

CUMIU

Provisional Candidate Deployment Security Assessment

ChinaAMC USD Digital Money Market Fund, Tokenized Unlisted Class I USD
Public-evidence review of an unauthenticated candidate Ethereum deployment

REPORT	B3-CUMIU-2026-001
ISSUED	1 October 2026
BASELINE	Candidate graph at Ethereum block 26,077,917
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 7

7 RWA Linkage and Public Verifiability 9

8 Limitations and Conclusion 10

A Candidate Deployment Inventory 10

B Evidence and Source Index 11

Assessment of a technically high-confidence but issuer-unconfirmed candidate deployment. Technical observations, product evidence and exclusions are defined in Section 2.

1 Executive Summary

bench3.ai assessed the public code, configuration and recorded behavior of an Ethereum deployment that identifies itself as ChinaAMC USD Digital Money Market Fund Class I USD with symbol CUMIU. The technical correlation is very high, but no issuer-, administrator- or tokenization-agent-controlled publication was found that binds ISIN HK0001153516 to the exact proxy and implementation/RuleEngine graph. The deployment therefore remains a candidate and the opinion is provisional. [E01-E04; S01-S04]

The reviewed graph comprises an EIP-1967 proxy, an exact-matched CMTAT implementation, a nonzero RuleEngine and one active RuleWhitelist. Recorded assessment work covered initialization, upgrade and role state, rule configuration, transferFrom validation semantics, complete public event history through the cited anchor, and public RWA linkage. It did not authenticate the deployment for the legal share class or audit private registrar, allowance, key-custody, NAV or settlement records. [E01-E08]

Provisional assessment conclusion

No reportable implementation vulnerability was confirmed for the candidate deployment. One control observation and one unconfirmed candidate are reported. The unconfirmed candidate concerns a real code-level omission in delegated-transfer validation, but current public evidence does not establish the operational preconditions or policy violation required to classify it as an exploitable vulnerability.

Classification	Recorded result
Confirmed vulnerabilities	Critical 0 High 0 Medium 0 Low 0
Control observations	1; privileged lifecycle and upgrade authority
Unconfirmed candidates	1; delegated-transfer spender eligibility
Deployment identity	Candidate; issuer mapping unconfirmed

Material qualification

The reviewed token code does not validate the transferFrom caller as a policy subject: the active path checks the token owner and recipient, while the current rule also ignores the spender. Recorded read-only behavior checks confirmed that this omission affects delegated-transfer execution. The official product model describes permissioned direct-shareholder wallets, administrator-executed transactions and no peer-to-peer or secondary-market trading; public history contained no Approval or holder-to-holder transfer event. Without an issuer-attested live allowance/operator inventory and policy for frozen or delisted spenders, the condition remains an assurance gap rather than a confirmed vulnerability. [E03-E04; B3-CUMIU-U01]

2 Scope and Assessment Basis

2.1 Candidate deployment baseline

Parameter	Assessment record
Network	Ethereum mainnet; chain ID 1
Candidate token proxy	0x85D38585c3aC08268F598282a84b7c0Ddfc0d04F
Current implementation	0x37686928ddf77be20fc4199f03f0638d90d9907e
Policy graph	RuleEngine 0x938ac352e422985b86FE0Fa8bf2D0216A30bEef2; active RuleWhitelist 0x43EdBAB290E6B539a507800B1220e4a80E23B732
Primary technical snapshot	Block 26,077,917 hash 0xf525476002386ea0f6dd5beb46f64530e3d4f2747e1d1fb633f9b61bc033a70d 2026-09-28 19:02:47 UTC
Identity status	High-confidence technical candidate; issuer-approved product mapping not established

The proxy runtime Keccak-256 was recorded as 0x5e4dcb0bb1910f6429e5fe91678990088a51c6d1cfe1b31d05fb9d948cc7867c and the implementation runtime Keccak-256 as 0x445fed923e4f0bb8d6aef48ad4669413d6339e3d84911775ee5485db92065778. Sourcify exact creation/runtime correspondence was recorded for the implementation with Solidity 0.8.17+commit.8df45f5f. Exact bytecode correspondence does not authenticate the asset-to-address mapping. [E01-E02; E07]

2.2 Assessment type and methods

Method	Applied scope
Bytecode-bound static review	Proxy/implementation relationship, initialization, authorization, transfer hooks, RuleEngine and RuleWhitelist behavior using archived exact-matched source.
Read-only state review	Recorded fixed-block implementation, role, pause, rule-list and whitelist state; no production transaction was signed or broadcast.
Historical review	Archived complete proxy and RuleEngine event censuses through block 26,077,473 and deployment-transaction reconstruction.
Read-only behavior checks	Recorded eth_call results for delegated-transfer and allowance-order hypotheses. These checks establish code behavior, not the existence of a live allowance/operator relationship.
Public product and RWA review	Issuer, administrator, tokenization-provider and fund-level materials available through 30 September 2026.

Method boundary: all production interactions supporting this assessment were read-only and are bound to the observation blocks and dates identified above. No state-changing production transaction or private-system test forms part of the evidence basis. [E03-E05]

2.3 Included and excluded boundaries

Included: the four-address candidate execution graph, its recorded deployed configuration, initialization and public history, the assessed transferFrom path, and public evidence describing the named share class.
Excluded: issuer authentication of the address graph; private wallets and delegated-operator inventories; administrator and signer custody; registrar and distributor ledgers; NAV production; subscription/redemption operations; cash settlement; legal advice; financial-statement audit; and reserve or solvency attestation.

The publication date is 1 October 2026. It is not a statement that chain state, roles or business policies were re-observed on that date. Technical state is bound to the exact observation anchors identified in this report; public RWA synthesis has an evidence cutoff of 30 September 2026.

3 System and Threat Model

The candidate deployment is a permissioned, upgradeable CMTAT token. The proxy delegates token logic to the implementation. ValidationModule applies pause, owner/recipient freeze and RuleEngine checks before balance movement. The active RuleEngine delegates to one RuleWhitelist that evaluates the transfer owner and recipient. [E03-E04]

Security principal	Recorded authority or dependency
Configured administrator	DEFAULT_ADMIN_ROLE and the implementation's broad business-role treatment; security-sensitive mint, burn, freeze, pause, enforcement and upgrade powers.
RuleEngine administrator	Can change the external policy engine or its active rules; the recorded graph had one nonzero active rule.
Direct shareholder / approved wallet	May hold token units subject to permissioning and administrator-operated product procedures described in the prospectus.
Delegated spender	ERC-20 allowance authority; the deployed transfer validation does not independently evaluate this caller's whitelist or freeze status.
Registrar / administrator records	Private records and reconciliation determine the legal and operating relationship beyond public balances.

Assessed security properties

The review considered whether an ordinary caller could seize an uninitialized proxy, bypass the installed policy graph, exploit allowance evaluation order, or exercise delegated transfers contrary to the intended restriction boundary. It also considered whether the public deployment could be treated as authenticated CUMIU scope and whether chain supply could be equated with legal shares or fund assets.

Trusted administrator action or compromise remains capable of changing token behavior. Such power is not itself classified as a permissionless vulnerability; it is a trust dependency whose operational controls were not available for assessment. [B3-CUMIU-O01]

4 Technical Assessment

4.1 Initialization and implementation identity

The proxy was created in transaction 0x27e5f51891dc7f9402b2f42654b8e631fd806151c3f72a6fc191406db24cd691 at block 23,038,326 with nonempty initializer calldata. The receipt recorded the implementation upgrade, DEFAULT_ADMIN_ROLE grant and Initialized(1). At block 26,070,619, initializer storage remained version 1, the EIP-1967 slot still resolved to the assessed implementation, and an unrelated initialize replay reverted as already initialized. The previously alleged public-initialization takeover is therefore not present in this candidate deployment. [E05]

4.2 Installed policy graph

At block 26,077,473 the proxy was unpaused and referenced nonzero RuleEngine 0x938ac352e422985b86FE0Fa8bf2D0216A30bEef2. The engine contained exactly one active RuleWhitelist with 12 whitelisted addresses. Complete archived event history identified no RuleEngine replacement, RemoveRule or ClearRules event through that block. The zero-engine hypothesis is not the recorded deployed state and requires trusted reconfiguration rather than an ordinary-caller path. [E03-E04]

The RuleEngine runtime Keccak-256 was 0x0f06de0740adfde4d5f05ca1b91976aaf289a84a842a5303c50e81905b569602; the active RuleWhitelist runtime Keccak-256 was 0xb207b5257652e132fb2a409bcd2925ba89722e7037d4b9b5b1e58e383a0d3ed6. Exact-matched source showed that the engine forwards from, to and amount, and the active rule checks whitelist[from] and whitelist[to]. [E03; S05-S06]

4.3 Delegated-transfer validation

The deployed transferFrom route spends allowance and then enters the token-transfer hook. The hook supplies from, to and amount to the validation layer but not msg.sender. The implementation's approve route also does not apply a spender-eligibility gate. Consequently, a spender that already holds sufficient allowance is not independently rejected because the spender itself is frozen, not whitelisted or otherwise ineligible; owner and recipient checks still apply. [E03-E04]

Recorded read-only behavior checks confirmed that an ineligible spender with otherwise sufficient delegated authority could execute transferFrom between eligible token accounts. This establishes the code behavior. It does not establish a live allowance, an independently controlled spender, or an issuer policy that freeze, delisting or KYC revocation must terminate existing delegated authority. [E03-E04]

Recorded public history through block 26,077,473 contained 19 mint transfers, 11 burns, no holder-to-holder transfers, no Approval event and no Freeze/Unfreeze event. The official prospectus describes no peer-to-peer or secondary-market trading and places token transactions under Manager instruction or confirmation and Administrator execution. These facts weaken current ordinary-participant reachability but do not prove that private allowance or operator relationships do not exist. [E03; S02]

4.4 Allowance-order hypothesis

Although transferFrom spends allowance before invoking transfer validation, the active RuleEngine and RuleWhitelist cannot read token allowance and do not branch on pre-spend or post-spend allowance state. Recorded read-only comparisons produced the same authorization outcome across the assessed allowance states; a later revert would roll back the prior write atomically. No current authorization difference was established from this ordering. [E03-E04]

5 Recorded Validation and Coverage

Recorded check	Result and evidentiary meaning
Deployment initialization	Constructor calldata, receipt, storage and replay evidence show atomic initialization and reject the public-takeover hypothesis.
Two-RPC fixed-block state	Consistent implementation, RuleEngine, rule count, active RuleWhitelist, pause state and whitelist count were recorded at block 26,077,473.
Event-history census	Proxy and RuleEngine histories were paginated through the anchor; no P2P transfer, Approval, freeze/unfreeze, engine replacement or rule removal was recorded.
Delegated-transfer behavior	Read-only validation confirmed the missing spender check; this is mechanism evidence, not proof of a production actor path.
Allowance-order comparison	The assessed allowance states yielded the same result because the only active rule does not inspect allowance.
Product/deployment identity review	Issuer and service-provider materials establish the product and Ethereum model but do not publish the assessed address graph.

The behavior checks establish the assessed code paths; they do not establish that a live allowance/operator relationship or the relevant private-policy semantics existed in production. [E03-E05]

6 Findings and Control Observations

No confirmed implementation vulnerability is reported. The records below distinguish a present trust dependency from a technically real but operationally unsubstantiated candidate. Neither is included in vulnerability severity totals. No issuer response or remediation evidence was recorded.

ID	Title	Classification / status
B3-CUMIU-O01	Privileged lifecycle and upgrade authority remains a trust dependency	Control observation; applicable to candidate snapshot
B3-CUMIU-U01	Delegated-transfer validation does not evaluate spender eligibility	Unconfirmed candidate; verification pending

001 | Privileged lifecycle and upgrade authority remains a trust dependency

Attribute	Record
Affected components	CMTAT authorization, pause/freeze, mint/burn, RuleEngine and upgrade paths
Classification	Control observation. No implementation-vulnerability severity assigned.
Evidence	E03-E05; Appendix A

Description. The candidate system is deliberately administrator-controlled. The configured administrator receives DEFAULT_ADMIN_ROLE and the implementation treats that principal as holding the security-sensitive business roles used for issuance, destruction, account restrictions, pause and upgrade administration. RuleEngine configuration is likewise privileged. The reviewed state did not expose these powers to an unrelated caller.

Impact and preconditions. Compromise, misuse or erroneous action by the authorized control plane could change transfer policy, restrict holders, alter supply or replace executable logic. The impact requires authorized control or compromise of the relevant principal; private key custody, approval thresholds, separation of duties and recovery controls were not assessed.

Recommendation. The issuer, Administrator and tokenization operator should maintain an authenticated deployment and authority manifest, multi-party approval for security-sensitive changes, documented emergency procedures, key rotation and monitoring for upgrades, RuleEngine/rule changes, role changes, mint/burn, freeze and pause events. Routine upgrades should identify the approved source/build and effective block.

Status. Applicable to the candidate snapshot; compensating organizational and custody controls were not assessed.

U01 | Delegated-transfer validation does not evaluate spender eligibility

Attribute	Record
Affected components	approve; transferFrom; ValidationModule; RuleEngine; active RuleWhitelist
Classification	Unconfirmed candidate - verification pending. No vulnerability severity assigned.
Evidence	E03-E04; S02; S05-S07

Description. The deployed delegated-transfer path validates the token owner and recipient but does not supply msg.sender to the policy layer. The active rule also ignores the spender. A caller with sufficient allowance can therefore pass token-policy validation even if the caller is independently frozen or not whitelisted, provided the owner and recipient satisfy the checks. Recorded read-only behavior validation confirmed this result.

Impact and preconditions. A policy bypass would require a positive live allowance or equivalent delegated authority, an independently controlled spender that later becomes restricted, and an intended policy under which that restriction must terminate previously granted transferFrom power. None of these decisive production conditions was established. The public product model and event history instead show tightly administered mint/burn operation with no recorded Approval or P2P transfer through the anchor.

Recommendation. The issuer and Administrator should define whether spender freeze, whitelist removal or KYC revocation must invalidate existing delegated authority and provide a block-bound allowance/operator inventory. If spender eligibility is intended to be enforced, the contract operator should add spender-aware

checks to allowance grant and transferFrom execution, then verify the change against the exact deployed implementation and rule set.

Status. Code behavior substantiated; production reachability and policy violation not substantiated. No issuer response or remediation evidence recorded.

Initialization and rule-configuration validation

Deployment records, fixed-block storage and a rejecting replay show that the proxy was atomically initialized and was not publicly claimable at the assessed state. The installed RuleEngine was nonzero and retained one active RuleWhitelist throughout the recorded history. Allowance-order comparisons produced no authorization difference under that rule. These technical statements are not remediation findings and do not transfer to a later implementation or rule configuration. [E03-E05]

7 RWA Linkage and Public Verifiability

Public product evidence identifies the ChinaAMC USD Digital Money Market Fund Tokenized Unlisted Class I USD, ISIN HK0001153516, as an accumulating class using end-of-day variable NAV. It identifies Standard Chartered Bank (Hong Kong) Limited as administrator, registrar, tokenization agent, platform operator and token custodian, and identifies Ethereum as the primary blockchain. [E01; E06; S01-S04]

Layer	Publicly supported statement	Unresolved boundary
Legal product	The share class, ISIN and principal service-provider roles are described in official materials.	No official artifact binds that legal share class to the assessed proxy.
Pricing	The class uses end-of-day variable NAV for subscription and redemption.	Private dealing records and same-cutoff token/share reconciliation were not available.
Fund assets	Fund-level financial and valuation evidence exists in public issuer and audited materials.	This assessment did not attest assets, liabilities, custody balances or current solvency.
On-chain units	The candidate proxy's metadata, supply and execution graph were recorded at fixed state.	Candidate token supply cannot be stated as the legal share count without the missing mapping and registrar reconciliation.

Public materials support the named fund's identity and financial disclosures, but they do not authenticate the candidate deployment for its legal share class. That missing mapping prevents a complete token-to-product conclusion; this assessment provides no credit rating or reserve opinion. [E06]

8 Limitations and Conclusion

ID	Limitation	Effect on conclusions
B3-CUMIU-L01	Issuer-approved deployment mapping is unavailable.	The report cannot authenticate the candidate graph as the production contract for Class I USD or ISIN HK0001153516.
B3-CUMIU-L02	Live delegated allowances, operator controllers and spender-lifecycle policy are not public.	B3-CUMIU-U01 cannot be closed as safe or promoted to a confirmed vulnerability.
B3-CUMIU-L03	Issuer release manifest, complete administrator inventory and private key/change controls were not assessed.	Exact-matched bytecode supports the reviewed execution logic but not issuer-approved release provenance or operational security.
B3-CUMIU-L04	Registrar, custody, NAV, legal-share and settlement records were outside scope.	No legal ownership, valuation, reserve, solvency or completed-payment assurance is provided.

Conclusion

Subject to the provisional identity and evidence boundaries above, no reportable implementation vulnerability was confirmed in the candidate proxy's recorded initialization, policy-engine configuration, allowance-order or ordinary-caller paths. Broad authorized controls remain a trust dependency, and delegated-transfer spender eligibility remains an unconfirmed candidate requiring issuer policy and live-authority evidence.

This opinion applies only to the exact candidate addresses and observation anchors listed in the report. It must not be represented as an authenticated audit of the CUMIU production product. A different implementation, RuleEngine, rule set, role state, or authenticated deployment requires a new applicability review.

A Candidate Deployment Inventory

The inventory below records the technically correlated candidate graph at the principal observation snapshot. Identity remains provisional. [E01-E04]

Component	Address	Recorded identity
Candidate proxy	0x85D38585c3aC08268F598282a84b7c0Ddfc0d04F	EIP-1967 proxy; 708-byte runtime; candidate
Implementation	0x37686928ddf77be20fc4199f03f0638d90d9907e	CMTAT_PROXY; Sourcify exact match; Solidity 0.8.17
RuleEngine	0x938ac352e422985b86FE0Fa8bf2D0216A30bEef2	One active rule at block 26,077,473
RuleWhitelist	0x43EdBAB290E6B539a507800B1220e4a80E23B732	Active rule; 12 whitelisted addresses at block 26,077,473

The later identity-review snapshot at block 26,077,917 recorded raw supply 5,300,427,443,000,000,000,000,000 and paused=false. This fixed-state quantity is not asserted to equal the legal share count. [E01-E02]

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	CUMIU public deployment-identity evidence review
E02	CUMIU public deployment-identity evidence record
E03	CUMIU delegated-transfer and policy evidence record
E04	CUMIU technical assessment outcome
E05	CUMIU proxy initialization verification record
E06	Tokenized Treasury RWA anchor and public-verifiability assessment
E07	CUMIU deployment registry snapshot
E08	Tokenized Treasury final assurance and delivery opinion

Primary public sources

- S01** | ChinaAMC USD Digital Money Market Fund product page
Issuer product identity, share class, ISIN and launch information; recorded in the evidence review through 29 September 2026.
- S02** | ChinaAMC Digital OFC Prospectus, September 2026
Official product, permissioning, service-provider, blockchain and dealing model; document dated 14 September 2026 and archived with SHA-256 in E01/E03.
- S03** | Standard Chartered support for ChinaAMC tokenised fund
Primary service-provider relationship evidence retained in E01; it does not publish the contract address.
- S04** | Libeara ChinaAMC case study
Tokenization-provider product relationship evidence retained in E01; it does not authenticate the candidate graph.
- S05** | Sourcify exact-match RuleEngine record
Bytecode-bound source record used by the archived technical assessment.
- S06** | Sourcify exact-match RuleWhitelist record
Bytecode-bound source record for the only active rule at the recorded anchor.
- S07** | CMTAT current spender-aware validation reference
Upstream comparison recorded by the technical assessment; not the source identity of the candidate deployment and not evidence of remediation.
- S08** | ChinaAMC Digital OFC 2025 audited financial statements
Historical fund-level financial evidence cited by the RWA assessment; not a same-date reserve or deployment attestation.

Scope attachment

cumiu-scope-manifest-en.json
SHA-256: 871b0b6fed3035a141d3461878fb3d7d7cfe82707749539f21e86a0a239c55b0