

# iBENJI

## Public Smart-Contract Security Assessment

Franklin OnChain Institutional Liquidity Fund

Ethereum and BNB Chain assessment with material private-settlement and source limitations

|          |                                                                   |
|----------|-------------------------------------------------------------------|
| REPORT   | B3-IBENJI-2026-001                                                |
| ISSUED   | 1 October 2026                                                    |
| BASELINE | Fixed Ethereum and BNB Chain observations on 28-29 September 2026 |
| 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 . . . . . 7

6 Findings and Control Observations . . . . . 8

7 RWA Linkage and Public Verifiability . . . . . 9

8 Limitations and Conclusion . . . . . 9

A Evidence and Source Index . . . . . 10

Assessment of official token and module deployments, retained verified source, runtime identities, fixed-state role/configuration observations, assessment conclusions and public product evidence.

# 1 Executive Summary

bench3.ai assessed the official iBENJI deployments on Ethereum and BNB Chain, including the Fund Token, Registry, Authorization, Transactional, Transfer Agent, Intent Validation, MultiSig and related token-writing control surfaces. The work addressed deployed identity, role and feature authorization, allowance-based transfers, request creation and cleanup, privileged settlement, multisig execution and upgrade boundaries. [E01-E08]

**Assessment conclusion**

No reportable vulnerability was confirmed in the examined public-contract scope. This conclusion is materially qualified: both live Transactional implementations remain without exact verified source/build correspondence; the production CX settlement builder and account/requestId composition are private; and the issuer's authoritative allowance lifecycle policy is unavailable. These gaps are preserved as limitations rather than converted into clean findings dispositions.

| Classification                 | Recorded result                                                                  |
|--------------------------------|----------------------------------------------------------------------------------|
| Confirmed vulnerabilities      | Critical 0   High 0   Medium 0   Low 0                                           |
| Control observations           | 2; privileged token-writing authority and policy-dependent allowance persistence |
| Material technical limitations | Unverified Transactional runtimes and private CX settlement builder              |

The examined public paths support a bounded conclusion about current deployed authorization and the tested ordinary-caller hypotheses. They do not establish correctness of every Transactional cleanup/replay transition, private settlement record composition, legal shareholder reconciliation or cash settlement.

## 2 Scope and Assessment Basis

### 2.1 Assessment identity

| Parameter       | Assessment basis                                                                                                                                                                                                                               |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assessment type | Public smart-contract and deployment assessment; not a full platform, settlement, legal or financial audit                                                                                                                                     |
| Evidence cutoff | Technical production evidence through 29 September 2026; RWA linkage evidence through 30 September 2026                                                                                                                                        |
| Networks        | Ethereum mainnet and BNB Smart Chain                                                                                                                                                                                                           |
| Methods         | Official deployment inventory review, proxy/implementation resolution, verified-source and runtime comparison, fixed-block role/configuration reads, retained event-history analysis, read-only negative calls and issue-classification review |

### 2.2 Core deployment inventory

The inventory below records the official proxies and their active implementation identities at the cited blocks. Source-match terminology follows the retained Sourcify registry: the Ethereum implementation records use source, creation and runtime match, the corresponding BNB records use exact match, and both Transactional implementations remain unverified. [E01-E04]

| Network   | Component and proxy                                       | Implementation identity                                                                                                                                          |
|-----------|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ethereum  | Fund Token 0x90276e9d4a023b5229e0c2e9d4b2a83fe3a2b48c     | MoneyMarketFund_V6 at 0xa74372dfde0df8a08a3ac7b60c5379f90ac9c7dd; Sourcify source match; creation and runtime match recorded                                     |
| Ethereum  | Authorization 0x12abff8dca2d09d99019dfcc9bf07539a8264066  | AuthorizationModule_V2 at 0x52eba4771c4e4e6ce7c9cdeef0d464ebd8a28da2; Sourcify source match; creation and runtime match recorded                                 |
| Ethereum  | Transactional 0x1933797bbf8f901b69bb81245d5a82091a0e0b76  | Version 4 at 0xe96863c6ae912b5d33d6d88fb63f906d6e5013ef; runtime hash 0x58713f7c255e7b16db9686bfd40cf8d4cdec2638221742be87c5fc47fed7321; unverified source/build |
| Ethereum  | Transfer Agent 0xab266e4fa5d088cc440433c3ea1e066fd710a0a5 | TransferAgentModule_V5 at 0xcf638feed21cfd8f00e8e8c66b7150fb9b57de53; Sourcify source match; creation and runtime match recorded                                 |
| BNB Chain | Fund Token 0x3d0a2a3a30a43a2c1c4b92033609245e819ae6a6     | MoneyMarketFund_V5 at 0xd001e4edbea7d0e46cfee05cb95bc9664dc1da34; Sourcify exact match                                                                           |
| BNB Chain | Authorization 0xfe1ce41141d489983e87cad56943e4d92bd12014  | AuthorizationModule_V2 at 0xf416a5f3305971558a1ce2e73c7d054118949240; Sourcify exact match                                                                       |

| Network   | Component and proxy                                       | Implementation identity                                                                                                                                                     |
|-----------|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BNB Chain | Transactional 0xab56aa7f1ed443401cefb3ed17d2795d4da59f6c  | Version 4 at<br>0xada26ec4aefc2b5ca3b4d38c130d0cbaf511a7e1; runtime<br>hash 0x36f0e42dbca6e109fb7926cd7086f62c46e5e39396<br>1a707ec0b9c1c0216c4755; unverified source/build |
| BNB Chain | Transfer Agent 0x6c4dd0157b714e269e11242e2a4812ab2c043318 | TransferAgentModule_V5 at<br>0x31c2f6c0ad0397e61886d773ea7ba1cecae90729;<br>Sourcify exact match                                                                            |

The attached scope manifest also identifies the Registry, Token Registry and Intent Validation deployments, two Ethereum SwapPools, weighted multisig and fixed role-enumeration anchors used at the token-writing boundary. This inventory identifies the assessed basis; it does not imply complete dependency testing or private legal-share, NAV or settlement assurance. [E01-E04; S01]

### 2.3 Exclusions

Excluded were the proprietary Benji/FTIS production settlement builder, private request and shareholder databases, authentication and KYC systems, address-reuse and offboarding records, payment rails, NAV and portfolio accounting, legal shareholder register, organization-level key custody and approval procedures, and complete end-to-end CX settlement. Production interaction was read-only.

## 3 System and Threat Model

iBENJI uses upgradeable token and module contracts on two EVM networks. Authorization modules maintain shareholder, freeze and administrative roles. Transactional modules create and maintain asynchronous requests. Transfer Agent modules perform privileged settlement and token-writing operations. Intent Validation and weighted multisig components support authorized transaction execution, while Ethereum SwapPools hold constrained token-writing capability for configured pairs. The public contracts are one layer of a broader proprietary transfer-agent platform. [E01-E04]

| Actor or layer                           | Relevant capability                                                                  | Security boundary                                                                           |
|------------------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Approved holder or spender               | Direct and allowance-based transfer when enabled; self-service requests when enabled | Must remain subject to authorization, freeze, balance, allowance and feature controls       |
| Transfer Agent and module operators      | Mint, burn, settle, administer transfers and write token state                       | Privileged execution requires correct backend record composition and operator authorization |
| Weighted multisig and module owners      | Authorize upgrades and higher-impact administrative changes                          | Signer custody, independence and approval procedures remain external trust dependencies     |
| Private Benji platform and legal records | Bind identities, requests, settlement and legal ownership                            | Not publicly verifiable from token state alone                                              |

## 4 Technical Assessment

### 4.1 Deployment and source correspondence

The Ethereum Fund Token, Authorization and Transfer Agent implementations were tied to current official proxies and had Sourcify source matches, with creation and runtime matches recorded, at the recorded block. The corresponding BNB Chain implementations were tied to current official proxies and had Sourcify exact matches. The two Transactional implementations were each 18,045 bytes, exposed the expected request, cancellation, clearing, unlisting and detail selectors, and reported version 4. Their executable bodies were identical after normalizing implementation-self constants and excluding differing metadata, which closes a cross-chain divergence concern. It does not prove exact equivalence to the available TransactionalModule\_V4 source or every cleanup and replay state transition. [E01-E04; L01]

### 4.2 Holder transfer and request controls

Verified token source defines direct holder transfer and allowance-based third-party transfer as separately administered features. transferFrom applies authorization and freeze checks to source and destination while using the dedicated third-party-transfer flag. At Ethereum block 26,077,505, instant transfer, direct ERC-20 transfer and third-party transfer were all enabled. The examined self-allowance condition therefore did not establish a distinct capability or a bypass of a documented global pause. [E02-E03]

At Ethereum block 26,074,034 and BNB block 124,473,344, both Transactional proxies reported self-service disabled. Read-only calls to purchase, partial-liquidation and full-liquidation request selectors from an ordinary address reverted with SELF\_SERVICE\_NOT\_ENABLED before pending state. The recovered runtimes also contained an active isAccountFrozen call consistent with the V4 guard. This refuted current ordinary-holder pending-request accumulation and frozen-request creation, but L01 remains because exact source/build correspondence for the active runtimes is absent. [E02; E08]

### 4.3 Privileged token-writing authority

Complete same-block enumeration found four Ethereum contract holders of WRITE\_ACCESS\_TOKEN and one BNB contract holder, with no EOA holder. Transfer Agent calls remained administrator-gated. The two Ethereum SwapPools used a shared verified version-6 implementation with constrained configured pairs, authorized trader/destination checks, balances and token-level shareholder/freeze controls; no generic arbitrary-call entrypoint or privileged Fund Token sink was present. [E02-E03]

The remaining Ethereum role holder was weighted multisig 0x7687da958f1b8799b8b0df39d2f2d729cf3d85bf with normal threshold 2, high threshold 6, eleven positively weighted signers and two submitters. Ordinary callers reverted INVALID\_CALLER, and a configured submitter without signatures reverted INSUFFICIENT\_THRESHOLD\_ACQUIRED. A production upgrade record showed signedDataExecution with four signatures. Broad authority remains a privileged control dependency rather than an ordinary-caller escalation in the observed configuration. [E02-E03; O01]

### 4.4 Private CX settlement boundary

Verified TransferAgentModule\_V5 accepts account and requestId as separate privileged settlement parameters, reads request type/date/amount by requestId, applies the token effect to account and calls clearTransactionStorage(account, requestId) without an on-chain requirement that the request belongs to that account. Only an administrator can call the settlement path. Public evidence did not reveal whether the proprietary builder derives both values from one trusted record or permits independent lower-trust input. The code shape is established; ordinary-actor reachability and production misbinding are not. [E01-E02; L02; S05]

## 4.5 Authorization lifecycle and allowances

Allowances remain in standard ERC-20 storage when AuthorizationModule\_V2 changes shareholder or freeze roles. No public issuer policy states that deauthorization, offboarding, recovery or later reauthorization of the same address promises a clean allowance state, and no privacy-safe snapshot of address reuse and outstanding allowances was available. Persistence is established, but whether later allowance revival violates an intended security invariant is not. [E01-E02; O02; S04]

# 5 Recorded Validation

| Validation record                       | Recorded result and limit                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Proxy and implementation resolution     | Official Ethereum and BNB core proxies were resolved to the recorded implementations. Ethereum Fund Token, Authorization and Transfer Agent implementations had Sourcify source matches with creation and runtime matches recorded; the corresponding BNB implementations had Sourcify exact matches. Both Transactional implementations remained source/build unverified. |
| Transactional runtime comparison        | Executable bodies matched across chains after normalizing self constants and metadata; this is runtime similarity, not an exact source/build attestation.                                                                                                                                                                                                                  |
| Self-service negative calls             | Six ordinary-caller request calls reverted with SELF_SERVICE_NOT_ENABLED at the two fixed blocks.                                                                                                                                                                                                                                                                          |
| WRITE_ACCESS_TOKEN enumeration          | Every fixed-block member was enumerated and resolved to a Transfer Agent, constrained SwapPool or weighted multisig; no ordinary arbitrary-call path was found.                                                                                                                                                                                                            |
| Multisig negative and historical checks | Ordinary and unsigned-submitter calls reverted; one production signed execution corroborated the positive threshold path. Cryptography and key custody were not independently audited.                                                                                                                                                                                     |
| Private settlement                      | No production builder source, privacy-safe argument-correlation trace or end-to-end mismatched-ID validation was available.                                                                                                                                                                                                                                                |

## 6 Findings and Control Observations

### Zero confirmed vulnerabilities

No reportable implementation vulnerability was confirmed in the assessed public-contract scope. O01-O02 are control observations and do not resolve the Transactional and private-settlement limitations listed in Section 8.

### O01 — Token-writing and upgrade authority remains a material privileged dependency

| Field               | Assessment                                                                                 |
|---------------------|--------------------------------------------------------------------------------------------|
| Classification      | Control observation - applicable at snapshot; no vulnerability severity assigned           |
| Affected components | Transfer Agent modules, Ethereum SwapPools and weighted multisig; BNB Transfer Agent       |
| Condition           | Compromise, misuse or faulty configuration of authorized module, owner or signer controls  |
| Status              | No ordinary-caller escalation found; organizational key and approval controls not assessed |

WRITE\_ACCESS\_TOKEN permits material token-wide state changes. The live role graph limited those powers to identified contracts and a thresholded multisig, and the examined contract holders did not expose generic lower-trust execution. The security result therefore depends on continuing role integrity, holder implementation identity and signer custody. [E02-E03]

**Recommendation:** Franklin Templeton should maintain a signed inventory of every token-writing role holder, implementation and owner; require independent approval for upgrades and material token changes; and monitor role, threshold, submitter, pair-policy and implementation changes against the report snapshot.

### O02 — Allowances persist across authorization-state changes without a published lifecycle rule

| Field              | Assessment                                                                                                |
|--------------------|-----------------------------------------------------------------------------------------------------------|
| Classification     | Control observation - policy-dependent; no vulnerability severity assigned                                |
| Affected component | Fund Token allowances and AuthorizationModule_V2 shareholder lifecycle                                    |
| Precondition       | An address is deauthorized and later reauthorized or reused while a historical allowance remains          |
| Status             | Technical persistence established; intended clean-slate invariant and production exposure not established |

Deauthorization and freeze-state changes do not clear ERC-20 allowances. The public evidence does not state whether the same address may later represent a clean-slate re-onboarded identity or whether operators treat historical allowance state as continuing authority. The report therefore neither labels revival a vulnerability nor assumes it is safe. [E01-E02]

**Recommendation:** Franklin Templeton should publish and enforce an authoritative address-offboarding and re-onboarding policy. If reauthorization is intended to create a clean state, the operator should revoke or invalidate outstanding allowances before funding or reactivating the address and retain auditable reconciliation evidence.

## 7 RWA Linkage and Public Verifiability

Public issuer records identify iBENJI as the token of Franklin OnChain Institutional Liquidity Fund Ltd., and the official contract catalogue binds the assessed Ethereum and BNB deployments to the product. SEC Form D and the BVI Financial Services Commission register support the existence of the private fund and offering. [E05-E06; S01; S06-S07]

Public evidence does not include the offering memorandum, detailed token-to-share rights, NAV methodology, portfolio records, audited financial statements, redemption terms, legal shareholder register, custody attestation or a signed two-chain conservation statement. Ethereum and BNB balances therefore cannot independently prove legal ownership, fund assets, settlement completion or continuous supply reconciliation. The public RWA linkage is materially weaker than the deployment identity evidence.

## 8 Limitations and Conclusion

| ID  | Limitation                                                                                                       | Effect on conclusions                                                                                                                                   |
|-----|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| L01 | Both live Transactional implementations lack exact verified source/build correspondence                          | The report cannot prove all cancellation, clearing, unlisting, membership-deletion, request/account and exactly-once state transitions at source level. |
| L02 | Production CX settlement builder and account/requestId derivation are private                                    | The report cannot establish or exclude lower-trust miscomposition of the separately accepted privileged settlement parameters.                          |
| L03 | No authoritative allowance offboarding/re-onboarding policy or exposure snapshot                                 | Historical allowance persistence cannot be classified as either an intended continuing authorization or a violated clean-slate invariant.               |
| L04 | Weighted multisig source/cryptography and organizational key controls were not independently audited             | Observed thresholds and negative calls support current access control but not full signer-custody or cryptographic assurance.                           |
| L05 | Private product, legal-register, NAV, custody, portfolio, reconciliation and cash-settlement records unavailable | No legal-title, reserve, solvency, NAV, redemption or continuous two-chain conservation opinion is provided.                                            |

### Qualified conclusion

No reportable vulnerability was confirmed in the examined public deployments and recorded validation. The conclusion does not cover the exact active Transactional source semantics, private CX record composition or end-to-end legal and cash settlement. Any module upgrade, role-holder or multisig change, activation of self-service, address-lifecycle policy change, or new settlement builder changes the applicability of this opinion.

# A 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 | iBENJI public deployment and control assessment                   |
| E02 | iBENJI assessment conclusions and issue classification            |
| E03 | iBENJI independent role-holder and runtime evidence               |
| E04 | iBENJI official deployment registry snapshot                      |
| E05 | Tokenized-treasury RWA anchor and public-verifiability assessment |
| E06 | Portfolio-wide assessment basis and limitations                   |
| E07 | iBENJI weighted multisig production-configuration assessment      |
| E08 | iBENJI Transactional request-guard assessment                     |

## Primary public sources

**S01** | Franklin Templeton BENJI and iBENJI contracts catalogue

Primary issuer deployment inventory retained through the technical evidence cutoff.

**S02** | Franklin Templeton Benji platform overview

Primary issuer description of the proprietary platform and transfer-agent ownership record.

**S03** | Franklin Templeton suitability framework

Primary issuer context for whitelisting, multisig capability and administrative balance control.

**S04** | Benji API wallet creation documentation

Public wallet-lifecycle interface evidence; it does not define allowance cleanup or address-reuse policy.

**S05** | Benji API deposit documentation

Public application interface evidence; it does not disclose the production CX settlement argument builder.

**S06** | Franklin OnChain Institutional Liquidity Fund SEC Form D

Primary offering and legal-entity evidence retained for RWA linkage; not a token-to-register or asset attestation.

**S07** | BVI FSC register entry for Franklin OnChain Institutional Liquidity Fund Ltd.

Primary regulatory-register evidence for the fund entity; not an audit of token rights, assets or settlement.

## Scope attachment

**ibenji-scope-manifest-en.json**

SHA-256: ad43b8a8562e65d39247a6c4dfa754a7beac929e96cd7149a15819cff751bbd6