

MONY

Public Smart Contract Security Assessment

My OnChain Net Yield Fund

Bytecode-bound review of the Ethereum Diamond deployment

REPORT	B3-MONY-2026-001
ISSUED	1 October 2026
BASELINE	Ethereum block 26,077,991
AUTHOR	bench3.ai

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 7

6 Findings and Control Observations 8

7 RWA Linkage and Public Verifiability 10

8 Limitations and Conclusion 11

A MONY Deployment and Authority Inventory 12

B Evidence and Source Index 13

Assessment of the official MONY Ethereum entrypoint, its current EIP-2535 facet graph, authority accounts and public execution evidence. Scope, methods and exclusions are defined in Section 2.

1 Executive Summary

bench3.ai assessed the official Ethereum smart-contract deployment of MONY, the My OnChain Net Yield Fund. J.P. Morgan Asset Management identifies entrypoint 0x6a7c6aa2b8b8a6A891dE552bDEFFa87c3F53bD46. The assessment covered the EIP-2535 Diamond dispatcher, all 16 current facets and 68 selectors, initialization and upgrade history, ownership and roles, account restrictions, issuance and burn workflows, on-chain supply, administrative smart accounts and the boundary between token state and private fund operations. [E01-E07; S01-S05]

At Ethereum block 26,077,991, the MONY entrypoint had a 6,958-byte runtime with Keccak-256 0xf2dea1946270fa0b2005d60f1f55ab8a2be4ce89a8124c1559b530c2c33bf24f. The same 16-facet/68-selector address set was recorded at blocks 26,070,626, 26,077,242 and 26,077,991; every current facet had Sourcify exact creation/runtime correspondence, and no later DiamondCut or relevant role/ownership transition was recorded through the assessment block. [E01-E04]

Assessment conclusion

No reportable implementation vulnerability was confirmed in the examined MONY public-contract paths. Three material control observations are reported: immediate owner-directed upgrades, single-controller administrative accounts, and the legal/settlement boundary outside public token state. These observations are not included in vulnerability severity totals.

Classification	Recorded result
Confirmed vulnerabilities	Critical 0 High 0 Medium 0 Low 0
Control observations	3; privileged control, account concentration and off-chain settlement boundary
Unconfirmed candidates	0
Assessment boundary	Official public Ethereum contract system; private fund operations excluded

Material residual risk

The Diamond owner can replace MONY's executable surface through diamondCut without the installed 3,600-second governance delay applying to that action. The owner/TOKEN_ADMIN, ACCOUNT_ADMIN and TOKENIZATION_AGENT positions are held by separate Alchemy LightAccount proxies, each with one direct controller. These are significant custody and operational dependencies. Exact wrappers and read-only negative calls did not reveal an unrelated-caller route to exercise them. [E01-E04; B3-MONY-O01-O02]

Public chain state establishes token balances, supply and contract execution, not the private-placement register, investor rights, NAV, portfolio assets or final payment. MONY's private offering materials and authoritative operating records were not public. On-chain supply conservation therefore does not establish reserve sufficiency, legal ownership or completed subscription/redemption settlement. [E01; E05; B3-MONY-O03]

2 Scope and Assessment Basis

2.1 Deployment baseline

Parameter	Assessed MONY deployment
Network	Ethereum mainnet; chain ID 1
Official token endpoint	0x6a7c6aa2b8b8a6A891dE552bDEFFa87c3F53bD46
Final observation	Block 26,077,991 hash 0xaa2ca8bfb645bf784caa02ffa6b3b981c24fd987791732f66c1da7e94ef595b6 2026-09-28 19:17:35 UTC
Execution model	EIP-2535 Diamond; 16 current facets; 68 current selectors
Source correspondence	Exact creation/runtime matches for endpoint, all current facets and deployed MONY initializer; endpoint compiled with Solidity 0.8.17 and current facets with Solidity 0.8.26.
Recorded token state	decimals=4; total supply 102,812,542.6700 MONY; paused=false; tokenActive=true; delay=3,600 seconds

The deployment is not a conventional ERC-1967 token proxy. Its live implementation is the selector-to-facet graph enumerated by the Diamond loupe. MONY's deployed initializer is exact-matched DiamondInitTimelockable at 0xC6B9e851a599e0Da88b39f0E8Bc2B0683A503e81; constructor/init data established MONY's role-admin graph, four-decimal metadata, allowlist mode, 60-minute delay and active/unpaused state. [E01-E04; S06]

2.2 Assessment type and methods

Method	Applied scope
Diamond materialization	Fixed-block loupe enumeration of all facets/selectors and bytecode-bound source correspondence for current executables.
Static control-flow review	Upgrade, ownership, roles, timelock, account restrictions, transfer, mint and burn workflows using exact-matched deployed source.
Read-only fixed-state review	Owner/pending owner, roles, list mode, pause/active state, supply, balances, locked balances, controller accounts and implementation slots.
Historical event review	Complete public DiamondCut history through the anchor and incremental role, ownership and administrative-account event checks.
Negative-call evidence	Archived unrelated-caller eth_call checks for upgrade, ownership, role-gated mutations and administrative smart-account execution.
Public product and RWA review	Issuer, platform and public-fund evidence available through 30 September 2026.

Method boundary: all production interactions supporting this assessment were read-only and are bound to the observation blocks and transaction records identified above. No state-changing production transaction or private-system test forms part of the evidence basis. [E01-E04]

2.3 Included and excluded boundaries

Included: the official MONY entrypoint; 16 current facets; deployed MONY initializer; DiamondCut history; current owner, roles and LightAccount dependencies; token restriction, transfer, mint and burn paths; and public token balances/supply. Excluded: private placement memorandum; investor register; identity/KDA services; Morgan Money order acceptance; transfer-agent processing; NAV and dividend calculations; portfolio and custody records; cash/stablecoin settlement; HSM/MPC or organizational controls; legal advice; financial audit; and reserve or solvency attestation.

The publication date is 1 October 2026. Technical applicability is bound to block 26,077,991 and the recorded executable identities. Public RWA synthesis has an evidence cutoff of 30 September 2026.

3 System and Threat Model

MONY is a permissioned EIP-2535 token. The dispatcher maps calls into facets that share Diamond storage for balances, supply, allowances, roles, account activation, stop codes, locked balances, burn requests, pause state, token-active state, metadata, timelock and ownership. The on-chain system represents token lifecycle and pending-burn operations; fund accounting and settlement remain external. [E01-E04]

Principal	Current holder / authority boundary
Diamond owner and TOKEN_ADMIN	0x5aE5d4AdA523985DbA22CF046599979897C8418; single-controller LightAccount; can upgrade logic, administer roles and control global token state.
ACCOUNT_ADMIN	0x20aab6c346ac47f6b7f8c5d76f1f85d7367197d8; single-controller LightAccount; manages account activity, stop codes, locks and forced movement/burn.
TOKENIZATION_AGENT	0x9f5252058521e7458195a0350a0dc361c225857a; single-controller LightAccount; mints, burns and administers pending-burn requests.
BURNER	0xfb448891b3c1628b0e6b7b0c92b9e0013e28b5a9; zero-code direct address serving as the redemption sink.
Ordinary token account	Must be active; transfer paths enforce global active/unpaused state, sender/recipient and allowance-spender activity, allowance/balance and applicable stop codes.
Private fund operators	Control identity, order acceptance, register, NAV and settlement systems that are not represented completely by public token state.

Assessed security properties

The review considered unauthorized Diamond upgrades or ownership takeover, role acquisition, account-eligibility mutation, pause/state changes, mint/burn, forced movement, delegated-transfer restriction bypass, pending-burn processing and on-chain supply conservation. An ordinary attacker was modeled as an address without the owner or administrative roles and without control of the LightAccount controllers.

Authorized administrators retain broad powers appropriate to a regulated token, including upgrades, issuance/destruction, restrictions and corrections. The security opinion therefore depends on the separation between authorized control and ordinary callers; private custody and organizational approval controls were not assessed. [B3-MONY-O01-O02]

4 Technical Assessment

4.1 Current Diamond execution surface

The fixed-block loupe enumerated 16 facet addresses and 68 selectors. The graph covers loupe and interface support, upgrade, ownership, timelock, roles, pause, global token state, metadata, account administration, stop codes, ERC-20 behavior, mint, direct burn, burn preparation and pending-burn response. No live selector pointed to unidentified code, and each current facet had an exact creation/runtime source match. [E01-E04; Appendix A]

The MONY entrypoint itself was compiled with Solidity 0.8.17+commit.8df45f5f. The current shared facet set was compiled with Solidity 0.8.26+commit.8a97fa7a. MONY's initializer, address, supply, initialization data and five-cut history were assessed separately and are not inferred from another product using the same facets. [E01-E04]

4.2 Upgrade and ownership controls

diamondCut selector 0x1f931c1c routes to DiamondCutFacet 0x6e4D1A8b0A6b2ED26c50873C2c75FeAC77385295. Exact source executes LibDiamond.enforceIsContractOwner before any facet change or initializer delegatecall. The five ERC-173 selectors route to ERC173FacetTimelockable 0x7d7D5C1C2C9D45f6C73db9cCF6236ceb84d71965; transfer and renunciation use the live timelock path, and acceptance requires the pending owner. [E03-E04; S07-S08]

At the assessment state, owner was 0x5aE5d4AdA523985DbAB22CF046599979897C8418 and pending owner was zero. Archived unrelated-caller calls reverted diamondCut with DMND0001, ownership transfer with FACT1004 and ownership acceptance with DMND0018. The owner LightAccount rejected unrelated execute and upgradeToAndCall calls with NotAuthorized(address). These samples corroborate the exact source guards; they do not assess controller-key custody. [E01-E04]

The installed 3,600-second delay applies to designated actions such as role grants and ownership transfer/renunciation. It does not wrap diamondCut. Once the owner LightAccount authorizes the call, MONY execution logic can be replaced without that delay. [B3-MONY-O01]

4.3 Roles, restrictions and token lifecycle

At blocks 26,070,626 and 26,077,242, role history showed four surviving grants and no revokes: TOKEN_ADMIN, ACCOUNT_ADMIN, TOKENIZATION_AGENT and BURNER. Incremental checks through block 26,077,991 found no relevant role change. TOKEN_ADMIN administers itself and the other roles. The first three role holders are 61-byte Alchemy LightAccount proxies using exact-matched LightAccount v2.0.0 implementation 0x8E8e658E22B12ada97B402fF0b044D6A325013C7. [E01-E04; S09]

Ordinary transfer and transferFrom require active and unpaused global state, active sender and recipient, an active allowance spender, sufficient allowance/balance and applicable stop-code checks. Transfers to BURNER enter the pending-burn workflow; TOKENIZATION_AGENT can approve or reject pending burns and can execute role-gated direct mint/burn/prepare-burn paths. ACCOUNT_ADMIN controls account activity, stop codes, locks and forced movement. Archived unrelated-caller calls reverted at the corresponding role boundaries. [E01-E04]

4.4 MONY deployment and upgrade history

MONY was deployed at block 23,890,166 in transaction 0x3a29c30a1854eaf26d464d072a9121dfd0587afe8dead2d8e5735510d3f2e838. Five DiamondCut events account for its public upgrade history through the assessment: deployment at block 23,890,166; timelock addition at 23,898,087; major current-facet cut at 24,441,490; access-control replacement at 24,442,114; and burn-preparable update at 24,756,010. No later DiamondCut was recorded through block 26,077,991. [E01-E04]

4.5 Supply and accounting boundary

At block 26,077,991, two nonzero MONY balances summed exactly to raw total supply 1,028,125,426,700, equivalent to 102,812,542.6700 MONY at four decimals. lockBalanceOf returned zero for both nonzero holders. This supports current on-chain conservation and absence of hidden locked units outside the public balance sum at that snapshot. [E01]

$1,028,125,426,700 \text{ raw units} / 10^4 = 102,812,542.6700 \text{ MONY}$

The chain does not expose MONY's authoritative private-placement register, NAV, portfolio, custody assets, cash/stablecoin settlement or final investor entitlements. On-chain conservation is therefore not a fund-level accounting or reserve proof. [E05; B3-MONY-O03]

5 Recorded Validation and Coverage

Validation relevant to the opinion is summarized below.

Recorded check	Result and evidentiary meaning
Diamond loupe enumeration	16 facets and 68 selectors at blocks 26,070,626 and 26,077,242; address-selector set unchanged at the later public refresh.
Exact source correspondence	Entrypoint, MONY initializer, all current facets and LightAccount implementation had exact creation/runtime verification records.
Upgrade history	Five DiamondCut events account for MONY's history; no later cut through block 26,077,991.
Owner and role state	Owner, zero pending owner, four surviving roles, account implementations and direct controllers were recorded at fixed state.
Unauthorized mutation calls	Unrelated calls to upgrade, ownership, mint/burn, stop-code, force-transfer, pause and queue paths reverted at recorded guards.
Administrative wallet calls	Unrelated owner-wallet execute and upgrade calls reverted NotAuthorized(address).
Balance/supply reconciliation	Two nonzero balances summed to total supply and both recorded locked balances were zero at block 26,077,991.
Representative issuance	A recorded shared privileged route minted MONY to an active holder; evidence of authorized operation, not an ordinary-user mint path.

Recorded negative calls corroborate individual guards; they are not exhaustive. Private custody, approval, settlement and incident-response controls were outside scope. [E01-E04]

6 Findings and Control Observations

No implementation vulnerability was confirmed. The observations below concern privileged controls and the off-chain product boundary; they are not included in vulnerability severity totals. No issuer response or remediation verification was available.

ID	Title	Classification / status
B3-MONY-O01	Owner-directed Diamond upgrades are not subject to the governance delay	Privileged-control observation; applicable at snapshot
B3-MONY-O02	Principal administrative roles depend on single-controller smart accounts	Operational concentration observation; applicable at snapshot
B3-MONY-O03	Public token state does not establish legal ownership, NAV or settlement	Integration / record-of-ownership observation

001 | Owner-directed Diamond upgrades are not subject to the governance delay

Attribute	Record
Affected components	DiamondCutFacet.diamondCut; owner LightAccount; TimelockableFacet
Classification	Privileged-control observation. No implementation-vulnerability severity assigned.
Evidence	E01-E04; S07; Appendix A

Description. The installed diamondCut wrapper enforces the current Diamond owner, but the 3,600-second governance delay used for designated role and ownership actions does not apply to facet changes. Once authorized by the owner LightAccount, an upgrade and optional initializer delegatecall can execute without that delay.

Impact and preconditions. Compromise or misuse of owner authority could replace token logic affecting restrictions, supply and accounting in one authorized transaction. The risk requires owner authorization or controller compromise; no unrelated-caller bypass was established. Private approvals and custody controls were not assessed.

Recommendation. The issuer and contract operator should require verifiable multi-party upgrade approval and a documented delay for routine upgrades where operationally compatible, with narrowly defined emergency procedures. Each approved release should identify exact facet addresses, selector changes, source/build identities and effective transaction. Monitoring should cover DiamondCut and owner-account implementation/controller changes.

Status. Applicable at the assessment snapshot; mitigation not verified.

002 | Principal administrative roles depend on single-controller smart accounts

Attribute	Record
Affected components	Owner/TOKEN_ADMIN, ACCOUNT_ADMIN and TOKENIZATION_AGENT LightAccounts
Classification	Operational concentration observation. No implementation-vulnerability severity assigned.
Evidence	E01-E04; S09; Appendix A

Description. MONY's three principal administrative roles are held by separate LightAccount v2.0.0 proxies, each exposing one direct controller. The same role-holder accounts also appeared in the recorded JLTXX control graph, creating a cross-product dependency; this report's technical conclusions and inventory remain specific to MONY.

Impact and preconditions. A controller compromise or erroneous authorized action can affect upgrades/roles, account eligibility and forced movement, or issuance/burn processing, depending on the affected role. Reuse across funds can increase operational blast radius. HSM/MPC custody, enterprise approvals, organizational separation, transaction policies and recovery were not assessed.

Recommendation. The issuer and fund operator should document controller custody, approval thresholds, role separation, rotation, monitoring and emergency revocation. Product-specific control accounts or enforceable transaction policies should be considered where they materially reduce cross-product impact. Recovery and reconciliation exercises should include controller compromise and shared-account incidents.

Status. Single-controller architecture and cross-product account reuse observed; compensating controls not assessed.

003 | Public token state does not establish legal ownership, NAV or settlement

Attribute	Record
Affected components	Token balances and supply; private placement records; NAV, order, register and settlement systems
Classification	Integration and record-of-ownership observation. No implementation-vulnerability severity assigned.
Evidence	E01; E05; S01-S03

Description. Public evidence identifies MONY as a Rule 506(c) private-placement fund and the assessed address as its Ethereum token. Public chain state exposes balances, supply, mint/burn and restriction controls. It does not expose the private placement memorandum, precise share-class rights, authoritative investor register, NAV calculation, portfolio/custody records or final cash/stablecoin settlement.

Impact and preconditions. Users and integrators who treat a token balance or burn as sufficient evidence of legal ownership, valuation, reserve sufficiency or completed payment may rely on a state transition that is only one part of the fund workflow. This is a product/integration boundary, not evidence that the contract mis-accounted supply.

Recommendation. The issuer, fund operator and transfer/settlement operators should provide authoritative documentation for token-to-share rights, register priority, NAV and dealing cutoffs, subscription/redemption finality, exception handling and reconciliation. Integrators should not represent public token supply as fund

assets or final legal ownership without the corresponding authoritative records.

Status. Applicable to the public/private operating boundary; no private evidence or remediation response was available.

Upgrade and ownership guard validation

All 68 live selectors route to 16 identified, exact-matched facets. The installed diamondCut wrapper enforces the Diamond owner, the ownership wrapper enforces timelock and owner/pending-owner conditions, and the owner LightAccount rejects unrelated execution. These validation results apply to the reviewed MONY graph and do not establish safety after a later cut, owner change or controller upgrade. [E03-E04]

7 RWA Linkage and Public Verifiability

J.P. Morgan's official launch materials identify MONY as an Ethereum tokenized money-market/private-placement fund investing at a high level in U.S. Treasury securities and fully collateralized repurchase agreements, with returns reinvested daily. The official token address, public supply and contract control plane are verifiable. The private placement memorandum, precise share-class rights, NAV formula, transfer agent, custodian, financial statements, independent audit and legal register were not public in the reviewed evidence. [E05; S01-S04]

Layer	Publicly supported statement	Unresolved boundary
Legal product	Official launch material identifies MONY, Ethereum and the exact token address.	The PPM, precise token/share rights and authoritative investor register are not public.
Pricing and returns	Official materials describe daily reinvestment and the high-level investment strategy.	NAV formula, dealing cutoff, published NAV history and investor-level allocation were not established.
Fund assets	The stated strategy is U.S. Treasuries and fully collateralized repo.	Portfolio, liabilities, custodian records, financial statements and independent audit were not available.
On-chain units	Official address, supply, balances, mint/burn and administrative restrictions are public.	Token supply cannot be closed to legal shares or underlying assets from public evidence alone.

Public evidence does not connect token units to fund assets through authoritative legal, valuation, custody and register records. Those private records were unavailable; their absence from this assessment is not evidence that MONY is unbacked. [E05]

8 Limitations and Conclusion

ID	Limitation	Effect on conclusions
B3-MONY-L01	No issuer-maintained public repository, signed release manifest or reproducible-build workflow was available.	Sourcify binds current deployed bytecode to source/metadata, but development history and issuer-approved release provenance were not assessed.
B3-MONY-L02	Private placement, register, identity, NAV, portfolio, custody, order and settlement systems were outside scope.	The opinion does not cover legal ownership, valuation, reserves, solvency, order finality or payment completion.
B3-MONY-L03	Controller custody, approval thresholds, organizational separation and incident controls were not public.	The observed single-controller architecture cannot be qualified by unverified compensating operational controls.
B3-MONY-L04	The assessment is a fixed-state public-contract review.	Any later DiamondCut, owner/role change, LightAccount upgrade or policy-relevant configuration change may invalidate the conclusions.

Conclusion

Within the official MONY Ethereum deployment, exact executable identities and recorded state, no reportable implementation vulnerability was confirmed in the examined upgrade, ownership, role, restriction, mint, burn and accounting paths. Immediate owner-directed upgrades, single-controller administrative accounts and the public/private record boundary remain material trust and integration risks.

This conclusion is limited to the public Ethereum contract system at block 26,077,991. It is not a complete fund-operating-system audit, legal opinion, financial audit, reserve attestation or assurance that unknown defects do not exist. Applicability must be reassessed after changes to facets, selectors, owner, roles, administrative-account implementations or relevant operating policy.

A MONY Deployment and Authority Inventory

The facet inventory below is the MONY loupe result at the assessment state. All current facets had nonempty runtime and exact creation/runtime source correspondence. [E01-E04]

Facet	Ethereum address	Selectors
DiamondLoupeFacet	0x4D9832828a3898c9fCaF8799CAcdcf709068bA24	4
AccessControlFacetTimelockable	0xe79A30d2a2134fcccCBbfB9A79F39E6AB1637B3f	5
DiamondCutFacet	0x6e4D1A8b0A6b2ED26c50873C2c75FeAC77385295	1
ERC173FacetTimelockable	0x7d7D5C1C2C9D45f6C73db9cCF6236ceb84d71965	5
PausableFacetTimelockable	0xb1d84E1289942e45caa9C1103CBC867104F5f087	3
ManagedAccountFacet	0x71fF8c0E761B7640c1e294bF9b1b05b3a7df77A6	16
ERC165Facet	0x66f853ea787118985Be98a7f3a071b9FE1390231	5
ManagedTokenFacetTimelockable	0xeFbD67C1A8bc587599a475f720783282724e83B5	3
TokenMetadataFacet	0x5Be781F803552A0532FB03F6513D5a4bacb665a9	2
BurnableFacet	0x88183F91a0A7315BD3e2102BE7520c88cE9EFF67	1
ERC20FacetTransferBurnableStoppable	0x1aA6CF30f6b4F18F5cf12cC0F2c8543eaabE62D6	9
MintableFacet	0xe70C597957E542209eD44f2fbaE58370089E59be	1
TimelockableFacet	0xcA76E9791De59331219bBa4BE1d05404eda8764C	7
BurnResponsibleFacet	0x8c2FbC1DF5918CB15b96aD4d57298988c73dac32	3
StopCodesFacet	0x996440281f77B4D664878B0B14a10E909Fc3310B	2
BurnPreparableFacet	0x981b3af7957841CE2c8869Ee25055a693a89006B	1

MONY administrative account inventory

MONY role	Role holder / direct controller
Owner / TOKEN_ADMIN	Holder 0x5aE5d4AdA523985DbAB22CF046599979897C8418 Controller 0xBB30949145942aa7a5BDCd358160a8D6cEd119Cc
ACCOUNT_ADMIN	Holder 0x20aab6c346ac47f6b7f8c5d76f1f85d7367197d8 Controller 0x09D3A27bc30cf916ccfaA80A878b3E46098b8147
TOKENIZATION_AGENT	Holder 0x9f5252058521e7458195a0350a0dc361c225857a Controller 0x40E06b1daAe4A4910a66617EE4197026019b6C6c
BURNER	Holder 0xfB448891b3c1628b0e6b7b0c92b9e0013e28b5a9 Controller Zero-code direct address at snapshot

MONY initializer: 0xC6B9e851a599e0Da88b39f0E8Bc2B0683A503e81

LightAccount implementation: 0x8E8e658E22B12ada97B402f0b044D6A325013C7

Administrative-proxy runtime Keccak-256: 0xaaa52c8cc8a0e3fd27ce756cc6b4e70c51423e9b597b11f32d3e49f8b1fc890d

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	MONY public Ethereum deployment evidence review
E02	MONY public Ethereum deployment evidence record
E03	MONY Diamond, authority and validation evidence record
E04	MONY technical assessment outcome
E05	Tokenized Treasury RWA anchor and public-verifiability assessment
E06	MONY deployment registry snapshot
E07	Tokenized Treasury final assurance and delivery opinion

Primary public sources

S01 | J.P. Morgan Asset Management MONY launch release

Issuer source identifying MONY, Ethereum and the exact official token address; reviewed through 29 September 2026.

S02 | Kinexys tokenized money market funds

Public description of tokenized-fund lifecycle and platform role retained in the assessment evidence.

S03 | Kinexys Digital Assets

Public platform description; generic multi-chain capability is not evidence of another live MONY deployment.

S04 | Official MONY Ethereum contract explorer record

Public explorer entry for the issuer-published MONY address.

S05 | Sourcify exact-match MONY entrypoint record

Bytecode-bound source record for the MONY FactTokenDiamond entrypoint.

S06 | Sourcify exact-match MONY initializer record

Bytecode-bound source and metadata for MONY's deployed DiamondInitTimelockable initializer.

S07 | Sourcify DiamondCutFacet record

Bytecode-bound source for the live MONY upgrade wrapper.

S08 | Sourcify ERC173FacetTimelockable record

Bytecode-bound source for the live MONY ownership wrapper.

S09 | Alchemy LightAccount v2.0.0 deployment reference

Publisher reference for the administrative-account implementation identified in the archived review.

Scope attachment

mony-scope-manifest-en.json

SHA-256: 1cf504fe1d381f24568f252e376625e1280397a9e0cb7d179ebc7ee46dde5588