

April 29, 2026

Office of the Comptroller of the Currency
Chief Counsel's Office – Comment Processing
400 7th Street SW
Suite 1E-216
Washington, DC 20219

Re: Docket ID OCC-2025-0372
RIN 1557-AF41

Implementing the Guiding and Establishing National Innovation for U.S. Stablecoins Act for the Issuance of Stablecoins by Entities Subject to the Jurisdiction of the Office of the Comptroller of the Currency

Technical Comment on Distributed Infrastructure Supporting Payment Stablecoins

To the Office of the Comptroller of the Currency:

This submission provides technical observations regarding the operational suitability of the distributed transaction processing environments that may support the issuance, administration, transfer, and settlement of payment stablecoins under the proposed rule. It does not address the policy merits of payment stablecoins in the abstract. It addresses a narrower supervisory question: whether the transaction processing environment supporting a payment stablecoin should itself be subject to an evidentiary review before approval or waiver is granted.

The data-based observations in this submission rely on publicly available performance datasets and architectural disclosures referenced in Appendix A.

EXECUTIVE SUMMARY

The proposed rule appropriately focuses on issuer governance, reserve management, redemption obligations, operational controls, and compliance requirements. Those are necessary components of prudential supervision. The proposal, however, does not expressly require an evidentiary record demonstrating that the distributed transaction processing environment supporting issuance and settlement is operationally suitable for regulated financial activity.

That supervisory gap matters because a payment stablecoin does not merely move across a transaction processing environment. Once issued, **it is instantiated within** that environment. It therefore inherits that environment's ordering logic, confirmation semantics, governance structure, operational capacity, attack surfaces, failure characteristics and recovery constraints as part of its own operational risk profile.

Public data and architectural disclosures indicate that existing blockchain-based transaction processing environments vary materially in sustained throughput, transaction success behavior, sequencing design, governance concentration, and settlement timing. Most environments also rely on probabilistic confirmation models, statistical finality, discretionary sequencing layers, or challenge-period structures that raise additional questions regarding determinism, operational resilience, and settlement exposure.

Accordingly, the supervisory question should not end with whether the issuer is well governed. It should also include whether the transaction processing environment on which the instrument is issued and maintained is operationally suitable to support regulated payment activity.

For that reason, the OCC should require applicants seeking approval or waivers under the proposed rule to provide a documented evidentiary record addressing the transaction environment supporting issuance and settlement. At a minimum, that record should address transaction determinism, sustained operational capacity, transaction success behavior, governance and control structures, recovery procedures, sequencing dependencies, and material third-party operational relationships.

INTRODUCTION

This submission addresses the proposed rule implementing supervisory requirements for payment stablecoin issuers under the GENIUS Act.

For purposes of this submission, the term distributed transaction processing environment refers to the network, sequencing, validation, settlement, governance, and network recovery mechanisms on which a payment stablecoin is issued, administered, and transferred.

The proposal establishes supervisory expectations for governance, reserve management, redemption obligations, operational controls, and compliance requirements applicable to payment stablecoin issuers. Those elements are appropriate components of strong prudential supervision. However, issuer-level controls and reports do not eliminate infrastructure risk where the instrument depends on an external transaction processing environment for issuance, administration, transfer, ordering, and settlement.

Once a payment stablecoin is created on a distributed transaction processing environment, it does not simply traverse that environment as if the network were a neutral transport layer. The stablecoin exists within that distributed database environment and remains subject to its operational characteristics for as long as the instrument is issued, administered, and transferred in that transaction processing environment.

As a result, the reliability, accessibility, control, and recoverability of the instrument are influenced not only by issuer conduct, but also by the behavior and administration of the transaction environment itself. If that environment experiences outages, governance intervention, transaction reordering, degraded capacity, or compromised recovery processes, those characteristics can directly affect the stablecoin's operation.

THE CORE SUPERVISORY GAP

The proposed rule appropriately evaluates issuer-level controls. It does not require applicants to demonstrate that the distributed database transaction processing environment supporting issuance and settlement has been evaluated according to supervisory expectations ordinarily associated with operationally significant financial market infrastructure.

That omission is important because where a regulated issuer relies on an external transaction processing environment for core functions, that environment operates in substance as a critical operational dependency. Supervisory review therefore should not stop at reserve mechanics, redemption policies, and issuer administration and governance.

In this respect, the issue is not whether distributed infrastructure is novel. The issue is whether the specific transaction environment on which a regulated instrument is issued and maintained can demonstrate operational characteristics consistent with regulated payments and financial market infrastructures.

WHY THE TRANSACTION ENVIRONMENT BECOMES PART OF THE INSTRUMENT'S RISK PROFILE

A payment stablecoin inherits key features of the transaction processing environment in which it is instantiated. Those features include transaction ordering, confirmation and finality semantics, throughput constraints, governance control, key operational dependencies, and recovery behavior during failures or governance intervention.

Those features are not peripheral. They affect whether transactions are processed predictably, whether ordering can be manipulated or delayed, whether settlement can be treated as final in a defined way, whether operations can continue under systemic stress, and whether responsible parties and recovery procedures are identifiable and actionable if disruptions occur.

Accordingly, infrastructure review is not a separate policy preference layered on top of issuer supervision. It is part of understanding the operational risk profile of the instrument itself.

RELEVANCE TO EXISTING SUPERVISORY EXPECTATIONS

Operational resilience frameworks applicable to payment systems and financial market infrastructure generally require more than high-level design claims. They require demonstrable evidence regarding capacity, integrity, governance, recoverability, and critical third-party risk dependencies.

These supervisory frameworks emerged from a practical operational realization developed over decades of financial modernization. As markets moved from manual processes to electronic trading, real-time payments, and automated clearing and settlement, regulators recognized that small technical failures in automated systems could escalate rapidly into broader operational or systemic events. That experience drove a common supervisory emphasis on deterministic behavior for critical functions, preventive controls, resilience and capacity planning, clearly assigned governance and accountability, and evidence-based auditability. That same supervisory logic is directly relevant where payment stablecoins depend on distributed transaction processing environments for issuance and settlement. If a payment stablecoin depends on a distributed transaction processing environment for issuance and settlement, then the operational characteristics of that environment are relevant to the instrument's prudential risk profile whether or not the environment is organized as a traditional service provider.

Common supervisory concerns in this context include whether the environment has predictable transaction processing behavior, whether capacity is sufficient for expected activity, whether governance and intervention rights are identifiable, whether incident response and recovery procedures exist, and whether material operational intermediaries can affect ordering, inclusion, or finality.

EMPIRICAL OBSERVATIONS FROM PUBLIC DATA

Publicly available datasets and architectural disclosures indicate substantial variation across existing blockchain-based transaction processing environments. Observed differences include sustained production throughput, transaction failure or retry behavior, settlement timing, sequencing design, and governance concentration.

These observations do not establish that every distributed database transaction processing environment is unsuitable. They do, however, show that suitability should not be assumed. Where public datasets indicate meaningful transaction retry rates, discretionary ordering functions, delayed challenge periods, or unclear recovery governance, supervisory review should require those issues to be addressed directly rather than treated as outside the scope of issuer review.

Several environments also rely on probabilistic or economically conditioned confirmation models rather than deterministic processing with clearly defined finality. That may not preclude use in every case, but it does raise questions that should be examined expressly before a stablecoin issued on such an environment is treated as operationally suitable for regulated payment activity.

Transaction Integrity Concerns Arising from Maximal Extractable Value

Distributed transaction processing environments may also introduce economic ordering incentives that do not traditionally exist in regulated financial market infrastructure. In some blockchain architectures, validators or sequencing entities may have the technical ability to reorder, prioritize, delay, or exclude transactions in ways that generate economic advantage through mechanisms often described as maximal extractable value (MEV).

These dynamics introduce the possibility of transaction front-running, selective transaction inclusion, or censorship incentives within the transaction processing layer. Evaluating how such ordering incentives interact with fiduciary responsibilities, market integrity expectations, and supervisory oversight may therefore be relevant when assessing the suitability of distributed infrastructure for regulated financial instruments.

These considerations may also intersect with supervisory expectations regarding market integrity, fair access, and operational transparency that have historically informed oversight of regulated market infrastructure, including systems subject to Regulation Systems Compliance and Integrity.

LAYER-2 AND OTHER ADDITIONAL DEPENDENCIES

Certain architectures may introduce additional operational dependencies beyond those present in the underlying base environment. In some Layer-2 models, for example, transaction ordering and inclusion depend on identifiable sequencing processes operated by a single entity or a tightly controlled group.

Where a sequencing layer determines ordering or inclusion, supervisory review may require visibility into which parties control that function, how associated keys and governance rights are managed, what procedures exist if the sequencing function fails or is compromised, and whether users remain exposed to delayed or conditional settlement.

Some architectures also rely on challenge-period mechanisms before settlement is treated as final. Where those mechanisms exist, questions arise regarding liquidity support, economic exposure during the challenge window, and whether users are in fact receiving settlement characteristics consistent with regulated payment expectations.

RECOMMENDATION

Before granting approval or waivers under the proposed rule, the OCC should require applicants to provide a documented evidentiary record demonstrating the operational suitability of the distributed transaction processing environment supporting issuance, administration, transfer, and settlement of payment stablecoins.

At a minimum, that evidentiary record should address: (1) transaction determinism and confirmation semantics; (2) sustained operational capacity under realistic conditions; (3) transaction success behavior, including retry or failure characteristics; (4) governance and control structures, including system code maintenance, upgrade procedures, and testing of critical components, release management, and sequencing where relevant; (5) recovery procedures, incident response, and operational accountability; and (6) material third-party or operator dependencies capable of affecting ordering, availability, or settlement.

Requiring that evidentiary record would not displace issuer-focused supervision. It would close an observed material supervisory gap by ensuring that the infrastructure on which the instrument is issued and maintained is evaluated with the same operational discipline historically applied to other forms of financial market infrastructure.

BROADER APPLICABILITY

Although this comment is directed to payment stablecoins under the proposed rule, the same supervisory logic may apply more broadly as tokenized deposits, securities, collateral instruments, and other regulated financial products that are proposed for issuance on distributed database transaction processing environments.

Once any regulated financial instrument is instantiated within such an environment, the operational characteristics of that environment become relevant to the instrument's own risk profile. For that reason, the evidentiary approach described here may have relevance beyond payment stablecoins alone.

CONCLUSION

Stablecoins, tokenized assets, and real-time settlement rails are now being evaluated as production infrastructure by banks, payment networks, custodians, and regulators. Once a system performs these functions, by definition, it becomes part of financial market infrastructure.

This is the overlooked point: once a digital instrument is created on a blockchain, it does not simply move across that network. It lives within it. Yet the market still tends to treat blockchains as if they were merely transmission rails. They are not. A tokenized instrument instantiated on a distributed ledger inherits the network's rules, governance, attack surfaces, and failure characteristics as part of its own risk profile. Custody, MPC, Multisig, and Orchestration can sit above the ledger, but they do not eliminate risks embedded in the underlying distributed transaction processing network itself, including state-transition design, upgrade authority, finality assumptions, operational inconsistency, and susceptibility to interruption, attack, or coordinated compromise at the ledger layer.

The proposed rule appropriately addresses issuer-level supervision, but it does not yet expressly require a comparable evidentiary record regarding the operational suitability of the transaction processing environment on which the payment stablecoin is issued and maintained.

That record should be required before approval or waiver is granted. A payment stablecoin inherits core operational characteristics from the environment in which it is instantiated, and those characteristics are directly relevant to ordering, settlement behavior, resilience, governance, and recoverability.

Establishing a clear evidentiary framework for reviewing distributed transaction processing environments would help ensure that regulated stablecoin activity develops within an operational framework consistent with the standards historically applied to other forms of critical financial infrastructure.

We appreciate the opportunity to provide these observations and would be pleased to discuss additional technical observations if it would assist the supervisory evaluation process.

Respectfully submitted,

Mark Sulavka

TauriPay, a Public Benefit Corporation

APPENDIX A — PUBLIC DATA SOURCES REFERENCED

Transaction failure and retry datasets

<https://dune.com/queries/6645411/10476636>

<https://dune.com/queries/6717750/10572483>

Network throughput datasets

<https://chainspect.app/dashboard>

<https://rollup.wtf/>

Layer-2 architecture and settlement data

<https://l2beat.com/scaling/activity>

<https://l2beat.com/scaling/finality>

<https://l2beat.com/scaling/risk>

Nakamoto Coefficients

<https://nakafloow.io/>

APPENDIX B — The Five Supervisory Super-Categories

Distributed-Infrastructure Risk Concepts That Do Not Exist in Traditional Financial Market Infrastructure but Must Be Evaluated Under OCC Third-Party Risk, FFIEC Business Continuity, and PFMI / CPMI-IOSCO Standards

The supervisory blind spot is not at the custody, wallet, orchestration, access-control layer or datacenter SOC certification. It is at the state-transition layer itself. In traditional financial market infrastructure, settlement finality, operating rules, participant criteria, communication standards, and recovery procedures are expected to be clear, enforceable, testable, and operationally reliable. OCC third-party guidance likewise requires planning, due diligence, ongoing monitoring, contingency planning, and board-level oversight for critical activities, while FFIEC BCM focuses on the availability of critical financial services, resilience, third-party service providers, and exercises and tests. These frameworks already supply the right supervisory logic; what is missing is a precise taxonomy for blockchain-native failure modes. PFMI requires a clear and enforceable legal basis, clear and certain final settlement, comprehensive risk management, operational-risk controls, fair access criteria, and public disclosure of key procedures.

Existing supervisory frameworks already contain the correct governing principles. The gap is not the absence of risk-management law; it is the absence of a precise taxonomy for distributed-infrastructure risks that have no analogue in traditional financial market infrastructure. These include probabilistic processing, statistical rather than certain finality, operator-manipulable ordering, extractable ordering fees, ambiguous timestamp and forensic records, threshold-dependent failure behavior, opaque operator concentration, privileged key-based control, and insufficient evidence of resilience testing. Where a payment stablecoin or tokenized instrument is instantiated on such infrastructure, the instrument inherits these properties. Accordingly, these risks should be evaluated as core infrastructure risks under the OCC's third-party risk guidance, FFIEC business continuity expectations, and the PFMI/CPMI-IOSCO framework, rather than treated as issues remediable solely by custody, orchestration, or other upper-layer controls.

The five categories below are mutually exclusive over the distributed-infrastructure risk surface. Each maps cleanly to the existing OCC TPRM 2023, FFIEC BCM, and PFMI / CPMI-IOSCO clauses identified in the matrix. Each is the unit at which a supervisor can ask a single coherent question and receive a single coherent evidentiary record.

A. Determinism & Finality

Does the system produce a clear, irrevocable, and authoritatively timestamped settlement event?

Covers probabilistic vs deterministic finality, state consistency under partition or reorganization, and the authoritativeness of the timestamp / sequence record. Implicates **OCC TPRM 2023** diligence and ongoing monitoring for performance under stress, and **FFIEC BCM** integrity and recoverability of transaction state and **PFMI Principle 8** (clear and certain final settlement) and **Principle 1** (legal certainty). Where finality is probabilistic, the target probability and the monitoring mechanism should be documented; the gap between marketed and operational finality should be disclosed, not concealed.

B. Ordering Integrity & Inclusion

Is transaction ordering specified, enforceable, free of embedded conflicts of interest, and protected from selective exclusion?

Covers ordering authority and the ordering rule, ordering-based value extraction (MEV-class behaviors), and transaction inclusion guarantees against censorship, deprioritization, and queue manipulation. Implicates **OCC TPRM 2023** third-party review of incentives, governance, and subcontractors, and **FFIEC BCM** payment-systems continuity and third-party testing and **PFMI Principles 2, 3, 17, 18, 21, 23**. Where

ordering-based value extraction is technically possible, an empirical assessment of extractable value, including disclosure where extraction is bounded, should be required.

C. Concentration & Control Authority

Who can, in practice, change outcomes — through consensus participation, key authority, governance action, or persistent informal influence — and what is the threshold behavior?

Combines v5 §III (Control & Concentration) and §IV (Governance & Upgrade) into a single supervisory question because the spreadsheet, the comment letter, and the academic literature all treat consensus participation, sequencer keys, upgrade authority, and informal founder/early-operator influence as one control surface. Covers effective control concentration, decisive participation set, behavior at and past adversarial share, the safety-vs-liveness threshold relationship, static vs evolving fault tolerance, operator identity and affiliation transparency, governance transparency and accountability, privileged key authority, and persistence of informal authority. Implicates **PFMI Principles 1, 2, 3, 17, 18, 19, 23**, **DORA Article 11**, **OCC TPRM 2023** concentration-risk and management-escalation expectations, and **FFIEC BCM** interdependency analysis and governance/personnel resilience.

D. Continuity, Capacity & Recovery

Under stress and over time, does the system continue to operate within stated bounds, recover deterministically, and remain reconstructable?

Combines (Recovery and Continuity) and (Capacity and Performance Behavior) because capacity behavior under sustained or adversarial load is itself a continuity property — the supervisory test is whether the system degrades safely and recovers deterministically, not whether benchmarks were ever achieved under ideal conditions. Covers recovery semantics under stress, RTO/RPO specification and tested recovery, completeness and non-repudiation of records, execution-vs-access-layer divergence, throughput vs data availability, retention and replication control, point-in-time state reconstruction, sustained vs ideal-condition throughput, overload and degradation behavior, and retry semantics. Implicates **OCC TPRM 2023** contingency planning and transition planning, **FFIEC BCM** continuity, recovery, capacity planning, and stress-readiness sections and **PFMI Principles 1, 17, 22, 23**.

E. Evidence, Verification & Disclosure

Is the operational record built from independently reviewable evidence, or from assertion?

Combines v5 §VII (Testing and Verification), §VIII (Third-Party Dependencies), and §IX (Disclosure and Auditability). The unifying supervisory question is whether the applicant's filing rests on machine-checkable, independently re-runnable, contractually enforceable evidence — across the protocol specification, the production implementation, the dependency stack, and the public disclosure record. Covers state-transition specification, verified safety properties, liveness and fairness, adversarial action coverage, specification-to-implementation correspondence, capacity as temporal behavior, dependency inventory, contractual oversight, interoperability mechanisms, external data dependencies, substitutability, disclosure completeness, independent verification, and the evidence-of-testing standard. Implicates **OCC TPRM 2023** independent-review and audit expectations, **FFIEC BCM** exercises and **PFMI Principles 17, 18, 19, 22, 23**.

Master Matrix Distributed-Financial Market Infrastructure Risk

A. Determinism & Finality

#	Property	Failure Mode	Condition	Regulatory Implication	OCC TPRM	FFIEC BCM	PFMI	Illustrative Evidence Standard
A.1	Probabilistic vs deterministic finality	Settlement may be treated as final before irrevocability is established	Normal and stress	Finality may become a matter of confidence level rather than legal and operational certainty; gap between marketed and operational finality time may be material	Diligence and monitoring for performance under stress	Integrity and recoverability of transaction state	Principle 8; Principle 1	(1) formal definition of the finality event with conditions of irrevocability; (2) where finality is probabilistic, a documented confidence model with quantified bounds and a stated monitoring method; (3) measured finality latency under specified network and adversarial conditions; (4) disclosure of any gap between marketed and operational finality time
A.2	State consistency over time	Two participants may observe different valid states simultaneously	Partition, delay, fork	Ambiguity about the authoritative state for settlement and reporting	Ongoing monitoring; contingency planning	Data integrity, replication, reconciliation	Principles 1, 3, 17	(1) the state-consistency model under partition, delay, and fork conditions; (2) evidence — formal, exhaustive, or empirical — that the no-divergence property holds within stated bounds; (3) the procedure for resolving divergence when it occurs
A.3	Timestamp and sequence authoritativeness	No deterministic, authoritative event record	Forensic staging	Audit, reconstruction, control, and legal certainty are impaired where the authoritative sequence depends on a single operator's local view	Policy compliance, audit, safe operation	Incident handling and recovery depend on reliable records	Principles 1, 17, 22, 23	(1) the authoritative event-record structure and signing model; (2) the rule by which the authoritative sequence is determined; (3) evidence that authoritative sequencing does not depend on a single operator's local view; (4) procedures for forensic reconstruction

B. Ordering Integrity & Inclusion

#	Property	Failure Mode	Condition	Regulatory Implication	OCC TPRM	FFIEC BCM	PFMI	Illustrative Evidence Standard
B.1	Ordering authority and ordering rule	Designated participants may have discretion over the inclusion or sequence of transactions	Any time	Order determines outcome — priority, eligibility, price, fairness. Where an ordering authority exists, it is a control surface. Where ordering emerges from a structural rule, that rule must be specified	Third-party review of incentives, governance, subcontractors	Payment systems, continuity, third-party testing	Principles 2, 3, 17, 21, 23	(1) identify any designated ordering participant (leader, proposer, sequencer, block-builder); (2) where no such participant exists, specify the structural rule under which ordering emerges; (3) provide evidence — formal or empirical — that ordering is enforceable as specified; (4) provide evidence that ordering cannot be unilaterally altered by any participant
B.2	Ordering-based value extraction	Ordering participants may benefit economically from reordering, delay, insertion, or exclusion	Economic value at stake	Embedded conflict of interest within the settlement process; the magnitude and form of extractable rent are supervisory concerns	Incentive evaluation; subcontractor visibility	Intentional operational abuse	Principles 2, 23; MiFID II Article 27; SEC Rule 15c3-5; FINRA Rule 5320	(1) identify any economic incentive embedded in the ordering layer; (2) provide an empirical or structural assessment of extractable value, including disclosure where extraction is technically possible but bounded; (3) document what information is visible to ordering participants prior to ordering decisions
B.3	Transaction inclusion guarantees	Valid transactions may be delayed, censored, deprioritized, or dropped	Congestion, fee competition, selective inclusion	Availability includes timely execution, not merely uptime; selective filtering of transactions is a supervisory concern	Ongoing monitoring; escalation on performance deterioration	Payment systems, continuity, third-party testing	Principles 17, 18, 21, 23	(1) the inclusion rule and its enforcement mechanism; (2) evidence that inclusion cannot be selectively withheld by any participant without detection; (3) measured concentration thresholds for safety, liveness, and censorship attacks, including any asymmetry between them

C. Concentration & Control Authority

Combines Control and Concentration(and Governance and Upgrade Authority) into a single supervisory category. The grouping reflects the consensus question — who can, in practice, change outcomes — that consensus participation, key authority, governance action, and persistent informal influence all answer.

#	Property	Failure Mode	Condition	Regulatory Implication	OCC TPRM	FFIEC BCM	PFMI	Illustrative Evidence Standard
C.1	Effective control concentration	A small set of participants may control outcomes regardless of nominal participant count	Always	Practical control set may be smaller than apparent; concentration may not be visible without structural analysis	Concentration and subcontractor challenges; management escalation	Interdependency analysis; third-party resilience	Principles 2, 3, 17, 18, 19; DORA Article 11	(1) measured concentration across attack axes (safety, liveness, censorship); (2) a structural analysis distinguishing nominal participation from decisive participation; (3) affiliation mapping of operators; (4) identification of any participant whose participation is required for liveness or whose exclusion would break safety
C.2	Decisive participation set	Apparent decentralization may mask practical concentration	Live operations	Supervisors may evaluate the wrong control surface where the decisive set is smaller than the apparent set	Diligence tailored to actual activity	Interdependency analysis	Principles 3, 17, 18, 23	Demonstrate the size and composition of the decisive participation set per round of consensus; any sub-quorum, delegated voting, or rotating-committee arrangement should be disclosed
C.3	Behavior at and past adversarial share	The system may shift from safe operation to delay, censorship, inconsistent state, halt, or fork as adversarial share increases	Adversarial thresholds	A regulated institution may not know when the system degrades or into what failure mode; absence of documented threshold behavior is itself a material gap	Contingency planning; disruption scenarios; resilience; tests	Disruption scenarios, resilience, tests	Principle 17	(1) the threshold or thresholds at which behavior changes; (2) the behavior on either side of each threshold; (3) whether behavior above threshold is safe-halt or includes the possibility of incorrect commits; (4) the form of evidence supporting each documented threshold
C.4	Safety and liveness threshold relationship	Safety and liveness thresholds may be conflated or treated as a single cliff	Adversarial coordination above threshold	Financial infrastructure must support both correctness and continued execution; treating the two thresholds as identical may mask the failure-mode distinction	Contingency planning for loss of liveness even without loss of safety	Payment systems continuity; resilience and testing	Principle 17	(1) the safety threshold (above which incorrect commits become possible) and the liveness threshold (above which progress halts) as separately specified bounds; (2) evidence supporting each bound; (3) the operational consequence of crossing each threshold
C.5	Static vs evolving fault tolerance	A static fault budget may decay over time as detected adversaries continue to consume	Persistent adversary	Static fault tolerance may be lower in long-run operation than at a single point in time; evolving	Contingency and transition planning	Recovery from adversarial events	Principle 17	(1) state whether fault tolerance is static or evolves over operational time; (2) where evolving, document the detection and

		budget; an evolving model may detect and exclude adversaries		models alter the long-run guarantee but require evidence				exclusion mechanism; (3) where static, document the model for effective tolerance over a sustained adversarial engagement
C.6	Operator identity and affiliation transparency	The parties controlling nodes, keys, or emergency actions may not be fully knowable	Upgrade events, emergency actions, key rotation	Accountability cannot be verified where parties are not identified; due-diligence obligations require identified parties	Due diligence and subcontractor visibility	Governance, personnel, third-party providers, exercises	Principles 1, 2, 3, 23	(1) identification of all operators with privileged roles; (2) the participating operator set; (3) admission, removal, and rotation governance; (4) affiliation mapping covering direct and indirect relationships
C.7	Governance transparency and accountability	Decisions may be made via informal channels with undefined escalation	Protocol change events	Supervisory visibility is impaired where governance occurs outside documented channels	Oversight, accountability, documentation	Governance and personnel resilience	Principle 2	(1) a written governance charter; (2) amendment procedures, voting thresholds, and quorum requirements; (3) emergency powers and escalation paths; (4) documentation of any change-management gate
C.8	Privileged key authority	A small set of keyholders may pause, upgrade, alter, or redirect live operations	Any time	Privileged-key authority embedded in production infrastructure constitutes a live control plane and a supervisory control surface	Contract review, contingency planning, third-party controls	Change management, incident response	Principle 17	(1) the relationship between the upgrade path and the live commit path; (2) full disclosure of all privileged keyholders, key-rotation procedures, and multi-party authorization requirements; (3) evidence of separation between routine commit logic and upgrade authority where applicable
C.9	Persistence of informal authority	Historical privilege may entrench effective control beyond the formal governance structure	Persistent	Formal governance may not capture concentrations of informal influence	Management reporting	Resilience weakened where key roles depend on concentrated persons	Principle 2	Demonstrate that control analysis is structural (voting rule, key-holder mapping, participation rule), not reputational; any concentration of informal influence should be named, not assumed away

D. Continuity, Capacity & Recovery

Combines (Recovery and Continuity) and (Capacity and Performance Behavior). Capacity behavior under sustained or adversarial load is itself a continuity property; the supervisory test is whether the system degrades safely and recovers deterministically.

#	Property	Failure Mode	Condition	Regulatory Implication	OCC TPRM	FFIEC BCM	PFMI	Illustrative Evidence Standard
D.1	Recovery semantics under stress	The failure mode under stress may be ambiguous (halt, fork, reorganization, rollback, or inconsistent continuation)	Faults, partitions, mass exits	A supervisor cannot assess continuity where the failure mode under stress is ambiguous; a pre-defined deterministic recovery semantics is preferable to operator discretion	Contingency plans, transition planning, oversight	Continuity and recovery, DR, crisis management	Principle 17	(1) the deterministic failure-mode semantics under defined stress conditions; (2) the recovery procedure and the conditions under which it activates; (3) evidence that recovery does not produce a state inconsistent with prior commits
D.2	RTO / RPO specification and test	Recovery timeframes may not be documented, tested, or contractually owed	Disruption	Extended or undocumented recovery periods impair financial operations; absence of documented RTO/RPO is itself a material gap	Contingency planning and performance expectations	Recovery drills, defined RTO / RPO	Principle 17	(1) documented RTO and RPO with measurement methodology; (2) evidence of tested recovery procedures; (3) written runbooks for non-Byzantine failure modes (hardware, network partition, operator error); (4) contractually owed recovery commitments at the operator-agreement layer
D.3	Completeness and non-repudiation of records	Records may have gaps, discontinuities, lost transactions, or duplicate entries	Disruption, partition, split	Impairs audit, reconciliation, regulatory recordkeeping	Due diligence for audit and safe operation	Incident handling, recovery, exercises, tests	Principles 1, 17, 22, 23	(1) the signing model of authoritative records; (2) the replication model of authoritative records; (3) the non-repudiation assumption and its supporting evidence; (4) the verifiability of individual records against the authoritative record-stream
D.4	Execution layer vs access layer divergence	State observed by an institution via RPC, indexer, or API may not reflect system state	Any time	Visibility gap between system state and the state observable by a regulated institution may affect reporting and audit	Ongoing monitoring; fourth-party considerations	Availability; third-party testing	Principles 17, 22, 23	(1) whether the state visible at the access layer is reconcilable with the authoritative state; (2) the divergence-detection procedure and its frequency; (3) any reliance on third-party RPC, indexer, or API infrastructure for state visibility

D.5	Throughput vs data availability	Execution capacity may exceed data availability or indexing capacity, producing gaps in observable history	High load	Operational risk, audit limitation, delayed visibility for regulated institutions	Size actual (not nominal) evidence capacity	BCM capacity + data integrity	Principles 17, 22	(1) the data-availability capacity sized against execution capacity; (2) evidence that authoritative-record availability is maintained at peak execution rates; (3) any dependency on third-party infrastructure for authoritative record availability
D.6	Retention and replication control	Authoritative snapshots may not be standardized; replication assumptions may be unenforced	Long horizon	Authoritative-data location may be unclear; reliance on external providers may not be visible	Third-party inventory and oversight	Backup, replication, data integrity	Principles 17, 22	(1) the replication model for authoritative records; (2) a documented data-retention policy; (3) any single-provider dependency for authoritative historical record
D.7	State reconstruction (point-in-time)	Inability to reconstruct historical balances or verify sequences	Audit, dispute, regulatory reporting	Blocks the institution from meeting recordkeeping obligations	Evaluate dependency chain	Record availability, audit	Principles 1, 22	(1) the procedure by which any participant can reconstruct state at a specified historical point in time; (2) the data dependencies of that procedure; (3) the verifiability of the reconstructed state against the authoritative record
D.8	Sustained throughput vs ideal-condition throughput	Throughput claims may be benchmark-ideal; sustained performance under realistic conditions may be materially lower	Peak / stress	Settlement timing commitments may not hold; disclosure integrity is itself a regulatory concern	Operational resilience and performance monitoring	Capacity planning and stress readiness	Principle 17; DORA Article 11	(1) the analytical model used to derive advertised throughput; (2) the sustained throughput under realistic load conditions; (3) the explicit gap between advertised and sustained figures; (4) an explanation for any gap; (5) evidence that throughput scales predictably as the operating envelope expands
D.9	Overload and degradation behavior	Behavior under overload may be unpredictable	Overload	Inconsistent outcomes across participants under load are a supervisory concern	Ongoing monitoring; escalation	Queueing, backpressure, failure under overload	Principle 17	(1) the documented saturation bound and its derivation; (2) the behavior at and past saturation; (3) measured transaction-success rate under sustained peak load
D.10	Retry semantics	Completion may depend on persistence or retries rather than guaranteed processing	Congestion	Timing-material financial activity may not tolerate retry-shaped completion tails	Diligence tailored to activity	Continuity of critical financial services	Principle 17	(1) the consensus-layer outcome semantics (deterministic / retry / hybrid); (2) where retry semantics exist, the conditions under which they activate; (3) the supervisory rationale for any retry-based completion model

E. Evidence, Verification & Disclosure

Combines (Testing and Verification), (Third-Party Dependencies), and (Disclosure and Auditability). The unifying supervisory question is whether the filing rests on machine-checkable, independently re-runnable, contractually enforceable evidence.

#	Property	Failure Mode	Condition	Regulatory Implication	OCC TPRM	FFIEC BCM	PFMI	Illustrative Evidence Standard
E.1	State-transition specification	The initial state, next-state relation, admissible actions, and prohibited transitions may not be fully specified	Anywhere	A supervisor cannot reason about whether the system does what it claims without a complete specification	Due diligence for model validation	Scenario testing dependency	Principle 17	(1) a published state-transition specification (initial state, transition rule, liveness assumption); (2) evidence that the specification has been tested or proven against safety properties; (3) reproducibility of the verification artefacts
E.2	Safety properties (verified)	Invalid or conflicting states may be reachable; double-execution may not be excluded	Exhaustive exploration	Absence of regulator-grade evidence of correctness is itself a supervisory concern	Independent review and audit	Exhaustive validation	Principle 17	(1) the safety properties claimed; (2) the verification methodology used (formal proof, exhaustive model checking, adversarial trial, or combination); (3) evidence of the verification result, including any unfinished or unproven obligations
E.3	Liveness and fairness	The system may stall, exclude, or starve progress	Contention, adversarial fairness	Without an explicit liveness statement, no progress guarantee can be relied upon	Diligence for resilience under stress	Continuity of critical financial services	Principle 17	(1) the liveness property and the timing-assumption class under which it is claimed (asynchronous / partially synchronous / synchronous, including any "eventual delivery" qualifications); (2) evidence supporting the liveness claim; (3) statement of the foundational impossibility result (e.g., FLP) the design accommodates and how
E.4	Adversarial action coverage	Behavior under message loss, reordering, delay, partition, equivocation, censorship, key intervention, and recovery may not be modelled	Adversarial	Operational behavior under stress is unknown without adversarial trial evidence	Scenario testing evidence	BCM scenario testing	Principle 17	Evidence from one or more verification methods covering adversarial behavior, including formal proof, exhaustive state-space exploration, enumeration of adversarial placements, symbolic verification, and adversarial simulation. Methodology, scale, and reproducibility documented
E.5	Specification-to-implementation correspondence	The implementation may not faithfully refine the verified specification	Always	Verifying the specification is not equivalent to verifying the production code; absence of refinement evidence is a known industry gap	Independent testing and validation	Post-test actions	Principle 17	(1) the relationship between the verified specification and the production implementation; (2) any documented conformance mechanism; (3) honest acknowledgment where refinement evidence is incomplete

E.6	Capacity as temporal behavior	Capacity is not a single throughput number; it includes queue growth, backlog, latency under load, and queue-recovery behavior	Sustained peak and overload	Capacity is an action-level temporal property and should be evaluated as such	Performance monitoring	Capacity planning, stress readiness	Principle 17	(1) time-ordered measurements of queue growth, backlog, latency under load, and queue-recovery; (2) behavior characterization under both honest and adversarial load conditions
E.7	Dependency inventory	Hidden dependencies may not be inventoried (validators, sequencers, bridges, RPC providers, cloud, indexers, oracles)	Always	Third-party risk life-cycle cannot be executed on unknown parties	Full life-cycle third-party risk management	Interdependency analysis	Principles 17, 18, 19	(1) complete enumeration of every component in the commit path and at the access layer; (2) identification of any external party whose availability affects settlement; (3) separation of commit-layer dependencies from access-layer dependencies
E.8	Contractual oversight	SLAs, audit rights, remediation rights, ongoing monitoring, independent review, and incident reporting may not be in place	Always	Oversight and escalation may not be contractually enforceable	Contracts, SLAs, right to audit, remediation rights, ongoing monitoring, independent review, incident reporting	Third-party testing and exercises	Principles 2, 3, 17	Contractual arrangements with all commit-path dependencies, including SLAs, audit rights, remediation rights, ongoing monitoring obligations, independent review procedures, and incident reporting requirements. Absence of such contracts is a material gap regardless of protocol design
E.9	Interoperability mechanisms	Additional points of failure, inconsistencies, external governance dependencies	Cross-system flows	Cross-system mechanisms may amplify base-layer risks; in some implementations, interoperability mechanisms have been the site of material loss	Diligence for dependency chain	Continuity under correlated failures	Principles 17, 19	(1) whether the commit path depends on cross-system messaging; (2) where it does, full evaluation of the mechanism's governance, security model, and incident record; (3) where it does not, the boundary at which interoperability begins and the evaluation framework for that boundary layer
E.10	External data dependencies and incentive asymmetry	Where a transaction depends on external data, incentive structures may not align with the magnitude of the dependent value	External trigger	Where the cost of manipulation is less than the dependent value, manipulation is economically rational	Ongoing monitoring; sub-contractor visibility	Scenario testing for data failure	Principles 17, 23	(1) whether external data dependencies exist in the commit path; (2) where they exist, analysis of incentive alignment between provider penalty and dependent transaction value; (3) where they exist only at the application layer, the boundary between application and commit-layer guarantees
E.11	Substitutability	Dependencies may be embedded in design and not substitutable without re-instantiation	Exit, migration, failure of operator	Contingency planning may be constrained; regulatory exit strategy may not be achievable	Exit strategy, transition planning	Continuity when vendor fails	Principle 17	(1) documented exit criteria and migration procedures; (2) evidence that authoritative records are portable; (3) assessment of any lock-in risk arising from protocol-specific data formats or access methods
E.12	Disclosure completeness	Marketing claims may differ from operational behavior; ordering risks, governance control,	Always	Participants cannot understand the risks they assume; incomplete disclosure is	Documentation and transparency	Governance, interdependencies, disclosures	Principle 23	(1) documented threshold behavior; (2) measured concentration across attack axes; (3) throughput methodology including analytical model, sustained operational figure, and explicit gap; (4) verification

		recovery limits, and capacity limits may not be disclosed in standardized form		itself a supervisory deficiency				evidence; (5) a fully completed Appendix B response with no field unanswered without justification
E.13	Independent verification	Reliance may be on assertion rather than independently reviewable evidence	Always	Supervisors should not be required to rely on assertion; end-to-end independent verification is a supervisory expectation	Independent reviews, audits, testing	Exercises, tests, post-test actions	Principle 17	(1) independently re-runnable verification artefacts; (2) external independent confirmation of structural claims where available from non-commercial academic literature; (3) commissioning of an independent third-party review — absence is a material gap
E.14	Evidence-of-testing standard	"Widely used," "battle-tested," or operational throughput claims may be substituted for evidence	Always	Operational experience and market adoption are not adequate proxies for regulator-grade evidence	Diligence tailored to activity and risk	Exercises and tests	Principle 17	One or more independent verification methods covering safety, liveness, and adversarial behavior, with documented methodology, scale, and reproducibility. The disclosure posture: an incomplete or unavailable response to any question is itself a signal

Bridging Recommendation

Before granting approval or waivers under the proposed rule, the OCC should require applicants to provide a documented evidentiary record demonstrating the operational suitability of the distributed transaction processing environment supporting issuance, administration, transfer, and settlement of the payment stablecoin. At a minimum, that evidentiary record should address each of the five categories above: (A) transaction determinism and confirmation semantics; (B) ordering integrity and inclusion guarantees; (C) concentration and control authority, including consensus participation, governance, sequencing, key, and upgrade authority; (D) sustained operational capacity, recovery procedures, and continuity of authoritative records; and (E) independent verification, dependency oversight, and disclosure completeness, including material third-party or operator dependencies capable of affecting ordering, availability, or settlement. Requiring that record would not displace issuer-focused supervision; it would close a material supervisory gap by ensuring that the infrastructure on which the instrument is issued and maintained is evaluated with the same operational discipline historically applied to other forms of financially significant infrastructure.

APPENDIX C — Supervisory Infrastructure Evaluation Questions

The following questions illustrate operational due diligence considerations that may assist supervisors, financial institutions, and new entrants in evaluating distributed transaction infrastructure used to issue or process regulated financial instruments.

1. Operational Capacity (Production)

1.1 Sustained Production Capacity

- Reported sustained TPS in live production: _____
- Transaction scope included (check all that apply):
 - ☐ Signature validation ☐ State execution ☐ Balance checks ☐ Fee settlement
- Evidence / references (dates, environment): _____

1.2 Peak Production Capacity

- Highest observed production TPS: _____
- Conditions under which achieved: _____

1.3 Capacity Saturation Behavior

- Behavior at or above capacity (check all that apply):
 - ☐ Queue delay ☐ Increased latency ☐ Transaction drop ☐ Re-attempt required
- Impact on operational consistency: ☐ None disclosed ☐ Moderate ☐ Severe
- Notes: _____

1.4 Public Capacity Claims vs. Observed Production Capacity

- Advertised capacity (website, conferences, documentation): _____ TPS
- Observed sustained production throughput: _____ TPS
- Material discrepancy present? ☐ Yes ☐ No ☐ Not disclosed
- Explanation (if applicable): _____

2. Operational Consistency

2.1 Definition of 'Properly Submitted Transaction'

- Definition: _____

2.2 Historical Consistency Rate

- Success rate under normal load: _____ %
- Success rate under peak / stress conditions: _____ %

2.3 Re-attempts and Reordering

- Are re-attempts required? ☐ Yes ☐ No ☐ Not disclosed
- Is transaction ordering mutable after submission? ☐ Yes ☐ No ☐ Not disclosed
- Responsibility for recovery: ☐ User ☐ Application ☐ Network ☐ Not specified

3. Execution Integrity Risks

3.1 Maximal Extractable Value (MEV) Exposure

- MEV permitted or tolerated? ☐ Yes ☐ No ☐ Unclear
- Conditions enabling MEV: _____

3.2 Censorship / Queue Control

- Ability to manually or systematically delay or deprioritize transactions? ☐ Yes ☐ No
- Ability to jump queue or reorder transactions? ☐ Yes ☐ No
- Controls or mitigations disclosed: _____

3.3 Front-Running / Sandwiching

- Technically possible? ☐ Yes ☐ No
- Observed frequency (if available): _____

4. Benchmarking and Projections

4.1 Sharding Arithmetic Used? ☐ Yes ☐ No ☐ Not disclosed

- Details: _____

4.2 Gas Budget Arithmetic Used? ☐ Yes ☐ No ☐ Not disclosed

4.3 Partial / Message-Only Metrics Used (check all that apply):

- ☐ Message broadcast only
- ☐ Ordering without signature validation
- ☐ RPC counts
- ☐ Internal protocol messages
- ☐ Other: _____

4.4 Projection Disclosure

- Which metrics are measured vs projected: _____

5. Confirmation Semantics

5.1 Definition of Confirmation

- ☐ Optimistic ☐ Probabilistic ☐ Final / Irreversible ☐ Not clearly defined

5.2 Latency Claims

- Marketed confirmation time: _____
- Represents: ☐ Start of processing ☐ Ordering only ☐ Final settlement

5.3 Correlation to Re-attempts

- Are confirmations correlated with retries or reordering? ☐ Yes ☐ No ☐ Not disclosed

6. Governance and Sequencer Control

- Entity responsible for transaction ordering: _____
- Number of sequencing processes: _____
- Control of sequencing keys: ☐ Single entity ☐ Committee ☐ Distributed validators ☐ Not disclosed
- Operational procedures if sequencing infrastructure fails: _____

7. Core Design Pattern and Coordination Disclosure

7.1 Architecture Model

- ☐ PBFT state machine ☐ Sequencer-based architecture ☐ Directed Acyclic Graph (DAG) ☐ Hybrid

7.2 Sequencer Control Structure

- Number of active sequencers: _____
- Configuration: ☐ Single ☐ Rotating ☐ Committee ☐ Other
- Can sequencer reorder transactions? ☐ Yes ☐ No ☐ Not disclosed

7.3 Sequencer Keyholder Transparency

- Who controls sequencing keys? _____
- Number of parties required to recover control: _____
- Are identities publicly disclosed? ☐ Yes ☐ No ☐ Pseudonymous

7.4 Emergency Intervention and Recovery

- Runbooks or operational recovery procedures documented? ☐ Yes ☐ No
- Escalation path defined? ☐ Yes ☐ No
- Responsible recovery parties: _____

7.5 Coordination Channels

- Coordination channels used: ☐ Governance ☐ On-chain ☐ Private chat ☐ Internal dev coordination
- Are operators publicly identified? ☐ Yes ☐ No ☐ Pseudonymous

7.6 Decentralization Consistency

- How does the project reconcile decentralization claims with operational coordination mechanisms?

8. Upgrade Governance and Change Management

8.1 Protocol Upgrade Authority

- Who approves upgrades? ☐ Core dev team ☐ Governance ☐ Validators ☐ Token vote

8.2 Smart Contract Upgradeability

- Are core contracts upgradeable? ☐ Yes ☐ No
- Upgrade mechanism: ☐ Proxy ☐ Governance contract ☐ Admin key

8.3 Emergency Bug Response

- Emergency patch procedure documented? ☐ Yes ☐ No

8.4 Testing Controls

- Test environments used before deployment? ☐ Yes ☐ No
- Independent security audits conducted? ☐ Yes ☐ No

8.5 Rollback Procedures

- Rollback procedure documented? ☐ Yes ☐ No

9. Operational Governance, Documentation, and Accountability

Supervisory evaluation may require visibility into operational governance, documentation practices, and independently auditable performance data.

9.1 Governance Documentation

- Formal governance documents available? ☐ Yes ☐ No

9.2 Incident Logging

- Are outages and incidents formally logged? ☐ Yes ☐ No

9.3 Public Transparency

- Are operational incidents publicly disclosed? ☐ Yes ☐ No

9.4 Accountability

- Are responsible parties documented after incidents? ☐ Yes ☐ No

9.5 Disclosure and Auditability

- Metrics independently auditable? ☐ Yes ☐ No
- Known failure modes disclosed? ☐ Yes ☐ No
- Historical degradations documented? ☐ Yes ☐ No

10. Settlement Exposure and Challenge Periods

- Does the system rely on delayed settlement mechanisms (challenge periods)? ☐ Yes ☐ No
- Challenge period duration: _____
- During challenge period, who bears economic exposure?
☐ User ☐ Liquidity provider ☐ Market maker ☐ Not disclosed

The purpose of this framework is to assist decision makers in distinguishing between theoretical design claims and observed production characteristics, enabling comparisons of distributed networks on a consistent and defensible basis while aligning blockchain adoption with existing operational, risk, and compliance standards applicable to financial markets infrastructure. **Incomplete or unavailable responses may themselves provide useful signals regarding the operational maturity and transparency of a given transaction processing infrastructure environment.**