DTCC

DTCC DIGITAL ASSETS

Framework for the Evaluation and Selection of Layer 1 and Layer 2 Blockchain Networks

Overview

The Depository Trust & Clearing Corporation ("DTCC") applies a structured, risk-based framework to evaluate and select blockchain networks for its digital asset services. These networks, including Layer 1 ("L1") protocols and Layer 2 ("L2") scaling solutions, support the issuance, recording and lifecycle management of tokenized securities within DTCC's ecosystem.

The framework is designed to ensure that the selected networks can comply with applicable securities laws, regulatory expectations and DTCC's standards for resilience, transparency and risk management. The requirements presented in this framework are subject to the terms of the Securities and Exchange Commission's ("SEC") No-Action Letter, which authorizes The Depository Trust Company ("DTC") to operate its tokenization service, and any other legal or regulatory requirements that may apply to DTC's tokenization service over time.

Each network is evaluated against a defined set of criteria, with the specific use case determining whether key requirements are sufficiently met to support selection. Selection decisions are subject to internal governance and supported by documented analysis, creating a consistent, objective and auditable record of the evaluation process.

Evaluation Framework and Methodology

The evaluation process progresses from initial risk screening through business and technical assessment. Each stage operates as a gating mechanism, meaning that a network must satisfy defined requirements at each stage before advancing to the next. This approach is intended to ensure that network selection is aligned with DTCC's responsibilities as a market infrastructure provider for the global financial services industry and, more specifically, DTC's responsibilities as a designated Systemically Important Financial Market Utility ("SIFMU").

The framework is grounded in the following principles:

- **Regulatory alignment as a baseline requirement**. Networks must support compliance with regulatory obligations, including auditability, reporting and supervisory access.
- **Risk mitigation through early screening**. Networks presenting regulatory, legal or operational risks are excluded prior to further evaluation.
- **Client and market relevance**. DTCC evaluates whether there is clear client demand for the network and whether it supports specific, practical use cases.
- **Operational and technical fitness**. Networks must demonstrate the ability to operate reliably at the scale required for financial market infrastructure.

Exclusion Criteria

The initial stage of the evaluation process applies a set of exclusion criteria that are designed to identify networks that would not be suitable for further consideration. These criteria are non-discretionary in nature and reflect minimum requirements for participation in a regulated environment. Application of these criteria is intended to ensure that networks posing unacceptable regulatory, legal or operational risk are not incorporated into DTCC services.

A network may be excluded where one or more of the following conditions are present:

- **Regulatory or legal concerns**. The network is subject to sanctions, restrictions or adverse regulatory findings, or has been associated with activity that presents elevated compliance risk.
- **Lack of regulatory engagement or legal clarity**. The network does not demonstrate a clear legal or jurisdictional framework or lacks sufficient legal clarity or available information to support regulatory compliance within DTCC's intended use case.
- **Inadequate governance transparency**. Governance structures, whether centralized, foundation-led, consortium-based or decentralized, do not provide sufficient transparency, predictability and change-management visibility to enable assessment of operational and regulatory risks.
- **Insufficient compliance capabilities**. The network does not support required controls, including the ability to enable regulatory reporting, auditability or enforcement of compliance requirements
- **Audit-resistant privacy features**. The network employs privacy mechanisms that materially inhibit transaction traceability or supervisory review.
- **Unresolved critical security concerns**. The network demonstrates material security weaknesses or lacks adequate remediation of prior vulnerabilities.

Business and Market Assessment

Networks meeting the initial screening requirements are evaluated to assess whether they support viable and appropriate use within DTCC's service offerings. This stage is intended to ensure that technical evaluation is limited to networks that demonstrate both practical applicability and sustainable operating characteristics within a regulated financial environment.

Key considerations include:

- **Client demand and use case alignment**. DTCC assesses whether there is identifiable demand from market participants and whether the network supports defined use cases consistent with DTCC's product strategy.
- **Market position and ecosystem strength**. Evaluation includes consideration of the network's adoption, liquidity and the depth of its supporting ecosystem, including infrastructure providers and developer activity.
- **Integration feasibility and operational cost**. DTCC evaluates the complexity and cost of integrating the network into its existing architecture, including dependency on third-party providers and the ability to support ongoing operations at an institutional scale.

Technical Assessment

Networks that satisfy the business and market evaluation are subject to a comprehensive technical review to determine whether the network can meet the performance, security and operational requirements associated with financial market infrastructure.

The assessment encompasses the following areas:

- **Performance and Reliability.** DTCC evaluates whether the network can support sustained and peak transaction volumes, provide transaction finality characteristics appropriate for the intended use case, including sufficient certainty, settlement assurances and recovery mechanisms, and maintain consistent operational availability.
- **Security and Resilience.** Assessment includes review of the network's security architecture, audit

coverage, incident response capabilities and overall track record of secure operation.

- **Privacy and Data Handling.** Networks are evaluated for their ability to protect transactional and participant data, ensure that information necessary for verification, audit, and operational continuity remains available and recoverable, and enable required regulatory visibility. Mechanisms for controlled or selective disclosure are an important consideration.
- **Regulatory Alignment.** DTCC assesses the extent to which the network supports compliance with applicable regulatory frameworks, including auditability, reporting functionality and legal clarity across relevant jurisdictions.
- **Interoperability and Standards.** Given DTCC's multi-ledger operating model, networks must demonstrate the ability to interoperate with other systems and support recognized industry standards for data exchange and messaging.
- **Governance.** Governance structures are evaluated for transparency, predictability and the ability to support controlled and well-understood changes to the protocol.
- **Proven Deployment and Institutional Use.** DTCC considers evidence of real-world deployment, including adoption by financial institutions and demonstrated operational stability over time.
- **Compatibility with DTCC Infrastructure.** The network must be capable of integration with DTCC systems, including those supporting token issuance, lifecycle management and data aggregation.
- **Ecosystem Maturity; Operational Risk**. Assesses robustness of developer community, tooling, language support; whether material dependencies on validators, infrastructure providers, governance participants or other critical components could adversely affect operational resilience, network availability or market integrity.

Considerations for Layer 2 Solutions

L2 solutions are evaluated using the same core criteria for L1 networks, with additional focus on their dependence on and interaction with the underlying L1 network. This ensures that enhancements in performance do not introduce incremental risk that would be inconsistent with regulatory expectations.

In particular, DTCC assesses:

- Whether the L2 solution keeps the same strong security protections as the underlying L1 network
- Whether transactions can be settled and funds or assets can be moved back to the L1 network reliably
- Whether the network provides defined mechanisms for dispute resolution, recovery, incident response, rollback prevention and continuity of operations following technical failures whether the L2 solution can handle more activity at lower cost without adding unacceptable risk
- Whether the L2 relies on concentrated infrastructure components, including sequencers, operators or other critical network services, and whether such dependencies create unacceptable operational or resilience risks

Ongoing Monitoring and Review

DTCC recognizes that blockchain networks, the legal and regulatory environment surrounding networks and tokenization will evolve over time. As such, networks selected for use and this framework are subject to ongoing monitoring to ensure continued alignment with regulatory requirements and operational expectations. DTCC will monitor whether this framework continues to be appropriate and effective and may update or amend the framework and accompanying requirements from time to time.

By applying clearly defined selection criteria, enforcing strict exclusion standards and maintaining continuous oversight, DTCC seeks to ensure that all networks incorporated into its digital asset services meet the standards of safety, transparency and reliability required by regulators and market participants.

Last updated: August 12, 2026