proxies; and BNB Entitlements and USYC. Owners and component configuration were populated. No current official EVM proxy was found uninitialized or publicly takeover-reachable. [E02-E03]

4.2 EVM transfer, mint and burn authority

The BNB implementation contains a self-transferFrom branch that skips one sender capability check. At block 124,559,624, however, transfer and transferFrom were both non-public and both required the same role mask 0x808008, corresponding to roles 3, 15 and 23. No role could call transferFrom while lacking transfer permission, so the necessary production asymmetry was absent. [E02-E03]

On Ethereum and Arc, setMinterAllowance, incrementMinterAllowance and decrementMinterAllowance were non-public and assigned only role bit 20. The Ethereum history tied that role to a privileged administrator/minter account, and current nonzero allowances belonged to configured system actors including the Teller and CCTP TokenMinterV2. No ordinary actor could grant itself mint authority. [E02-E03]

The BNB satellite token's positive minter allowance also gates third-party burn. The deployed-control assessment confirmed the primitive but found no lower-trust production actor gaining additional authority: the direct operational EOA already had unlimited mint authority, while Circle TokenMinterV2 accepts burn only from TokenMessenger and burns its own balance through burn(uint256), not a selected holder through burn(address,uint256). This is a privileged-control property rather than a current ordinary-user path. [E07; B3-USYC-002]

4.3 CCTP V2 route

At the recorded blocks, Ethereum CrossChainTeller supported BNB domain 17 and bound its redeemer to the official BNB CrossChainTeller; BNB supported Ethereum domain 0 and bound the opposite peer. Both used canonical TokenMessengerV2 0x28b5a0e9C621a5BadaA536219b3a228C8168cf5d and MessageTransmitterV2 0x81D40F21F12A8F0E3252Bccb954D722d4c464B64, maxFee 0 and finality threshold 2000. Canonical token-pair lookups mapped each remote USYC to the opposite official local token, local burn limits were 75,000,000 USYC and required allowances were present. Arc domain 26 was not configured, consistent with the retained official matrix not advertising Arc USYC support. [E02-E03; S07-S08]

A separate hypothesis noted that the BNB implementation does not bind one outer CCTP recipient field. The exact BNB deployment has immutable teller() and usdc() values equal to zero, and redeemComplete necessarily reaches a typed teller.sellFor call to address(0), which reverts. The enclosing revert rolls back transferred USYC, nonce use, balances and logs. No redemption bypass or persistent state change was reachable in this configuration. [E05]

4.4 Teller pricing, permit and fees

Ethereum Teller uses the current reported price for redemption and, after the business cutoff, a forecast next price for subscription. The product and economic assessment found this asymmetry intentional and documented. Across all 520 paired recorded production rounds through the cutoff, nextPrice was strictly greater than currentPrice. A profitable synthetic downward forecast is mathematically possible but can be created only by the trusted reporting path; no ordinary investor-controlled or normal production instance was established. [E04]

B3-USYC-F01 is a deterministic implementation defect: the Teller applies the transaction-time DST offset when converting a historical oracle timestamp, so the branch can invert under a narrow timing condition around a daylight-saving transition. All 520 reviewed rounds were weekday reports outside that condition, and only the trusted reporter controls updatedAt. A permissioned investor can reach the affected pricing path after such a round exists but cannot choose the reporter timestamp. The available evidence does not establish realistic reachability or material impact sufficient for severity assignment. [E06; S03]

Ethereum and Arc USDC assets accepted the Teller's permit(address,address,uint256,uint256,bytes) selector; invalid empty-signature probes reached the overload and reverted with the expected signature-length error. The verified Ethereum FeeManager used one combined daily subscription/redemption volume and current 4/3 bps default rates with a 1,000,000 USDC free tier. Direct calls showed equal aggregate fees for one 2,000,000-unit operation and two 1,000,000-unit operations crossing the threshold. No split or reorder underpayment was established. [E02-E03]

4.5 Solana production completion

At finalized slot 451,407,195, the six-decimal Token-2022 mint had raw supply 118,972,506, or 118.972506 USYC. Nine enumerated token accounts reconciled exactly to this supply; two accounts held 9.882377 and 109.090129 USYC and the remaining seven were zero. All transfer-fee withheld amounts were zero. This is on-chain token reconciliation only, not a reserve or legal-register attestation. [E08-E09]

Solana control	Current identity / setting	Security significance
Mint/freeze/permanent delegate/mint close	Teller PDA DZ7j2YLDq7847t2HtCWaDQUTpLJ4BinPGsY8w9AAi63y	Program-derived authority; ordinary keys cannot sign directly, but authorized program paths can mint, freeze, burn or force-transfer.
Yieldcoin Manager	EMfvuBR8rre2f7sNqdDyPzQW7kgBUSVtxg7nX93YwAdm	Upgradeable custom program; current mainnet binary not publicly source/build verified.
Program upgrade	P3S7WBL3BviBuhW5HYtm8aicQQcivhJCs1Ewq9Xvb7B	Direct on-curve System account; no on-chain multisig or timelock was visible in the observed upgrade route.
Operational extension/price authority	EMMxaez3JFNMRFdKZgnC3KtZck6gmSS4n6AMHXUMvPZL	Direct key controlling price updates and transfer-fee, confidential-transfer and pause settings.

Solana control	Current identity / setting	Security significance
Transfer hook	Extension present; program ID null	No hook runs on current transfers; admission relies materially on default-frozen accounts and privileged thaw/permission lifecycle.

The Yieldcoin Manager ProgramData recorded deployment slot 422,537,133 and raw ELF payload SHA-256 1909b07d60243269dde2eb06ff5a7d60ef796d8eb26151f692330d510dad6438. Public build verification reported the program unverified and no issuer-published mainnet source, IDL, release commit or reproducible build was found. Circle's devnet IDL agreed with selected interfaces and account layouts but is not mainnet source correspondence. [E08-E09; B3-USYC-O01; L01]

A representative production subscription moved 1.200000 USDC to the treasury and minted 1.055021 USYC to the entitled signer. A subsequent redemption burned 1.055021 USYC and returned 1.199999 USDC; the one-base-unit difference was consistent with integer rounding. The same user permission record and expected Teller, fee-config, token programs and PDA accounts were used. These transactions corroborate the observed route but do not prove every instruction constraint of the unverified binary. [E08-E09]

The Solana treasury held approximately 425,066.494101 USDC while the indicated value of the recorded USYC supply was about 135.459796 USDC. The excess demonstrates that this is shared operational liquidity, not a one-token reserve vault. The balance is not evidence that all fund assets or liabilities are on chain or attributable only to Solana holders. [E08]

5 Recorded Validation and Coverage

ID / method	Recorded check	Outcome and limit
V01 read-only	Ten official EVM proxies: owners, initialized fields and repeated initializer calls	Initialized configuration and reverts recorded; no public initialization takeover established.
V02 read-only	BNB transfer and transferFrom capability masks	Both non-public and identical at 0x808008; source asymmetry not reachable through current role configuration.
V03 read-only/history	Ethereum/Arc minter configuration and Ethereum current minters	Configuration selectors assigned only privileged role bit 20; no ordinary self-grant path.
V04 read-only	CCTP domains, peers, endpoints, token pairs, finality, burn limits and allowances	Canonical Ethereum/BNB route internally consistent at recorded blocks.
V05 selector/fee probes	USDC bytes-permit and fee split/order behavior	Permit ABI compatible; splitting did not recreate free-tier capacity or reduce aggregate fees.
V06 pricing and economic assessment	Current/next-price asymmetry and historical rounds	Intentional trusted-input design; all 520 paired rounds had nextPrice above currentPrice.
V07 timestamp control assessment	Historical timestamp/DST conversion	Code defect confirmed, but trigger required a trusted-reporter Sunday hour absent from 520 rounds.
V08 cross-chain and minter control assessment	BNB outer-recipient and limited-minter burn conditions	Outer-recipient path reverts atomically at immutable zero Teller; minter-burn primitive had no lower-trust production route.
V09 Solana read-only	Mint, extension state, nine accounts, ProgramData and representative deposit/redeem	Supply reconciled and sampled route completed as expected; no exact mainnet source/build proof.

Negative calls and fixed-state observations establish only the sampled boundary. They do not prove all role combinations, future upgrades or private administrative paths safe. Historical absence of a trusted-input condition supports current reachability analysis but is not a formal invariant.

6 Implementation Defect and Control Observations

B3-USYC-F01 is a confirmed deterministic implementation defect. The evidence establishes the timestamp-conversion error, but does not establish realistic reachability of its trusted-reporter DST-transition condition or material impact sufficient for severity assignment. B3-USYC-O01 and B3-USYC-O02 remain separate control observations concerning privileged authority and deployment assurance. No issuer response or remediation evidence was recorded.

ID	Title	Classification / status
B3-USYC-F01	Historical oracle timestamps use the current transaction's DST offset	Confirmed implementation defect; realistic reachability and impact insufficiently established for severity assignment
B3-USYC-O01	Solana program replacement and operational administration rely on direct keys without exact deployed-build proof	Governance/source-assurance observation; applicable at snapshot
B3-USYC-O02	Issuer-authorized roles can freeze, force-transfer or burn holder balances	Privileged-control observation; disclosed operating dependency

F01 | Historical oracle timestamps use the current transaction's DST offset

Attribute	Record
Affected component	Ethereum Teller proxy 0xE35F963BFC71b51eC95147f26c030D674ea30e6; exact-matched implementation 0xb69ecb156dc0028198028c501340d5367845ca72
Classification	Confirmed implementation defect; reported separately from severity-assigned findings
Evidence	E06; retained Teller and oracle sources, fixed-block configuration and 520-round history; S03

Description. The Teller's historical timestamp conversion derives the Eastern-time DST offset from `block.timestamp` rather than from the oracle `updatedAt` value being converted. Around DST transitions, the same historical timestamp can therefore be assigned the current transaction's offset, deterministically changing the calendar-date comparison that selects `currentPrice` or `nextPrice`.

Impact and preconditions. Branch inversion requires the latest oracle round to satisfy a narrow timing condition around a daylight-saving transition. The trusted reporter, not an ordinary investor, controls `updatedAt`. All 520 reviewed rounds were weekday reports outside that condition. Once such a round exists, a permissioned investor can reach the affected pricing path, but the available evidence does not establish a realistic way for an ordinary actor to create the prerequisite or a supported material impact sufficient for severity assignment.

Recommendation. The Teller operator should derive the Eastern-time offset from the timestamp being converted, so historical `updatedAt` values use their own DST status rather than `block.timestamp`'s status. Regression tests should cover spring and autumn transition boundaries and historical/current timestamps with different offsets before deploying a corrected implementation.

Status. Confirmed implementation defect. Supported realistic reachability and material impact are insufficient for severity assignment; no issuer response or remediation evidence was recorded.

001 | Solana program replacement and operational administration rely on direct keys without exact deployed-build proof

Attribute	Record
Affected components	Yieldcoin Manager, ProgramData, price/extension administration and mainnet interface provenance
Classification	Governance and source-assurance observation; no ordinary-attacker severity assigned
Evidence	E08-E09

Description. Direct key P3S7...Xvb7B can replace the custom Solana program without an on-chain multisig or timelock visible in the observed upgrade transaction. Separate direct keys control price and Token-2022 extension settings. The current mainnet ELF is not tied to a public exact source tree, IDL or reproducible build. USYC also depends on the shared upgradeable Token-2022 program; E09 tied that executable to a verified official source commit, and its separate upgrade authority is a standard platform-governance dependency rather than an issuer-controlled defect.

Impact and preconditions. Compromise or misuse could redefine PDA-signed mint/burn/freeze behavior, permission checks, fees, prices and treasury use. No ordinary route to the keys was identified. Missing source/build correspondence prevents exhaustive assessment of every mainnet instruction and account constraint.

Recommendation. Circle and the program operator should publish the exact deployed source commit, mainnet IDL, locked Solana/Anchor toolchain and reproducible ELF hash. Upgrades and price/extension administration should use documented multi-party authorization, hardware-backed custody, rotation and independent monitoring.

Status. Applicable at the recorded Solana snapshot; no off-chain custody or build-attestation evidence recorded.

002 | Issuer-authorized roles can freeze, force-transfer or burn holder balances

Attribute	Record
Affected components	EVM minters/administrators; Solana Teller PDA, permanent delegate and default-frozen lifecycle
Classification	Privileged-control observation; no implementation-vulnerability severity assigned
Evidence	E02-E03, E07-E09

Description. Current EVM and Solana designs permit authorized fund actors to mint and burn; Solana additionally places freeze, thaw, permanent-delegate transfer/burn and mint-close powers behind the custom program. Newly created Solana accounts default frozen, while the transfer-hook program ID is currently null, so transfer admission depends materially on the privileged thaw/permission lifecycle.

Impact and preconditions. Authorized or compromised control-plane actors can immobilize or destroy balances and alter admission state. The review did not establish an ordinary caller bypass. These powers support regulated-asset administration but create custody, availability and governance dependencies for holders and integrators.

Recommendation. The issuer and transfer agent should document the legal and operational triggers, approval quorum, audit trail and reconciliation procedure for freeze, force-transfer and burn actions. Integrators should not treat USYC balances as censorship-resistant or irreversible and should monitor relevant role, allowance, program and extension changes.

Status. Applicable to the disclosed permissioned operating model; private governance controls not assessed.

Classification criteria

The numeric confirmed-vulnerability total includes only issues with assigned severity based on supported reachability and impact. A deterministic code defect may remain separately confirmed without severity when its production trigger or material impact is not established. Authorized issuer powers and ordinary privilege/trust dependencies remain separate control observations rather than implementation defects merely because they are consequential.

7 RWA Linkage and Public Verifiability

USYC is described as a digital representation of shares in the Hashnote International Short Duration Yield Fund. The transfer agent maintains the legal register, price derives from fund NAV divided by outstanding shares, and returns accrue through a rising token price rather than rebasing. Public token contracts, price interfaces and selected transactions expose part of this mechanism; they do not make the public chain the complete legal or asset record. [E10; S03-S06]

Assertion	Available public evidence	Assurance boundary
Product and deployment identity	Circle publishes the official Ethereum, BNB, Arc and Solana components. [S01]	Public attribution applies to the recorded roster and does not cover unlisted or future networks.
Legal-share linkage	Public explanations state that token activity is reflected in the transfer-agent register. [S04-S05]	The live register was not accessible for holder-by-holder or same-cutoff reconciliation.
On-chain quantity	EVM configuration and Solana supply/accounts were observed; Solana balances reconciled to supply. [E02-E03, E08-E09]	No complete same-time aggregate across every ledger and legal share record was obtained.
NAV and fund assets	Public pricing methodology and retained corporate financial disclosure provide product-level context. [S03, S06]	No real-time portfolio, prime-broker/custody balance or same-day signed fund reconciliation was obtained.

A Teller or treasury stablecoin balance is operational liquidity, not proof of the fund's complete assets or of one-to-one reserve coverage. Public evidence supports the product linkage mechanism but does not close, at one cutoff, all network supply, the legal register, assets, liabilities and completed cash settlement.

8 Limitations and Conclusion

ID	Limitation	Effect on conclusions
L01	No issuer-published mainnet source, IDL, release commit or reproducible build matched the Solana Yieldcoin Manager binary.	Observed interfaces and transactions support bounded route conclusions, not exhaustive source-level assurance over every instruction and account constraint.
L02	Key custody, organizational quorum, rotation, monitoring and incident procedures were unavailable.	Observed address and role restrictions do not establish that privileged controls are operationally secure.
L03	Private legal register, NAV workpapers, portfolio/custody records, cash settlement and all-network reconciliation were outside scope.	No legal-share, reserve, valuation, solvency or completed-payment assurance is provided.
L04	Historical and behavioral validation was targeted.	The workpapers do not prove all state transitions, trusted-input failures, future upgrades or private administrative paths safe.
L05	Arc source correspondence was incomplete relative to Ethereum, despite fixed runtime/state observations.	Arc conclusions rely more heavily on deployed identity, state and behavior than on a complete public source build.

Conclusion

B3-USYC-F01 remains a confirmed implementation defect: historical oracle timestamps use the current transaction's DST offset. Its narrow daylight-saving-transition condition depends on a trusted-reporter timestamp, all 520 reviewed rounds were weekday reports outside that condition, and an ordinary investor cannot choose updatedAt. Supported realistic reachability and material impact are insufficient for severity assignment. Separately, the recorded EVM controls, CCTP bindings, other pricing/fee analysis and observed Solana routes did not establish an ordinary-attacker issue. The two privileged-control observations and incomplete Solana source/build correspondence remain material qualifications. No issuer response or remediation evidence was recorded.

The conclusions apply only to the listed deployments and observation points. Changes to implementations, permissions, minter allowances, CCTP endpoints, Teller price/fee behavior, Solana programs, extension authorities or the official network roster require 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 Authority Inventory

Network	Component	Address / identifier
Ethereum	USYC / Teller / Oracle / Entitlements	0x136471a34f6ef19fE571EFFC1CA711fdb8E49f2b 0xeE35F963BFC71b51eC95147f26c030D674ea30e6 0x74f2199AEb743f68f05943e5715A33EaF2b61f53 0x902D906b8d988092213bE799B18Bd2cbd64F808C
Ethereum	CrossChainTeller / FeeManager	0x5dbeCcECEbCdC2ce3258f6E638373d2923560c7d 0x41ECF227A4cE2564e8fD1a01082cB56Bb8E1344F
BNB Chain	USYC / Entitlements / CrossChainTeller	0x8D0fA28f221eB5735BC71d3a0Da67EE5bC821311 0x6B7d54003f73bE979cf92BF369432aC534853692 0xf38979E05650be7926EA07BB59C48Fb9b1DB3D08
Arc	USYC / Teller / Oracle / Entitlements	0x8a5D989Bbb96929F689B0200f435f3dA42bF490 0x51A8CE47dC08ba5CD19c7aa84EA6fD6664f60f9b 0x4BC8d5aCD3d040d2903dD9C5B7048520c6ff537A 0xb69ecb156Dc0028198028c501340d5367845ca72
CCTP	TokenMessengerV2 / MessageTransmitterV2 / TokenMinterV2	0x28b5a0e9C621a5BadaA536219b3a228C8168cf5d 0x81D40F21F12A8F0E3252Bccb954D722d4c464B64 0xfd78EE919681417d192449715b2594ab58f5D002
Solana	USYC mint / Yieldcoin Manager / ProgramData	7LWanZteUKtvFjv4MHYgKXXdAuCQYFPJysL9pxxdRQGn EMfvuBR8rre2f7sNqdDyPzQW7kgBUsvtxg7nX93YwAdm DwbKhT65kW49dw6e3cjz1qwhkm2akDehGsraLBau7s7M
Solana	Teller PDA / fee-config PDA / upgrade authority	DZ7j2YLDq7847t2HtCWaDQUtPlJ4BinPGsY8w9Aai63y 8575TtzfD7gkiM62TQcA5zRQ3TJpPMYzKrQ1EW3a3Aqf P3S7WBL3BviBuhW5HYtm8aicQQcivhJCs1Ewq9Xvb7B

The inventory records official and recursively resolved public components. It does not imply equal review depth, exact public source correspondence for every implementation, or assurance over private fund systems. [E02-E03, E08-E11]

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	USYC EVM deployment and control assessment
E03	USYC EVM source, configuration and validation assessment
E04	USYC current/forecast price economic assessment
E05	USYC CCTP recipient-binding assessment
E06	USYC historical-timestamp and DST assessment
E07	USYC minter and third-party-burn authority assessment

ID	Assessment record
E08	USYC Solana production deployment assessment
E09	Independent Solana production deployment review
E10	Tokenized Treasury RWA anchor and public-verifiability assessment
E11	Original Tokenized Treasury asset scope registry

Primary public sources

- S01** | Circle USYC smart-contract addresses
Official Ethereum, BNB Chain, Arc and Solana deployment roster observed 29 September 2026.
- S02** | Circle USYC Solana subscribe and redeem quickstart
Official public Solana account and transaction model; interface aid, not exact mainnet source/build proof.
- S03** | Circle - Understand USYC pricing
Business-day reporting and the current/forecast price model informed the pricing assessment.
- S04** | Circle - USYC subscription, redemption and functionality
Permissioned investor, transfer-agent register and operational-halt description.
- S05** | Circle USYC product page
Product and fund-share context used in the RWA linkage assessment.
- S06** | Circle 2025 Form 10-K
Public financial context retained in the RWA assessment; not a real-time USYC reserve reconciliation.
- S07** | Circle CCTP supported chains and domains
Official domain and supported-asset matrix used for Ethereum/BNB/Arc route interpretation.
- S08** | Circle CCTP V2 contract addresses
Canonical TokenMessengerV2 and MessageTransmitterV2 identities used in fixed-block checks.
- S09** | OtterSec Solana verified-build status - Yieldcoin Manager
Public status reported unverified during the 2026-09-29 Solana completion review.

Scope attachment

usyc-scope-manifest-en.json
SHA-256: 245e3e429712a5a4cd92d2be20bf3ede30d7c5a57a1a8094bc5bc8213561f9de