

JLTXX

Smart Contract Security Audit

JPMorgan OnChain Liquidity-Token Money Market Fund
Public-evidence assessment of the Ethereum deployment

REPORT	B3-JLTXX-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 Security Model 5

4 Technical Assessment 6

5 Recorded Validation and Coverage 8

6 Findings 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 15

Assessment of the public Ethereum contract deployment at block 26,077,991. Scope, methods and exclusions are defined in Section 2.

1 Executive Summary

bench3.ai assessed the public Ethereum implementation of JLTXX, the Token Class of the JPMorgan OnChain Liquidity-Token Money Market Fund. The assessment addressed the deployed execution surface, administrative authorization, account restrictions, delegated transfers, issuance and redemption accounting, and the relationship between on-chain balances and the fund's disclosed operating model.

The implementation is an EIP-2535 Diamond comprising a 547-byte dispatcher and 16 active facets exposing 68 selectors, with exact-matched verified source. The assessment baseline is Ethereum block 26,077,991, timestamped 2026-09-28 19:17:35 UTC. [E01-E04]

Assessment conclusion

No reportable implementation vulnerability was confirmed in the examined authorization, restriction-enforcement and accounting paths. Three material control observations are reported. The conclusion applies to the identified public-contract deployment, subject to the scope and limitations below.

Classification	Recorded result
Confirmed vulnerabilities	Critical 0 High 0 Medium 0 Low 0
Control observations	3; reported separately from implementation vulnerabilities

Material residual risk

The one-hour governance delay does not apply to owner-only diamondCut, so the owner can replace token execution logic without that delay. Three single-controller LightAccounts hold the principal administrative roles, and the same accounts control MONY. These are significant trust and operational dependencies, although the recorded review did not identify an unauthorized route to exercise them. Off-chain custody and approval arrangements behind the controllers were not established. [E01; observations O01-O02]

The fund's Investor Register, rather than the public token ledger alone, determines legal ownership. Consequently, a successful token transfer, a token burn and completed off-chain settlement are not interchangeable assurances. The private register, reconciliation service and payment process were outside the assessed boundary. [S02-S03; observation O03]

2 Scope and Assessment Basis

2.1 Deployment baseline

Parameter	Assessed deployment
Production network	Ethereum mainnet; chain ID 1
Token entrypoint	0x09864f52B035AE22eE739dFa5c748fA080D07bD8
Final observation	Block 26,077,991 2026-09-28 19:17:35 UTC
Source correspondence	Sourcify exact creation/runtime matches recorded for the dispatcher and all 16 current facets; Solidity 0.8.26+commit.8a97fa7a.

Final block hash:

0xaa2ca8bfb645bf784caa02ffa6b3b981c24fd987791732f66c1da7e94ef595b6

Dispatcher runtime Keccak-256:

0x6b5dcb5c1b9c1b261d97547bfa8bd62130aed456788a9962595f94bdf50a405b

The assessment is bound to deployed addresses, selector routing, runtime hashes and verified compilation metadata. An issuer-maintained repository, signed release manifest and source-control commit were not available. [E01-E03]

2.2 Included components

Scope element	Extent of assessment
Dispatcher and active facets	Enumeration and code identity of all 16 facets / 68 selectors; targeted examination of the authorization, restriction and accounting paths described in Section 4.
Shared libraries and storage	Routing, role administration, timelock, token balances/supply/allowances, managed accounts, locked units, stop codes and burn-request state relevant to those paths.
Administrative accounts	Recorded proxy implementation and controller identity; relevant execution authorization boundary. Not a complete audit of LightAccount or ERC-4337 infrastructure.
Production state and history	Fixed-block configuration, role membership, ownership, balances, deployment/upgrade events and representative historical transaction routes.
Public product specification	Issuer address binding and the disclosed token-to-share/register relationship. Reviewed as business context, not as a legal or financial assurance engagement.

2.3 Methodology

The assessment is based on retained source-review records, verified-source correspondence, read-only Ethereum RPC/explorer observations, event-history analysis and targeted negative `eth_call` samples. Observations at blocks 26,077,208 and 26,077,991 record unchanged facet routing and relevant control configuration. No transaction was signed or broadcast. [E01-E04]

Validation was targeted and excluded a complete unit-test suite, stateful fuzzing, formal verification and end-to-end fund-operation testing. Facet and selector counts are not test coverage.

2.4 Exclusions

Excluded are the private Investor Register, investor identity/KYC decision systems, Kinexys Digital Assets (KDA) operating services, order acceptance, transfer-agent reconciliation, payment rails, NAV and dividend calculations, underlying portfolio and custody records, and organization-level key management. Ethereum consensus, general ERC-4337 infrastructure and the complete third-party wallet implementation were not independently audited as standalone products. The unavailable deployment initializer is addressed as limitation L01, not treated as a current executable facet.

3 System and Security Model

JLTXX is a permissioned fund token. Its Ethereum endpoint routes calls to facets by selector and executes those facets in the Diamond's storage context. Token policy is implemented in the routed facets and shared storage libraries. The recorded live surface contains no separate NAV oracle, external eligibility engine, investor-register contract or payment-settlement contract. Administrative smart accounts are execution dependencies rather than additional token-policy modules. [E01-E03]

Layer	State or authority	Boundary considered
Holder / delegate	Token balance, allowance and transaction request	Cannot acquire administrative authority merely by holding tokens or an allowance.
Diamond and facets	Routing, roles, eligibility, restrictions and token accounting	Public-code assessment boundary. Privileged and ordinary paths have different authority requirements.
Administrative accounts	Owner, ACCOUNT_ADMIN and TOKENIZATION_AGENT	Authority to change code, eligibility or supply; controller custody remains a dependency.
Fund operating services	Request processing, authoritative share records and payments	Private operating boundary; public chain state alone does not prove correctness.

3.1 Adversary model and security objectives

The threat model includes external addresses without administrative roles, approved holders, and allowance spenders affected by changes to their own or their owner's eligibility. Security objectives are preservation of upgrade/role authorization, enforcement of current restrictions, and consistent token accounting across transfer, issuance, lock and redemption transitions.

Controller compromise, erroneous administrative action and reconciliation failure remain material risks. Authorized administrative powers are assessed as trust dependencies unless they violate an implementation invariant.

3.2 Privileged roles and effective powers

Principal	Powers relevant to the assessment	Trust dependency
Owner / TOKEN_ADMIN	Owner-only diamondCut; role administration, global controls and metadata paths. TOKEN_ADMIN administers itself and the other named roles.	Integrity of the upgrade authority and of changes to the role graph.
ACCOUNT_ADMIN	Account activation/deactivation, granular stop codes, lock/unlock, forced movement and forced burn.	Correct eligibility decisions and authorized correction procedures.
TOKENIZATION_AGENT	Mint, direct burn, preparation of burn requests, and approval/rejection of pending burns.	Alignment of token changes with accepted business instructions.
BURNER	Designated redemption destination used by the pending-burn workflow.	Correct interpretation of pending token state and subsequent processing.

At the final snapshot, paused was false, tokenActive was true, pendingOwner was zero and getDelay() was 3,600 seconds. The three principal administrative accounts were 61-byte LightAccount proxies with a shared exact-matched implementation and distinct direct controllers. Those account addresses were also used by MONY. Their on-chain structure does not reveal whether off-chain MPC, HSM custody or enterprise approval controls exist. [E01]

Role holders and controllers are listed in Appendix A; related control observations are detailed in Section 6.

4 Technical Assessment

4.1 Execution surface and upgrade authorization

Loupe enumeration identifies 16 active facets and 68 selectors. Each facet has an identified runtime hash, ABI and exact-matched source bundle. The inventories at blocks 26,077,208 and 26,077,991 agree, with no intervening routing or code change recorded. [E01-E03]

Selector 0x1f931c1c is routed to DiamondCutFacet. Its diamondCut entrypoint invokes LibDiamond.enforceIsContractOwner before selector changes or optional initialization. The recorded unauthorized-call sample reverted with DMND0001, consistent with the source guard. No unauthorized upgrade path was established; the owner's ability to replace logic remains a trust dependency. [E02-E03]

The recorded DiamondCut history contains the constructor cut at block 25,042,223 and no post-deployment cut through the final observation block. The constructor initializer at 0xf27362f7ddd1083194598c95921d7cff530e772d was not publicly source-matched. It is absent from the active facet set and no current selector routes to it; its historical source/build provenance remains unverified. [E01-E03; L01]

4.2 Role administration, governance delay and wallet authority

AccessControlFacetTimelockable and its imported access-control libraries expose the role-admin relationships. grantRole requires the timelock execution condition and the relevant role administrator; revokeRole checks role administration. TOKEN_ADMIN is self-administered and administers ACCOUNT_ADMIN, TOKENIZATION_AGENT and BURNER. The recorded event history and fixed-block hasRole observations identify one holder for each named role, with no recorded revocation through the reviewed history. [E01-E03]

Ordinary-caller samples for `queueTransaction` and `revokeRole` returned FACT0403. An unqueued `grantRole` request returned FACT1004 at the queue/execution boundary. Subsequent role-admin checks are supported by source review rather than by that early-reverting sample.

The three principal holders use the exact-matched `LightAccount` implementation listed in Appendix A. The recorded unrelated-caller execute sample returned `NotAuthorized(address)`, consistent with the identified controller boundary. [E01]

The 3,600-second governance delay does not apply to owner-only `diamondCut`. The resulting upgrade-control dependency is detailed in O01.

4.3 Transfer and delegated-spend restrictions

The installed `ERC20FacetTransferBurnableStoppable` composes the transfer logic with managed-account, global-state and stop-code checks. The inherited `transferFrom` path checks that the token is active and unpaused, that `from_` and the calling spender are currently active, and that a non-burn destination is active. The stoppable wrapper checks the source's transfer-stop flag and the destination's receive-stop flag; a transfer to the authorized burner uses the redemption-stop condition. `approve` also requires the approving owner and spender to be active. [E02-E03]

A pre-existing allowance does not bypass current eligibility checks. Negative samples for an inactive spender and an inactive source both returned FACT0200. Both used a zero amount, corroborating early eligibility rejection rather than a funded-transfer lifecycle. The conclusion rests on the reviewed source path and these supporting samples.

No alternate live transfer selector or subsequent facet replacement was recorded that would change this path at the final snapshot. The examined on-chain behavior is consistent with the public allow-listed operating model. The correctness and timing of the off-chain decision to deactivate an address remain outside scope. [E01-E03; S03]

4.4 Administrative restrictions, locks and corrections

`ManagedAccountFacet` exposes activation, deactivation, locking, unlocking, forced transfer and forced burn, including batch variants. `StopCodesFacet` manages per-account subscription, sending, receiving and redemption restrictions. The retained source review identifies `ACCOUNT_ADMIN` checks on eligibility and stop-code writes. Ordinary-caller activation and stop-code samples returned FACT0401. [E01-E03]

`LibManagedAccount` accounts for units moved between spendable and locked balances. Locking and unlocking change availability without issuing new units; forced transfer moves locked units one-for-one, while forced burn reduces locked units and supply by equal amounts.

Global pause and token activation constrain ordinary transfers. Authorized correction and recovery paths have separate restrictions; the ability to immobilize, move or destroy balances remains an explicit administrator dependency.

4.5 Issuance, pending redemption and supply conservation

`MintableFacet.mint(bytes32,address,uint256)` and `BurnableFacet.burn` require `TOKENIZATION_AGENT`; both unauthorized-call samples returned FACT0402. `BurnPreparableFacet` and `BurnResponsibleFacet` expose preparation and response operations for the role-controlled pending-burn workflow. [E01-E03]

The source review examined the accounting relationships below. S denotes total supply, B the sum of spendable balances and L the sum of locked units. Pending-redemption units remain included in the burner's token balance.

Operation / source anchor	Accounting relationship examined	Assessment basis
Transfer / LibERC20._transfer	Equal decrease and increase in balances; no supply change. Allowance spending changes allowance only.	Library source review [E02-E03]
Mint / LibMintable._mint	Recipient balance and S increase by the same quantity.	Source review; role-boundary samples [E01-E03]
Direct burn / LibBurnable._burn	Holder balance and S decrease by the same quantity.	Source review; role-boundary samples [E02-E03]
Pending request / LibBurnRequestable	Request moves units to the burner without changing S. Approval reduces burner balance and S equally; rejection returns units.	Request/response source review [E02-E03]
Lock / unlock / LibManagedAccount	Changes between B and L preserve B + L and do not change S.	Accounting-library review [E02-E03]
Forced movement / LibManagedAccount	Forced transfer preserves units; forced burn reduces locked units and S equally.	Source and role-guard review [E02-E03]

At block 26,077,208, the six recorded nonzero balances were 49,506,893,544; 10,134,294,776; 194,780,513; 100,237,785; 200; and 100 raw units. Their sum equals the recorded total supply of 59,936,206,918, and lockBalanceOf was zero for each recorded holder. At block 26,077,991, six nonzero balances again reconcile to the same aggregate supply. With two decimals, that supply is 599,362,069.18 JLTXX. [E01-E03]

Recorded snapshot: $\text{sum}(\text{holder balances}) = 59,936,206,918 \text{ raw units}$
Token amount: $59,936,206,918 / 100 = 599,362,069.18 \text{ JLTXX}$

The snapshot supports on-chain balance/supply reconciliation. It does not establish equality to the private Investor Register or underlying asset reserves.

5 Recorded Validation and Coverage

The following read-only observations support the analysis in Section 4. C denotes block 26,077,208; R denotes block 26,077,991. [E01-E03]

ID / baseline	Recorded check	Outcome and evidentiary limit
V01 C, R	Unrelated caller invokes diamondCut	DMND0001. Corroborates the owner guard; does not test authorized upgrade correctness.
V02 C, R	Unrelated caller invokes mint	FACT0402. Corroborates the TOKENIZATION_AGENT role boundary.
V03 C	Unrelated caller invokes burn	FACT0402. Authorization rejection, not execution of a successful burn lifecycle.
V04 C; stop codes also R	Unrelated caller activates an account or updates stop codes	FACT0401. Corroborates ACCOUNT_ADMIN restriction on the sampled writes.

ID / baseline	Recorded check	Outcome and evidentiary limit
V05 C	Unrelated caller queues a transaction or revokes a role	FACT0403. Samples reject before unauthorized administration.
V06 C	grantRole submitted without queued authorization	FACT1004. Establishes the queue precondition for this sample; later checks are supported separately by source.
V07 C	Inactive spender; active source and recipient; transferFrom amount 0	FACT0200. Early current-eligibility rejection; not a stateful funded-transfer test.
V08 C	Inactive source; active spender and recipient; transferFrom amount 0	FACT0200. Same limitation as V07; source path supports the post-deactivation conclusion.
V09 R	Unrelated caller executes through the owner LightAccount	NotAuthorized(address). Corroborates the sampled account execution boundary.
V10 C, R	Balance/supply snapshot and recorded holder lock balances	Aggregate supply reconciles; recorded holder locks are zero. Does not prove private-register or custody reconciliation.

5.1 Historical production-route corroboration

The following historical transactions corroborate production use of the identified issuance, burn and transfer routes. [E01]

Transaction / block	Observed route	Significance
0xf8f6...cd8e 26,059,813	ERC-4337 execution through the shared TOKENIZATION_AGENT; 596.26 JLTXX issued.	Corroborates authorized issuance and the cross-product control relationship.
0x88e2...8192 26,058,629	Agent-authorized burn of 250,000,000.00 JLTXX from the BURNER balance.	Corroborates the privileged burn route; not evidence of completed off-chain payment.
0x2ee8...9147 26,077,930	Transfer of 1.00 JLTXX between active holder accounts.	Corroborates the installed ordinary allow-listed transfer route.

6 Findings and Control Observations

No implementation vulnerability was confirmed. The three observations below concern privileged controls and integration boundaries; they are not included in vulnerability severity totals. No issuer response or remediation verification was available.

ID	Title	Category / status
B3-JLTXX-O01	Owner-directed upgrades are not subject to the governance delay	Privileged-control observation; applicable at snapshot
B3-JLTXX-O02	Administrative accounts are shared across fund products	Operational concentration observation; applicable at snapshot
B3-JLTXX-O03	Token transfers do not establish final legal ownership or settlement	Integration / record-of-ownership observation; applicable to disclosed model

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

Attribute	Record
Affected components	DiamondCutFacet.diamondCut; owner LightAccount; TimelockableFacet
Classification	Control observation. No implementation-vulnerability severity assigned.
Evidence	E01-E03; Appendix A

Description. The deployed upgrade entrypoint enforces Diamond ownership but does not use the 3,600-second governance delay applicable to designated actions such as role grants and ownership transfer/renunciation. The owner is a single-controller LightAccount. The account's execution check prevents an unrelated caller from exercising it in the recorded sample; once legitimately authorized, the owner can replace the implementation surface without that on-chain delay.

Impact and preconditions. Compromise or misuse of owner authority could alter transfer policy, supply accounting and other token behavior in a single authorized upgrade. The risk requires control of, or an authorized action by, the upgrade principal; no ordinary-caller bypass was established. Private approval and custody controls were not verified.

Recommendation. The issuer and contract operator should establish verifiable upgrade approvals and change controls, including multi-party authorization and a documented delay for routine upgrades where operationally compatible, with narrowly defined emergency procedures. Approved releases should identify exact facet addresses, source/build identities and selector changes. Operator monitoring should cover DiamondCut events and changes to the controlling wallet implementation or controller.

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

002 | Administrative accounts are shared across fund products

Attribute	Record
Affected components	Owner / TOKEN_ADMIN, ACCOUNT_ADMIN and TOKENIZATION_AGENT accounts
Classification	Operational concentration observation. No implementation-vulnerability severity assigned.
Evidence	E01, Administrator, role, and dependency graph; Appendix A

Description. JLTXX and MONY share the owner, ACCOUNT_ADMIN and TOKENIZATION_AGENT account addresses. Each is a LightAccount with a single direct controller. The recorded issuance sample uses the common agent route for both products. These shared accounts create a cross-product control dependency; MONY itself is outside this report's assessment scope.

Impact and preconditions. Controller compromise or erroneous authorized action may affect both products. Impact depends on the role: code and role changes, eligibility and forced movement, or issuance/redemption processing. HSM/MPC custody, enterprise approvals and recovery procedures behind these accounts were not assessed.

Recommendation. The issuer and fund operator should document the common-control exposure, key-custody arrangements, approval thresholds, role separation, rotation and emergency revocation. Product-specific accounts or enforceable transaction policies should be considered where they materially reduce cross-product impact. Operational recovery and reconciliation exercises should include shared-account incidents.

Status. Shared control observed at the snapshot; compensating organizational controls not assessed.

003 | Token transfers do not establish final legal ownership or settlement

Attribute	Record
Affected components	Holder transfer and redemption integrations; off-chain Investor Register boundary
Classification	Integration/control observation; disclosed operating model, not a demonstrated contract defect
Evidence	S02-S03; E01, Supply and accounting boundary

Description. The public product documents make the Investor Register authoritative and permit timing differences between token activity and the transfer agent's records. Token movements can be rejected or corrected under the operating model. Similarly, moving units to the burner or approving a burn is not itself evidence of completed external payment.

Impact and preconditions. An integration that treats public balances or burn events as unconditional legal or payment finality may recognize a business outcome prematurely. No deployed integration defect was demonstrated; the observation concerns the disclosed register and settlement boundary.

Recommendation. Fund operators and integrators should distinguish request receipt, register acceptance, cancellation/correction and completed payment in their systems. Reconciliation should use authoritative status records, defined settlement windows and an explicit exception-handling process for unresolved differences.

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

Classification criteria

Where an implementation vulnerability is established, severity considers the supported impact together with realistic reachability and preconditions. Critical denotes system-wide compromise or catastrophic loss; High denotes substantial asset or authority impact; Medium denotes material but bounded impact; Low denotes limited-impact defects. No numerical CVSS score or assurance rating is assigned in this assessment.

Control observations identify material trust or operational dependencies without establishing an implementation defect. Scope limitations identify assertions the evidence does not support. Neither is included in vulnerability totals.

7 RWA Linkage and Public Verifiability

JLTXX represents an interest in a government money-market fund, not a standalone dollar-backed stablecoin. The disclosed economic linkage is between token balances, registered fund shares and the fund's portfolio/NAV. The fund seeks a USD 1 share NAV and invests in the disclosed Treasury, collateralized-repurchase and cash instruments. A target NAV is not a guarantee of market value or principal. [S02-S04]

Assertion	Available public evidence	Assurance boundary
Product and token identity	Issuer announcement identifies the Ethereum token address. [S01]	Deployment attribution established for the listed address.
Legal share linkage	Prospectus describes Token Class balances and the authoritative Investor Register. [S02-S03]	The register is private; synchronized holder-by-holder ownership was not independently reconciled.
On-chain quantity	Recorded supply and holder balances reconcile at the stated block. [E01-E03]	Token accounting only; not portfolio, custody or legal-share assurance.
Valuation and portfolio disclosure	Public fund documents and the 31 August 2026 fact sheet. [S02, S04]	Disclosure dates differ from the contract snapshot. No same-cutoff token/register/custody reconciliation was obtained.

Public information supports the stated linkage mechanism and the identity of the Ethereum representation. It does not supply a continuous, independently reconciled connection from every outstanding token to a contemporaneous legal share record and corresponding custodial assets. This report therefore does not assign a reserve-coverage percentage or infer an unqualified one-to-one backing attestation.

A complete reconciliation requires records aligned by share class, valuation basis, legal entity and cutoff time. Fund-wide assets or an earlier NAV publication are not directly comparable with a later token supply without those alignments.

8 Limitations and Conclusion

ID	Limitation	Effect on conclusions
L01	Historical initializer provenance is incomplete. The constructor target is not publicly source-matched and is not a current facet.	Historical initialization logic and its source/build correspondence remain unverified; conclusions address the current deployed surface.
L02	Private register, request processing and settlement controls are outside scope.	No assurance is provided over legal-share reconciliation, request acceptance/rejection/correction, completed payments, or underlying fund/custody records.
L03	Engineering and organizational control provenance is incomplete.	Issuer release provenance and off-chain key custody, approvals, monitoring, incident response and compensating controls were not independently verified.
L04	Behavioral validation is targeted, not comprehensive.	The samples do not establish complete success/failure-path or state-transition coverage. No comprehensive regression/property-testing evidence is included.

Conclusion

The reviewed source paths and recorded production observations support the stated authorization, current-eligibility and local accounting controls. No reportable implementation vulnerability was confirmed. The conclusion remains subject to the privileged-control dependencies and limitations identified above.

The conclusions apply only to the listed deployment and observation dates. Material changes to contract implementations, permissions or administrative accounts require reassessment; an unchanged token address does not establish an unchanged system.

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

A Deployment and Authority Inventory

The following facet inventory applies at block 26,077,991. All 68 selectors, full runtime hashes and verified-source links are included in the attached scope manifest. [E01-E03]

Facet	Ethereum address	Count
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	0x5Be781F803552A0532FB03F6513D5a4bach665a9	2
BurnableFacet	0x88183F91a0A7315BD3e2102BE7520c88cE9EFF67	1
ERC20FacetTransferBurnableStoppable	0x1aA6CF30f6b4F18F5cf12cC0F2c8543eaabE62D6	9
MintableFacet	0xe70C597957E542209eD44f2fbaE58370089E59be	1
TimelockableFacet	0xcA76E9791De59331219bBa4BE1d0540eda8764C	7
BurnResponsibleFacet	0x8c2FbC1DF5918CB15b96aD4d57298988c73dac32	3
StopCodesFacet	0x996440281f77B4D664878B0B14a10E909Fc3310B	2
BurnPreparableFacet	0x981b3af7957841CE2c8869Ee25055a693a89006B	1

Administrative account and controller inventory

The first three role holders use the shared LightAccount implementation below. The BURNER address has zero runtime code at the assessment snapshot. [E01]

Role	Role holder / direct controller
Owner / TOKEN_ADMIN	Holder 0x5aE5d4AdA523985DbAB22CF046599979897C8418 Controller 0xBB30949145942aa7a5BDCd358160a8D6cEd119Cc
ACCOUNT_ADMIN	Holder 0x20aab6c346ac47f6b7f8c5d76f1f85d7367197d8 Controller 0x09D3A27bc30cf916ccfaA80A878b3E46098b8147

Role	Role holder / direct controller
TOKENIZATION_AGENT	Holder 0x9f5252058521e7458195a0350a0dc361c225857a Controller 0x40E06b1daAe4A4910a66617EE4197026019b6C6c
BURNER	Holder 0xfb448891b3c1628b0e6b7b0c92b9e0013e28b5a9 Controller Not a LightAccount in the recorded snapshot

LightAccount implementation: 0x8E8e658E22B12ada97B402fF0b044D6A325013C7

Administrative-proxy runtime Keccak-256:

0xaaa52c8cc8a0e3fd27ce756cc6b4e70c51423e9b597b11f32d3e49f8b1fc890d

Historical initializer, not an active facet:

0xf27362f7ddd1083194598c95921d7cff530e772d. Source/build correspondence was not obtained. [L01]

Machine-readable scope attachment

The attached **jltxx-scope-manifest-en.json** contains the deployment, selector, runtime and authority inventory, source references and evidence checksums.

Manifest SHA-256:

3e894343612531696c9974b36bdde2c009f4a817c4dae052a0bfeafc574ccbea

B Evidence and Source Index

Assessment evidence

E01-E04 identify the assessment workpapers supporting this report. S01-S08 identify the primary public sources. Evidence checksums are included in the scope manifest.

ID	Record	Role in this report
E01	Deployment and configuration assessment	Deployment, source correspondence, controllers, event history, production routes and balance aggregate.
E02	Source and authorization analysis	Facet inventory; role, transfer and accounting analysis; negative-call samples.
E03	Independent technical review	Independent review of the execution, authorization, eligibility and accounting conclusions.
E04	Production snapshot verification	Deployment and control-state verification at the final observation block.

Claim-to-evidence map

Report assertion	Primary assessment support
Execution scope and fixed-version identity	E01-E04; S01, S05-S07; full manifest
Upgrade / role / controller authority	E01; E02-E03 authorization analysis; S08
Current eligibility in delegated spend	E02-E03 delegated-spend analysis; E01 deployment verification
Local accounting and snapshot reconciliation	E02-E03 accounting analysis; E01 balance aggregate
Recorded sample results	E01-E02; Section 5 specifies each sample's block and interpretation
Share/register linkage and limitations	S02-S04; E01 business-boundary observations

Primary public sources

S01 | J.P. Morgan Asset Management - JLTXX launch announcement
13 May 2026. Issuer attribution and Ethereum deployment address.

S02 | SEC-filed prospectus - JPMorgan Trust IV, Token Class
13 May 2026, supplemented 17 August 2026. Product strategy, ownership register, token processing and correction powers.

S03 | SEC-filed summary prospectus - JLTXX
Supplemented 17 August 2026. Public operating model and eligibility/register boundaries.

S04 | J.P. Morgan - JLTXX fund fact sheet
Reporting date: 31 August 2026; earlier than the contract snapshot.

S05 | Sourcify - verified deployment source and compilation records
Entrypoint source and compilation record. Individual facet source links are in the scope manifest.

S06 | Ethereum observation block 26,077,991
Final observation block used in this assessment.

S07 | JLTXX deployment transaction
Block 25,042,223; 7 May 2026. Constructor DiamondCut and initializer identity.

S08 | Sourcify - Alchemy LightAccount implementation
Verified source record for the shared administrative-account implementation.