

Hkchain: A Layered Reference Architecture for Chain-Enforced Stablecoin Compliance

Technical Report · Version 1.0 · September 2026

Abstract.....	1	7. Governance and supervision planes.....	9
1. Introduction	1	8. Mapping to the compliance lifecycle	10
2. Design principles.....	2	9. Trusted sources and legal entity identifiers.....	10
3. The layered reference model.....	3	10. Reference implementation and current boundaries	11
4. Identity layer: the six-tier model.....	5	11. Conclusion	12
5. Admission layer: the seven gates.....	6	Glossary	13
6. Consensus and settlement layer	8	References	13

Suggested citation: Hkchain (2026). *Hkchain: A Layered Reference Architecture for Chain-Enforced Stablecoin Compliance*. Technical Report, version 1.0. <https://hkchains.net/docs/learn/technical-report>

Abstract

Licensed stablecoin regimes, such as Hong Kong’s Stablecoins Ordinance (Cap. 656, in force since 1 August 2025), require issuers to identify holders, screen against sanctions, transmit originator and beneficiary information with transfers, hold fully backed reserves under independent assurance, and report to the supervisor. Today these controls are usually implemented by each issuer in its own application code: token contracts, custody gateways and screening services. The result differs from issuer to issuer, can be bypassed by any path the application does not cover, and is visible to the supervisor mainly through reports.

This report describes a different placement: compliance as a layer of the payment rail itself, evaluated as a precondition for a transaction to be included in the ledger. We present an OSI-style reference model of seven layers (infrastructure, peer networking, consensus and settlement, admission, identity and authority, representation, and participant services) with governance and supervision as cross-cutting planes. Two structures carry most of the compliance function: a six-tier identity model at the identity layer and seven compliance gates at the admission layer. We map the model onto the compliance lifecycle of licensing, onboarding, pre-transaction checks, settlement and post-transaction monitoring, identify integration points for legal entity identifiers (LEI and vLEI), and describe a reference implementation, Hkchain, together with the boundaries of what it currently enforces. Token economics are outside the scope of this report.

1. Introduction

1.1 The problem

A licensed stablecoin issuer must be able to show, continuously, that every unit in circulation is backed and redeemable at par, that every holder is identified, that no sanctioned party is served, that originator and beneficiary information accompanies each transfer, and that suspicious activity is detected, reviewed and reported. In Hong Kong these obligations are set out in the Stablecoins Ordinance and in the HKMA’s Guideline on Supervision of Licensed Stablecoin Issuers and its AML/CFT Guideline for the same issuers.

The prevailing way to meet them on a public or shared ledger is to place each control in the issuer's application layer. Allowlists and freeze functions live in the token contract. Screening runs in the custody or wallet gateway. Travel Rule data is exchanged through bilateral messaging between service providers. Reserve assurance is published as a report on the issuer's website. This placement has three consequences:

- **Uneven.** Each issuer implements the same rules in its own way. A holder of two issuers' stablecoins is subject to two rule sets, and a supervisor must understand both.
- **Bypassable.** A control is only as complete as the application that hosts it. An alternative interface, a contract upgrade, or a transfer path the application did not anticipate can move value without the check.
- **Indirectly observable.** The supervisor sees the outcome of controls through periodic reports rather than through a shared, verifiable record.

1.2 Approach

We place the controls where every transfer must pass: the admission of transactions into the ledger. To make this placement precise we borrow the method of the OSI reference model. Each layer provides a defined service to the layer above and relies only on the layers below, and the layer at which a function sits determines what can bypass it. A control at the application layer can be bypassed by another application. A control at the admission layer cannot be bypassed by any application; it can only be changed through the governance of the rail.

1.3 Contributions

1. A seven-layer reference model for a compliant payment rail, with governance and supervision as cross-cutting planes (Section 3).
2. A six-tier identity model that binds every holding address to an accountable party (Section 4).
3. A seven-gate admission model evaluated before any transaction takes effect (Section 5).
4. A mapping of the model onto the compliance lifecycle (Section 8).
5. Integration points for trusted identity sources, including LEI and vLEI (Section 9).
6. A reference implementation and an explicit statement of its current enforcement boundaries (Section 10).

The model is technology-neutral and could be realised on other ledger platforms. Where this report describes mechanisms, it refers to the reference implementation as of version 1.0. Mechanisms that are proposed but not implemented are labelled as such.

2. Design principles

P1. Compliance is a precondition to inclusion. Rules that govern the movement of regulated money are evaluated by the ledger's state machine before a transaction takes effect, not by the applications that submit it.

P2. One rule set for every supported path. A transfer submitted through the native interface and a transfer submitted through the EVM interface pass the same gates in the same order. An interface that cannot carry the required evidence is disabled, not exempted.

P3. Identity attaches to accountable parties. Tiers describe natural and legal persons. Software agents and operational keys act under delegation from a person and inherit that person's identity; they are never identities in their own right.

P4. Evidence on the ledger, personal data off it. The ledger records outcomes, commitments (hashes) and decisions. Customer records and Travel Rule data stay with the regulated parties that hold them.

P5. Supervisors observe; they do not operate. The supervisory interface is read-only. Interventions such as a global pause go through governance.

P6. Rule changes are authorised and recorded. Tier definitions, issuer recognition, auditor registration, thresholds and the compliance authority change only through authorised on-ledger transactions, most of them through public governance proposals.

P7. Utility token and regulated money are separate. Network fees are paid in a native utility token. Stablecoins are never used as fee instruments, and the compliance perimeter is drawn around the regulated money.

3. The layered reference model

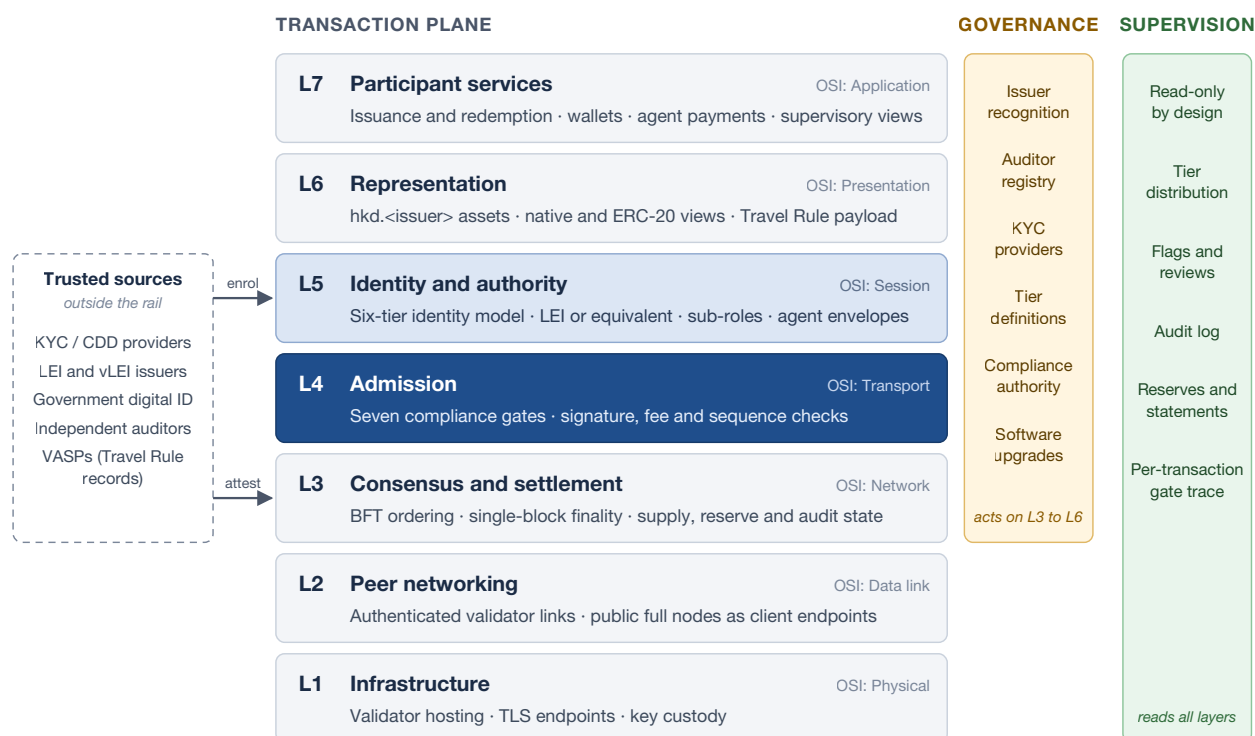
3.1 Why a layered model

The OSI Basic Reference Model (ISO/IEC 7498-1) separates communication into seven layers, each offering a service to the layer above through a defined interface. We use it for its method, not as a claim of protocol equivalence: a ledger runs over TCP/IP and, strictly, belongs entirely to the OSI application layer. The analogy is useful for three reasons. It separates concerns that are often mixed in stablecoin designs. It makes the interface between layers explicit, including what each layer may assume about the layers beneath it. And it makes the bypass question concrete: a function can be avoided by anything that does not traverse the layer where it sits.

3.2 The seven layers

Layer	OSI position	Service to the layer above	Principal functions
L7 Participant services	Application	Business functions for each regulated role	Issuance and redemption operations; holder wallets; agent payments; supervisory dashboards; public reserve lookup; reporting
L6 Representation	Presentation	One unambiguous representation of each asset and each item of compliance evidence, independent of client technology	Issuer-namespaced denominations (<code>hkd.<issuer></code>); native and ERC-20 views of the same balance; Travel Rule payload format; regulator-legible rejection reasons
L5 Identity and authority	Session	Resolution of any signing key to an accountable party, its tier and the mandate under which it acts; establishment, maintenance and termination of that relationship	Six-tier identity registry; institution identifier (LEI or equivalent); delegated sub-roles; agent policy envelopes; revocation and blacklisting
L4 Admission	Transport	Only authenticated, attributable and compliant transactions proceed to ordering and execution	Signature, fee and sequence checks; the seven compliance gates
L3 Consensus and settlement	Network	One final, replicated ledger state	Byzantine-fault-tolerant ordering; deterministic execution; single-block finality; supply, reserve and audit state
L2 Peer networking	Data link	Authenticated, encrypted links between known nodes; dissemination of transactions and blocks	Validator mesh; public full nodes as the only client-facing endpoints

Layer	OSI position	Service to the layer above	Principal functions
L1 Infrastructure	Physical	Compute, storage, network endpoints and key custody	Validator hosting; TLS endpoints; key management



Every transaction that changes the ledger descends from L7 and must pass L4 before it reaches L3.
 OSI positions are a functional analogy, not a claim of protocol equivalence with ISO/IEC 7498-1.

Figure 1. The seven-layer reference model. The admission layer (L4) sits below every participant service and above settlement, so every transaction that changes the ledger traverses it. Governance and supervision act across layers; trusted sources outside the rail feed onboarding outcomes into L5 and reserve attestations into L3.

Three relationships in the model carry the argument.

Admission sits between every application and settlement. Whichever participant service creates a transaction, and whichever representation it uses, the transaction must pass L4 before it can reach L3. This is the property that application-level controls lack.

Identity is established ahead of time; admission applies it per transaction. L5 answers, before any transfer, who a party is, which tier it holds and under what mandate each of its keys may act. L4 answers, for one transaction, whether that party may make this transfer now, given the evidence the transaction carries. As a transaction descends the stack it is created at L7, encoded at L6 (the asset denomination and the Travel Rule payload are attached), bound at L5 (the signer is resolved to a principal and a mandate), admitted at L4, and ordered and settled at L3.

Admission is re-evaluated at settlement. The gates run when a transaction enters a node's pool of pending transactions and again when the block containing it executes. A transaction whose parties changed status in between, for example because an address was blacklisted, fails at execution without effect.

3.3 Cross-cutting planes and external sources

- **Governance plane.** Changes to the rules, to the set of recognised participants and to the software itself. It acts on L3 to L6 through authorised transactions (Section 7.1).
- **Supervision plane.** Read-only access to the records of every layer: tier distribution, flags and review decisions, the audit log, reserve attestations, and per-transaction gate traces (Section 7.3).
- **Trusted sources (outside the rail).** KYC and due-diligence providers, legal entity identifier issuers, government digital identity schemes, auditors, and the service providers that hold Travel Rule records. They feed L5 (onboarding outcomes) and L3 (reserve attestations) through authorised transactions. The rail records their outcomes and commitments, not their underlying data (Section 9).

4. Identity layer: the six-tier model

4.1 Identity records and tiers

Every address that holds or moves the stablecoin resolves to an identity record. The record holds the tier, an institution identifier where applicable, a hash reference to the off-ledger customer record in IVMS 101 form, the enrolment time and the enrolling provider's signature. It holds no personal data. An address without a record can neither send nor receive the stablecoin.

Tier	Name	Typical party	Stablecoin capability enforced at admission	Travel Rule tier
0	Blacklisted	Sanctioned or blocked party	Cannot send or receive	none
1	Unverified	Registered address pending verification	Cannot originate transfers	none
2	Retail basic	Individual after basic due diligence	Transfers below HKD 8,000	minimal
3	Retail enhanced	Individual after enhanced due diligence	Any amount	full
4	Institutional	Licensed service provider or institutional client	Any amount	full
5	Licensed issuer	Licensed stablecoin issuer	Any amount; issue, distribute and complete redemptions; submit reserve attestations	full

The HKD 8,000 figure is the enhanced-information threshold for transfers under the HKMA AML/CFT Guideline; on the ledger it is a rule parameter, not a constant. The capability column is enforced through the Travel Rule tier of each level (Section 5.2): a tier-2 holder cannot claim a higher tier for a larger transfer, and must be re-onboarded at tier 3 or above to make one.

4.2 How tiers change

- **Tiers 1 to 4** are assigned and upgraded by KYC providers whose addresses are authorised by governance. The provider performs due diligence off the ledger and submits the outcome.
- **Tier 5** is granted only by a governance proposal, reflecting the issuer's licence.
- **Tier 0** can be applied at any time by the compliance authority. Three routes lead to it: a direct blacklisting, a sanctions-list update, and an officer's decision to block on a reviewed flag (Section 7.2). All three converge on one ledger operation, and each records a reason and an evidence reference, so every blacklisting can be traced back to its source document or case.

4.3 Delegation

Legal and natural persons act through several keys. The model supports three delegated sub-roles, each bound to a principal:

Sub-role	Bound to	May sign	Additional control
Reviewer	Issuer (tier 5)	Flag review decisions	None
Officer	Issuer (tier 5)	Final decisions on escalated flags	A block decision blacklists the subject
Agent	Holder (tiers 2 to 4)	Transfers only	Policy envelope: per-transaction cap, daily cap, revoked flag

Delegated keys carry no identity record of their own. At every identity-dependent gate the key is resolved to its principal first, so a delegate can never exceed its principal's tier, and sanctioning a principal stops all of its delegates in the same block. Revoking a delegation takes effect from the next block. Keys that issue or destroy the stablecoin are never delegable.

The agent sub-role addresses a problem that grows with agentic payments: distinguishing the accountable principal from the software acting for it, establishing the authority delegated, and checking that a proposed payment falls within that authority. In this model the principal is the identity, the agent is a capability, and the capability's limits are ledger state checked at admission.

4.4 Institution identifiers

The identity record's institution identifier is defined as a FATF-style service-provider identifier: an LEI or equivalent. It is used by two gates. The sanctions gate checks it against the list of sanctioned institutions, and the Travel Rule gate checks that the institution identifiers in a transaction's payload match those registered for its parties. Section 9 discusses how this field can be made verifiable.

5. Admission layer: the seven gates

5.1 Position in the transaction pipeline

Admission applies standard checks first: well-formedness, the fee floor, fee deduction and signature verification. The seven compliance gates run next, and only then does the sender's sequence number advance and the transaction's messages execute. If any blocking gate fails, the transaction leaves the ledger state unchanged.

The same gates apply on the EVM path. Each issuer's denomination is exposed at its own EVM address through an extended ERC-20 interface. Its transfer methods take a Travel Rule payload, construct the equivalent native transfer and run the same seven gates before executing; a failure reverts the call. The standard ERC-20 `transfer` and `transferFrom` methods revert with a message pointing to the extended methods, because they cannot carry Travel Rule evidence. Wallets that read balances through the standard ERC-20 interface continue to work.

5.2 The gates

#	Gate	Type	Question it answers	On failure
1	Identity	Blocking	Is either party, resolved to its principal, blacklisted?	Reject
2	Sanctions	Blocking	Is either party's institution identifier on the sanctioned-institution list?	Reject

#	Gate	Type	Question it answers	On failure
3	Travel Rule	Blocking	Does the transaction carry a Travel Rule payload whose tier matches the sender's registered tier and suffices for the amount, and whose institution identifiers and record references match the registry?	Reject
4	Threshold	Advisory	Is the amount at or above the enhanced-information threshold (HKD 8,000)?	Flag for review
5	Velocity	Advisory	Has the sender reached the configured number of transfers in the rolling window?	Flag for review
6	Role	Blocking	If the signer is a delegated key, is this message type within its role?	Reject
7	Agent policy	Blocking	If the signer is an agent, is the delegation unrevoked and the amount within the per-transaction and daily caps?	Reject

Gates 1 to 4 resolve delegated keys to their principals before any identity lookup. Advisory gates never reject in this version; they place the transaction in the issuer's review queue.

Sanctions have two axes. Address-level sanctions are applied as tier 0 and caught by gate 1. Gate 2 covers the institution axis: if a service provider appears on a sanctions list, transfers by its customers stop before their individual addresses are listed.

The Travel Rule is zero-threshold. Every stablecoin transfer with a counterparty must carry a payload, attached to the transaction itself rather than sent separately. Below the threshold a minimal payload suffices, and its record references must equal the hashes registered for both parties. At or above the threshold, and for tier 3 to 5 senders at any amount, a full payload is required, naming both parties' institution identifiers. The payload's declared tier is treated as a claim and checked against the sender's registered tier, so it cannot be forged upward. One payload covers exactly one transfer; a transaction bundling several transfers is rejected.

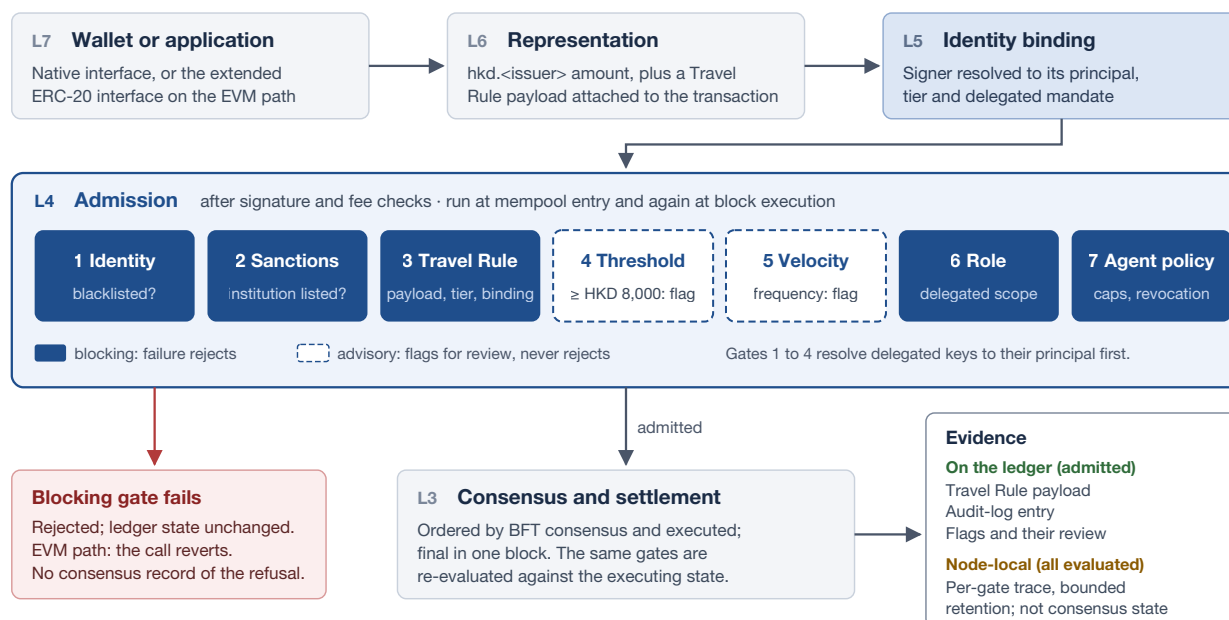


Figure 2. The path of a transfer through the admission layer. The transaction is encoded (L6) and bound to an accountable party and mandate (L5) before the seven gates run (L4). A failing blocking gate leaves the ledger unchanged; an admitted transfer is ordered and settled with single-block finality (L3) and leaves evidence on the ledger.

5.3 Evidence produced by admission

Admission produces two kinds of evidence, and the difference matters for anyone who will rely on it.

On the ledger (consensus state), for admitted transfers:

- the Travel Rule payload (tier, institution identifiers and record hashes), stored against the transaction hash;
- an audit-log entry for each transfer, indexed by party, time and type;
- flags raised by the advisory gates, with their full review history;
- the agent's spending window, where an agent signed.

Node-local (not consensus state), for every evaluated transaction including rejected ones:

- a per-gate trace recording each gate's result, its reason in regulator-legible language, and the resources it consumed, queryable by transaction hash within a bounded retention window;
- a simulation interface that evaluates a candidate transaction against the gates without changing state.

A rejected transaction therefore leaves no consensus record in this version. This is a deliberate choice: a rejected transaction does not consume block space, and a refusal does not become permanent ledger history. The consequence is that evidence of a refusal is operational evidence held by a node, not ledger evidence. Whether a regulated rail should keep a consensus-recorded log of refusals is an open design question (Section 10.3).

6. Consensus and settlement layer

6.1 Ordering and finality

A Byzantine-fault-tolerant consensus protocol orders transactions among a permissioned validator set and finalises each block when it is committed. Settlement is final after one block; there is no probabilistic reorganisation. The compliance decision and the settlement it permits therefore refer to the same ledger state.

6.2 Issuance and redemption

- **Issue.** A tier-5 issuer may create new units only if its most recent reserve attestation has been co-signed and is within the freshness window set by governance. New units go to a treasury controlled by the ledger, not to circulation.
- **Distribute.** The issuer releases units from its treasury to a recipient. This is the moment money enters circulation, and a distribution passes the same gates as any other transfer.
- **Redeem.** A holder submits units for redemption. The units are withheld from circulation and a redemption request opens. The issuer pays fiat off the ledger and acknowledges the request with a payment reference, at which point the units are destroyed. Redemption at par is an off-ledger obligation whose completion is recorded on the ledger.
- **Pause and freeze.** An issuer can pause activity in its own denomination; a global pause requires governance. The compliance authority can freeze individual accounts.

6.3 Proof of reserve

Reserve assurance requires two signatures. The issuer submits an attestation stating the period, circulation, reserve market value, a snapshot value for a randomly selected day, and the hash of the off-ledger assurance report. A registered auditor co-signs it, and only then does it become attested and able to

support new issuance. Auditors are registered and revoked by governance, so the auditor's standing is itself a ledger fact.

At the first block of each UTC day, the ledger records a statement per issuer: circulation, reserve value and the attestation it relies on. Any holder can query which attestation backs each denomination they hold, which turns public disclosure from a published report into a lookup anyone can perform.

7. Governance and supervision planes

7.1 Governance

Change	Authorised by
Recognise an issuer (tier 5)	Governance proposal
Register or revoke an auditor	Governance proposal
Register a new issuer denomination	Governance proposal (its EVM representation also requires a software release)
Authorise KYC providers; set tier definitions	Governance proposal
Appoint or rotate the compliance authority	Governance proposal
Adjust rule parameters (Travel Rule threshold, velocity limits)	Compliance authority
Update the sanctions list; blacklist; freeze accounts	Compliance authority
Pause an issuer's denomination	That issuer
Global pause	Governance proposal
Protocol software upgrade	Governance proposal, executed at a scheduled height

Governance proposals are public and pass through a voting period. The compliance authority is a single ledger address, which can be a multi-signature account, appointed by governance to take time-sensitive operational actions. Each of its actions is recorded with a reason and an evidence reference.

7.2 Review workflow

Advisory flags enter the issuer's review queue. A reviewer approves, escalates or blocks. Escalated flags go to an officer, who approves or blocks. Decisions, and hashes of the supporting evidence, are recorded on the ledger; the evidence itself stays in the issuer's case-management system. A block decision moves the subject to tier 0 with the flag's case reference as the evidence chain, so the path from an alert to a sanction is reconstructable from ledger records.

7.3 Supervision

The supervisor has a read-only view across all issuers: circulation and reserves per issuer, the distribution of identities by tier, sanctions events, flags and review decisions, the audit log, daily statements, and the gate trace of individual transactions. There is no supervisor-signed transaction type. This reflects the supervisory relationship: the supervisor observes, requires and sanctions under its legal mandate, while operational control stays with licensed issuers. Where emergency action on the rail is needed, it goes through governance, in which the supervisor can take part according to the governance arrangement.

8. Mapping to the compliance lifecycle

Payment compliance is commonly described as a lifecycle: licensing of the institution, onboarding of the customer, checks before a transaction, settlement, and monitoring and remediation afterwards. The table maps each control onto the layer that performs it.

Stage	Control	Layer or plane	Mechanism in the reference implementation
Licensing	Recognition of the licensed issuer	Governance	Tier 5 granted by governance proposal
Licensing	Reserve safeguarding and independent assurance	L3, governance	Two-signature attestation; issuance requires a fresh attestation; governed auditor registry
Onboarding	Identity verification	L5, trusted sources	Enrolment by an authorised KYC provider; tier; hash of the off-ledger record
Onboarding	Sanctions screening	L5	Tier 0; sanctioned-institution list
Onboarding	Authority, mandates and delegation	L5	Sub-roles; agent policy envelopes
Onboarding	Transaction permissions	L5, applied at L4	Tier-bound Travel Rule capability; agent caps
Onboarding	Ongoing due diligence	L5	Tier upgrades; blacklisting with evidence reference
Pre-transaction	Counterparty and principal checks	L4 (gate 1)	Both parties resolved to principals, registered and not blacklisted
Pre-transaction	Sanctions screening	L4 (gates 1, 2)	Address axis and institution axis
Pre-transaction	Authority and policy-limit checks	L4 (gates 6, 7)	Role allowlist; agent envelope
Pre-transaction	Travel Rule information	L4 (gate 3)	Payload tier, amount capability, registry binding
Pre-transaction	AML/CFT pattern checks	L4 (gates 4, 5)	Advisory flags into the review queue
Pre-transaction	Record of the authorisation outcome	L3	Payload, audit entry and flags for admitted transfers; node-local gate trace for all evaluated transactions
Settlement	Execution and finality	L3	Single-block finality
Post-transaction	Monitoring and reporting	Supervision plane	Flags, audit log, daily statements, report queries
Post-transaction	Protective actions	Governance plane, L5	Freeze, blacklist, pause
Post-transaction	Recall or reversal	Not on the ledger	Not supported after finality; value returns through redemption or a new transfer
Post-transaction	Disputes	Off the ledger	Outside the rail's scope

9. Trusted sources and legal entity identifiers

9.1 The rail as a relying party

The rail does not perform due diligence. It relies on outcomes asserted by trusted sources and records who asserted them and when. In the reference implementation the trust anchor is the transaction signature of a

KYC provider authorised by governance. The provider's signature over its own dossier is stored for audit but not verified by the ledger. The quality of every identity-dependent gate is therefore bounded by the quality of the onboarding evidence behind it, and making that evidence verifiable is the most direct way to raise it.

9.2 Where the LEI sits today

The institution identifier in each identity record is defined as an LEI or equivalent. Two gates depend on it: the sanctions gate (institution axis) and the Travel Rule gate (binding a payload's institution identifiers to the registry). In the current version it is a free-form field. The ledger does not check the ISO 17442 format (twenty characters ending in two check digits computed under ISO/IEC 7064 MOD 97-10) and does not check the identifier's registration status.

9.3 Integration path (proposal, not implemented)

1. **Structural validation.** For tier 4 and tier 5 records, require the institution identifier to be a well-formed LEI, and record explicitly whether an identifier is an LEI or another scheme.
2. **Verifiable onboarding.** When onboarding a tier 4 or tier 5 party, the enrolling provider verifies the entity's vLEI credential and, where relevant, a role credential for the person authorising the enrolment. The ledger records a digest of the verified credential and a reference to its status alongside the identifier.
3. **Lifecycle coupling.** A revoked or lapsed credential triggers a tier review through the existing downgrade and blacklisting routes, with the credential status as the evidence reference.
4. **Retail equivalents.** The same pattern applies to government-backed digital identity schemes as trusted sources for tiers 2 and 3.

With these steps the institution identifier used at admission becomes verifiable rather than asserted, and the institution-level sanctions check and Travel Rule binding inherit that assurance. They require no change to the layer structure: they strengthen the evidence entering L5 and leave L4 unchanged.

10. Reference implementation and current boundaries

10.1 Implementation

Hkchain is a Cosmos SDK application (v0.53) with four purpose-built modules: stablecoin (supply, issuance, redemption, pause and freeze), compliance (the admission gates, audit log, Travel Rule registry, delegation and review workflow), reserve (attestations, auditor registry, daily statements) and identity (the tier registry). EVM execution is provided by cosmos/evm (v0.6.0) and consensus by CometBFT (v0.38). The compliance gates are implemented as transaction-admission decorators shared by the native path and the extended ERC-20 interface.

Two deployments exist: a single-node development network and a five-validator permissioned test network. On the test network the validators accept peer connections only, and clients reach the ledger through a public full node. The test network carries two test issuer denominations, a supervisory dashboard, a block explorer that shows each transaction's gate trace, and an onboarding portal that issues test identities. Public documentation is at <https://hkchains.net/docs>.

10.2 Current boundaries

The following limits apply to version 1.0. They are stated so that the claims in this report can be relied on precisely.

1. **The perimeter is the regulated money.** The gates apply to stablecoin denominations. Transfers of the native utility token used for fees are not gated, by design (P7).
2. **Message coverage.** The gates evaluate single transfers, distributions, redemption requests and extended ERC-20 transfers. Other message types that can move value, namely multi-output sends, authorisation-wrapped sends and inter-chain transfers, are not yet inside the perimeter. They are to be brought inside it, or disabled, before any production deployment.
3. **Advisory rules do not block.** Threshold and velocity gates flag for review but never reject.
4. **Refusals are not consensus records** (Section 5.3).
5. **Sanctions updates are authorised transactions**, not a real-time feed.
6. **Onboarding evidence is signer-authenticated, not content-verified** (Section 9.1).
7. **The agent daily cap uses a fixed 24-hour window** that starts at the first spend. Across a window boundary an agent can spend up to twice the cap within 24 hours.
8. **Travel Rule content is exchanged off the ledger.** The ledger verifies tiers, bindings and commitments, not the completeness of the underlying records.
9. **Key custody on the test network uses software keys.** Hardware security modules and maker-checker controls are production requirements.
10. **No recall after finality** (Section 8).

10.3 Open questions and next steps

- **Refusal records.** Should refusals be committed to consensus state, and at what cost in block space and permanence?
- **Blocking versus flagging.** Per-rule configuration, set by governance, of whether an advisory rule rejects or flags.
- **Verifiable institution identity.** The LEI and vLEI integration path in Section 9.3.
- **Sanctions feed.** A real-time list feed with governance as fallback.
- **Perimeter completion.** Closing the message-coverage gap in Section 10.2.
- **Reporting.** Export of supervisory reports in the supervisor's prescribed formats.

11. Conclusion

Where a control sits determines what can bypass it. Placing stablecoin compliance at the admission layer of the rail, below every application and above settlement, gives all issuers one rule set, removes the paths by which application-level controls are avoided, and gives the supervisor a direct, shared view instead of a set of reports. The layered model gives regulators, issuers and technology providers a common vocabulary for specifying where each control lives, what it relies on and what may bypass it. The reference implementation shows that the model can be built from existing components. Its stated boundaries show what remains before it can carry production value.

Glossary

Term	Meaning in this report
Admission	Evaluation of a transaction before it is ordered and executed; failure leaves ledger state unchanged
Advisory gate	A gate that flags a transaction for review without rejecting it
Blocking gate	A gate whose failure rejects the transaction
Compliance authority	Ledger address appointed by governance to take operational compliance actions
Institution identifier	The identifier of the service provider responsible for a party; an LEI or equivalent
Policy envelope	The per-transaction cap, daily cap and revocation flag that bound an agent
Principal	The accountable natural or legal person to whom a delegated key resolves
Sub-role	A delegated key bound to a principal: reviewer, officer or agent
Tier	A party's identity level, from 0 (blacklisted) to 5 (licensed issuer)
Travel Rule payload	Originator and beneficiary evidence attached to a transfer: tier, institution identifiers and hashes of off-ledger records

References

- Hong Kong SAR. *Stablecoins Ordinance* (Cap. 656). In force 1 August 2025.
- Hong Kong Monetary Authority (2025). *Guideline on Supervision of Licensed Stablecoin Issuers*.
- Hong Kong Monetary Authority (2025). *Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Stablecoin Issuers)*.
- Financial Action Task Force. *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations*, Recommendations 15 and 16, as amended.
- Financial Action Task Force (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*.
- Joint Working Group on interVASP Messaging Standards (2020). *IVMS 101: interVASP Messaging Standard*.
- ISO 17442-1:2020. *Financial services: Legal entity identifier (LEI), Part 1: Assignment*.
- ISO/IEC 7064:2003. *Information technology: Security techniques, Check character systems*.
- Global Legal Entity Identifier Foundation. *vLEI Ecosystem Governance Framework*.
- ISO/IEC 7498-1:1994. *Information technology: Open Systems Interconnection, Basic Reference Model: The Basic Model*.
- Cosmos SDK documentation, v0.53. <https://docs.cosmos.network>
- CometBFT documentation, v0.38. <https://docs.cometbft.com>
- cosmos/evm, v0.6.0. <https://github.com/cosmos/evm>
- Ethereum Improvement Proposal 20 (EIP-20). *Token Standard*.