

BENJI

Multi-Chain Public-Contract Security Assessment

Franklin OnChain U.S. Government Money Fund
Public-evidence assessment with a conditional Aptos control-gap candidate

REPORT	B3-BENJI-2026-001
ISSUED	1 October 2026
BASELINE	Evidence observed through 30 September 2026; chain-specific points are listed in scope
AUTHOR	bench3.ai

Contents

1 Executive Summary 3

2 Scope and Assessment Basis 4

3 System and Threat Model 5

4 Technical Assessment 5

5 Recorded Validation 6

6 Findings and Control Observations 7

7 RWA Linkage and Public Verifiability 8

8 Limitations and Conclusion 9

A Evidence and Source Index 9

Assessment of identified public deployments, retained source-review records, fixed-state observations and recorded validation.
Private FTIS services and legal-register operations were outside the assessed implementation boundary.

1 Executive Summary

bench3.ai assessed the identified BENJI public execution surfaces across Ethereum, Polygon, Arbitrum, Avalanche, Base, Stellar, Solana and Aptos. The work addressed deployed identity, authorization and transfer restrictions, privileged issuance and settlement, cross-network request handling, non-EVM control configuration, and the public relationship between token balances and the Franklin OnChain U.S. Government Money Fund. [E01-E07]

Assessment conclusion

No reportable vulnerability was confirmed in the examined public-production scope. This is not a clean conclusion for Aptos: C01 remains an unconfirmed conditional candidate because the public record does not establish who controls the sole funded holder key. If a funded, unfrozen holder is independently controlled outside issuer custody, the validated vanilla-transfer path would bypass the custom shareholder registry. C01 is excluded from the confirmed-vulnerability total.

Classification	Recorded result
Confirmed vulnerabilities	Critical 0 High 0 Medium 0 Low 0
Conditional candidates	1; C01 on Aptos, verification pending and excluded from confirmed totals
Control observations	2; privileged Solana upgrade authority and Stellar signer concentration

Material qualification

The private FTIS production worker, durable replay and finality store, post-scheduling freeze policy and reconciliation process were not available. Solana source/build correspondence is incomplete, and no authenticated end-to-end cross-network transfer was performed. These gaps constrain the opinion to the public components and recorded state described below. [E01-E04]

2 Scope and Assessment Basis

2.1 Assessment identity

Parameter	Assessment basis
Assessment type	Multi-chain public-contract and public-evidence assessment; not a full operational, legal or financial audit
Evidence cutoff	Technical production observations through 29 September 2026; RWA linkage evidence through 30 September 2026
Networks	Ethereum, Polygon, Arbitrum, Avalanche, Base, Stellar, Solana and Aptos
Methods	Retained source review, deployment and implementation resolution, fixed-block/ledger/slot read-only observations, event-history analysis, archived negative calls and recorded bounded local/fixed-state validation

2.2 Deployment inventory

Network	Primary identifier	Recorded identity
Ethereum	Fund Token 0x3DDc84940Ab509C11B20B76B466933f40b750dc9	V6 implementation 0x20ca56f1215c3376b25bba1f2f9d3701c5def4c5 at block 26,077,255
Polygon	Fund Token 0x408A634B8a8f0dE729B48574a3a7Ec3fE820B00A	V5 implementation 0xc1df95cf7f96f020f511f2f03fbf6cc18f8464b2 at block 94,606,044
Arbitrum	Fund Token 0xB9e4765BCE2609bC1949592059B17 Ea72fEe6C6A	V5 implementation 0x956a399818c7cbabbd0b868a60f61ec9027136cd at block 509,766,342
Avalanche	Fund Token 0xE08b4c1005603427420e64252a8b120cacE4D122	V5 implementation 0x5c118e6a0bd2de0af66655806e3001727c13d105 at block 96,335,661
Base	Fund Token 0x60CfC2b186a4CF647486e42c42B11c C6D571d1E4	V5 implementation 0xab12adb95bbb71007669cde208a0b1f89d1a101 at block 51,912,448
Stellar	BENJI:GBHNGLLIE3KWGKCHIKMHJ5HVZHYIK7W TBE4QF5PLAKL4CJGSEU7HZIW5	Classic asset; ledger 64,667,065, hash 4d113d8dc8c a0c153ec319e21c8cceaab7968d87d0d3612994884d abb785bae9
Solana	Mint 5Tu84fKBpe9vfXeotjvfvWdWbAjj3hqsExvuHgFq FxA1	Token-2022 mint plus MultiSig, MultiChain and transfer-hook programs at finalized slot 451,404,746
Aptos	Metadata 0x7b5e9cac3433e9202f28527f707c89e1e4 7b19de2c33e4db9521a63ad219b739	Primary Fungible Asset with FTFunds and FTSecurity packages at ledger version 7,400,640,820

The attached scope manifest inventories the exact token entrypoints and supporting components material to the reviewed paths, with per-component identity and assurance limits. Listing identifies the assessed basis; it does not imply equal review depth, full test coverage, legal-title assurance or continuous cross-network conservation. [E03; E05-E07; S01]

2.3 Exclusions

Excluded were the private FTIS worker and book-entry database, authentication and KYC systems, durable cross-network message store, finality decisions, payment rails, fund accounting, legal shareholder register, underlying portfolio and custody records, organization-level key management, and end-to-end transaction operations. Production interaction was read-only.

3 System and Threat Model

BENJI represents registered fund shares across multiple ledgers. On EVM networks, upgradeable Fund Token, Authorization, Transactional and Transfer Agent modules separate holder eligibility, request creation and privileged settlement. Stellar uses a protocol-native classic asset; Solana uses Token-2022 plus issuer programs; Aptos uses a primary Fungible Asset plus custom fund and access-control packages. Cross-network movement depends on private FTIS records and privileged local execution rather than a reviewed public bridge protocol. [E01; E03]

Actor or layer	Relevant capability	Security boundary
Ordinary or approved holder	Hold and transfer through network-specific permitted paths	Must not acquire privileged mint, settlement, freeze or upgrade authority
Issuer and transfer-agent controllers	Authorize holders, mint/burn, freeze, correct balances and settle requests	Authorized power is a trust dependency; key custody and operating approvals were not assessed
FTIS private services	Bind application records to chain accounts, domains, finality and replay state	Private implementation and end-to-end reconciliation were outside scope
Fund and legal records	Determine authoritative registered ownership, NAV and settlement completion	Public token balances are evidence of units, not a standalone legal-register or reserve attestation

4 Technical Assessment

4.1 EVM authorization and deferred settlement

The five EVM token, Transactional and Transfer Agent deployments were resolved to the recorded implementations and active versions. At the observation points, self-service was disabled, pending-account counts were zero and reported token price was 1e18. Ordinary settlement calls were rejected at the administrator boundary. Recorded assessment evidence did not establish the four examined cross-network and deferred-settlement conditions as current ordinary-attacker vulnerabilities: the public application layer binds transfer records to a source wallet or holding, product, recipient address and quantity, but does not disclose a destination-network field or the opaque signing payload; no public actor-controlled route to privileged settlement arguments was established; and no EVM CXFER settlement was found in the indexed history. [E01-E02; S02-S04]

Those dispositions do not establish the private worker as correct. The final mapping from application transfer ID to on-chain account/requestId, durable domain/replay key, finality policy and post-scheduling freeze behavior remains outside the assessed implementation boundary and is retained as L01.

4.2 Aptos transfer enforcement

At ledger version 7,400,640,820, BENJI had no DispatchFunctionStore and was not marked untransferable. Aptos primary_fungible_store::transfer therefore derives or creates primary stores, verifies source ownership and freeze state, and transfers without consulting FTFunds.ManagedShareHolders. The sole funded holder owned the entire observed supply and its store was unfrozen. The account had no holder-signed history, no APT and sequence number zero; its creation and observed balance movements were issuer-associated. This supports an issuer-custody inference but does not prove key control. [E03-E04; S07]

Accordingly, the transfer mechanics are established while ordinary-holder reachability is not. C01 remains conditional rather than confirmed. Missing independent holder-key evidence cannot support either promotion or a clean conclusion.

4.3 Solana and Stellar control surfaces

Solana state recorded a Token-2022 mint, nine shareholders, zero pending transactions and active privileged mint, freeze and permanent-delegate controls. The MultiSig program and on-chain configuration were identified, but all three application programs shared direct upgrade authority AJyEpT8V17VniFmVhrUvegQJXy5g3qcRnqRe3joesXeJ outside the custom multisig. Public source/build attestation was incomplete: the MultiChain IDL omitted a successful production instruction and the transfer hook had no recovered canonical IDL. [E03; O01]

The Stellar classic asset used protocol-native trustline authorization and clawback. The issuer had thresholds 2/2/6, a zero-weight master key, ten weight-3 signers and four weight-1 signers; one weight-3 signer could satisfy low or medium operations. No ordinary route to signer authority was identified. [E03; O02]

5 Recorded Validation

Validation record	Result and evidentiary meaning
EVM fixed-state resolution	Five token/module stacks were resolved to implementations and versions; read-only calls recorded self-service false, zero pending accounts and price 1e18. This is point-in-time configuration evidence.
EVM security-condition assessment	Four examined cross-network and deferred-settlement conditions were not established as current ordinary-attacker vulnerabilities. Private worker correctness and future non-unit-price activation were not proved.
Aptos independent validation	Exact fixed framework/package sources and state established the vanilla-transfer path; public custody evidence did not establish an independently controlled holder.
Solana and Stellar observation	Control configuration, representative transactions and runtime identities were recorded read-only; incomplete Solana source/IDL correspondence constrains code-level assurance.
Production interaction	No transaction was signed or broadcast and no authenticated cross-network transfer was performed.

6 Findings and Control Observations

Zero confirmed vulnerabilities

No reportable implementation vulnerability was confirmed in the assessed public-production scope. C01 is an unconfirmed candidate and O01-O02 are control observations; none is included in the confirmed-vulnerability total.

C01 — Aptos vanilla transfer bypasses the custom shareholder registry

Field	Assessment
Classification	Unconfirmed candidate - verification pending; severity not assigned
Affected component	Aptos BENJI primary Fungible Asset at ledger version 7,400,640,820
Condition	A funded, unfrozen BENJI holder key is independently controlled by an investor or custodian outside issuer custody
Recorded conditional impact	Bypass of the custom recipient authorization and shareholder-accounting workflow; independent validation assessed the condition as potentially Medium if reachable
Status	Mechanics validated; ordinary-holder reachability not confirmed

The public framework transfer can move the signer's own BENJI to an address absent from ManagedShareHolders because the asset has no dispatch hook. It cannot steal another holder's balance, bypass a frozen source or mint supply. The decisive missing fact is control of the funded holder authentication key. Public transaction history is consistent with issuer custody but cannot prove it. [E03-E04]

Recommendation: Franklin Templeton should provide a dated custody attestation for every funded Aptos holder and confirm whether externally controlled wallets may hold BENJI. Before any external distribution, the issuer should enforce source and destination eligibility through dispatch hooks or make the asset untransferable outside the intended settlement path.

001 — Solana program upgrades depend on a direct authority outside the application multisig

Field	Assessment
Classification	Control observation - applicable at snapshot; no vulnerability severity assigned
Affected components	BENJI MultiSig, MultiChain and transfer-hook ProgramData accounts
Condition	Compromise or misuse of direct upgrade authority AJyEpT8V17VniFmVhrUvegQJXy5g3qcRnqRe3joesXeJ
Status	No ordinary-attacker route established; custody controls not evidenced

All three reviewed Solana programs were upgradeable by the same system account rather than the configured multisig authority PDA. An authorized upgrade can replace execution logic and therefore sits above the application-level signer thresholds. [E03]

Recommendation: Franklin Templeton should place program upgrades behind an independently controlled multisig with an appropriate threshold and monitored change process, or document equivalent institutional custody, approval and alerting controls for the current authority.

002 — Stellar low and medium operations can be authorized by one weight-3 signer

Field	Assessment
Classification	Control observation - applicable at snapshot; no vulnerability severity assigned
Affected component	BENJI Stellar issuer account
Configuration	Thresholds 2/2/6; ten weight-3 signers and four weight-1 signers; master key weight zero
Status	Authorized configuration; signer custody and off-chain approvals not assessed

A single weight-3 signer can satisfy low or medium thresholds. This concentrates operational authority over functions governed at those levels, while high-threshold actions still require aggregate weight six. [E03]

Recommendation: Franklin Templeton should confirm that mint, clawback, trustline authorization and freeze operations receive independent approval at the effective transaction layer, and should raise on-chain thresholds where single-key execution is not intended.

7 RWA Linkage and Public Verifiability

BENJI represents registered shares of the Franklin OnChain U.S. Government Money Fund rather than a warehouse receipt for a particular Treasury security. The prospectus describes a target \$1.00 share value, blockchain-integrated recordkeeping and transfer-agent-controlled movement across networks. Public SEC filings and audited financial reporting provide fund-level portfolio, net-asset and share evidence. [E06; S03; S05-S06]

The eight official supplies were summed only across chain-specific, non-atomic observation points. Private FTIS shareholder-register, same-cutoff legal-share, paired burn/mint and real-time custody records were unavailable; the aggregate is not a reserve attestation, legal opinion or proof of cash settlement.

8 Limitations and Conclusion

ID	Limitation	Effect on conclusions
L01	Private FTIS worker, replay/finality store and post-scheduling freeze policy unavailable	Public evidence cannot establish end-to-end account/request binding, domain uniqueness, finality, replay or correction behavior.
L02	Solana source, complete IDLs and reproducible build attestations incomplete	Observed runtime/configuration conclusions do not amount to full source-level assurance for the application programs.
L03	Aptos funded-holder key controller not independently evidenced	C01 cannot be confirmed or safely dismissed; the affected Aptos area does not receive a clean conclusion.
L04	No authenticated end-to-end production or staging cross-network transfer	The assessment does not validate the complete private-to-public settlement lifecycle.
L05	Private legal register, same-cutoff reconciliation, custody and portfolio records unavailable	No legal-title, reserve, solvency, NAV or continuous multi-chain conservation opinion is provided.

Qualified conclusion

No reportable vulnerability was confirmed in the examined public deployments and recorded validation. C01 remains visible outside confirmed totals, and the result must not be read as evidence that Aptos holder eligibility, private FTIS settlement or full fund operations are free of security defects. Any deployment upgrade, external Aptos wallet distribution, material authority change or activation of a new cross-network path 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	BENJI public deployment and control assessment
E02	BENJI assessment conclusions and issue classification
E03	BENJI non-EVM public-production review
E04	BENJI Aptos independent validation
E05	BENJI official deployment registry snapshot
E06	Tokenized-treasury RWA anchor and public-verifiability assessment
E07	Portfolio-wide assessment basis and limitations

Primary public sources

S01 | Franklin Templeton BENJI contracts catalogue
Primary issuer deployment inventory retained in the evidence; observed through 29 September 2026.

S02 | BENJI Solidity contracts, UAT deployment-aligned branch
Issuer repository commit recorded as aligned with active V6/V4/V5 deployments.

S03 | Franklin OnChain U.S. Government Money Fund prospectus
Primary product and registered-share context retained in the RWA workpaper.

S04 | SEC no-action response concerning Franklin blockchain transfer-agent records
Primary regulatory context for private book-entry linkage and administrative correction powers; dated 12 August 2026.

S05 | Franklin OnChain U.S. Government Money Fund 2026 N-CSR
Fund-level audited financial evidence retained for RWA linkage; not a same-cutoff token reconciliation.

S06 | Franklin OnChain U.S. Government Money Fund August 2026 N-MFP3
Fund-level portfolio and share reporting retained for RWA linkage; reporting date differs from chain snapshots.

S07 | Aptos primary fungible store source
Readable framework reference used alongside fixed PackageRegistry digest, bytecode, ABI and resources; the moving branch was not treated as the fixed deployment identity.

Scope attachment

benji-scope-manifest-en.json

SHA-256: ab869351a18eebd4402d7c9b7a433f2004dbc641489f4c7104b083a66ba82532