
**NEOFINGO WHITE PAPER SERIES**

WP-01 - TECHNOLOGY PROTOCOL

# The Neofingo Protocol

## Technical Architecture for Cross-Border Digital Trade Finance

API Orchestration · Cryptographic Integrity · Data Sharing Protocols
Cybersecurity Guardrails · AI-Enabled Compliance · The neo-LC Instrument

March 2026
Version 1.0 | For Consultation

*Published under the institutional umbrella of the Neofingo Committee; the 24-Hour Economy & Accelerated Export Development Authority, Office of the President, Republic of Ghana; ODI Global; the AfCFTA Secretariat; and the AU 4D Network*

# Contents

# 1. Executive Summary

This white paper sets out the complete technical architecture of the Neofingo protocol - an open-licence digital infrastructure designed to reconnect African SME exporters with international trade finance capital pools, beginning with the United Kingdom and the Republic of Ghana.

The global trade finance gap now exceeds $2.5 trillion, with Sub-Saharan Africa bearing a disproportionate share estimated at $120 billion annually (compared with the region's GDP at roughly $2 trillion). Ghana alone confronts a shortfall of approximately $7 billion. The root cause runs deeper than a shortage of capital. Correspondent banking relationships have contracted by nearly 40 per cent across the continent over the past decade, severing the trust infrastructure through which letters of credit - the foundational instruments of cross-border commerce - are issued, confirmed, and settled. Small and medium enterprises, which account for the overwhelming majority of African exporters, find themselves locked out of the very mechanisms that would allow them to convert production capacity into export revenue.

Neofingo addresses this structural failure through a five-layer protocol stack that operates entirely within existing regulatory perimeters in both the UK and participating African jurisdictions, such as Ghana. The protocol does not require any novel licensing regime. Instead, it provides a standards-compliant orchestration layer through which already-licensed banks, neobanks, electronic money institutions, fintechs, and trade intermediaries can interoperate across borders with dramatically reduced friction, cost, and risk.

At the heart of the protocol sits the neo-LC - a programmable, AI-assisted digital letter of credit that conforms to ICC UCP 600 and eUCP 2.1 rules, the UK Electronic Trade Documents Act 2023, and ISO 20022 messaging standards. The neo-LC transforms a paper-bound, error-prone instrument into a machine-readable, real-time workflow accessible from a mobile device in Tamale or a trade desk in the City of London.

Critically, this paper introduces the Neofingo Hash-Chain - a novel cryptographic hash-function chain that delivers document integrity, tamper evidence, and audit-trail immutability without requiring a distributed ledger or blockchain infrastructure to function. Where participants choose to deploy a permissioned ledger for additional utility - particularly around records immutability and constructive possession of electronic trade documents - the protocol accommodates that choice as an enhancement, but never as a prerequisite.

The paper specifies, in granular detail, the data sharing rules that make the protocol operational: which actor must share what category of data, at which point in the transaction lifecycle, with which counterparties, under which consent and legal bases, and subject to which jurisdictional constraints. These flows draw on best practice from digital public infrastructure deployments worldwide - India's Unified Payments Interface, the UK's Open Banking framework, Estonia's X-Road, and Singapore's Trade Data Exchange - whilst layering on the cross-border and interstate dimensions that the UK-Africa corridor uniquely demands.

Neofingo is designed to supply the missing orchestration layer: the connective tissue between regulatory environments, data regimes, settlement rails, and compliance engines that already exist but do not yet speak to one another across the jurisdictional divide that separates European capital from African enterprise.

# 2. Defining Our Problem Space: How Current Digital Trade Architecture Fails African SMEs

## 2.1 Critical Economic Actors Face Exclusion

The trade finance gap affecting African SMEs is often described in aggregate terms - billions of dollars of unmet demand - but its mechanics are granular and quite specific. Each rejected trade finance application represents a concrete sequence of system failures, and understanding those sequences is essential to designing a protocol that can interrupt them.

Consider a shea butter cooperative in northern Ghana seeking to export a $45,000 consignment to a specialty retailer in Bristol. The cooperative has the product, the buyer has the purchase order, and the commercial logic is sound. The transaction fails - or never begins - because of five interlocking frictions that the existing digital trade architecture does nothing to resolve.

### 2.1.1 Information Asymmetry and the Verification Desert

The Bristol buyer's bank cannot verify the cooperative's creditworthiness. Credit bureau data in Ghana is sparse for SMEs, and what exists is trapped in formats and systems that are illegible to UK-based risk engines. The cooperative may have a decade of reliable supply, verified by its aggregator and attested by the Ghana Cocoa Board, but none of that performance history is structured, portable, or machine-readable. The data definitely exists. No doubt about that. The infrastructure to make it flow, however, rather lamentably, does not.

### 2.1.2 Compliance Cost Inversion

For a UK bank or neobank, the marginal cost of performing Know Your Customer and Anti-Money Laundering checks on a Ghanaian SME counterparty routinely exceeds the profit margin on a sub-$50,000 trade. The ADB estimates that compliance costs have risen by more than 50 per cent across the industry since 2015, and they fall with particular weight on small-ticket, emerging-market transactions. The perverse result: the smaller the business, and the greater the developmental impact of financing it, the less economically viable it is for the financial institution to do so.

### 2.1.3 Documentary Latency and Error Cascades

A typical paper-based letter of credit presentation involves up to 27 separate documents exchanged between as many as 30 different stakeholders. Between 70 and 80 per cent of first-time paper LC presentations contain discrepancies - transposed figures, inconsistent descriptions of goods, missing certificates. Each discrepancy triggers a reject-repair cycle that adds days or weeks to processing time. For an SME whose working capital is already stretched, each additional day of documentary delay compounds the financing cost and erodes the commercial margin that justified the trade in the first place.

### 2.1.4 Correspondent Banking Retreat

The retreat of international correspondent banks from African markets has been well documented but insufficiently understood in its trade finance consequences. When a correspondent relationship closes, the African bank loses its ability to confirm or advise letters of credit denominated in hard currency. The bank's clients - SME exporters - lose access to the instrument entirely. Nostro account requirements have simultaneously been elevated to levels that lock large pools of capital in overseas accounts, capital that could otherwise be deployed productively within the domestic economy. The result is a double squeeze: higher collateral requirements and fewer channels through which to post them.

### 2.1.5 The Platform Fragmentation Trap

The digital trade finance landscape is populated by vertical solutions - electronic bill of lading platforms, invoice finance marketplaces, blockchain-based LC pilots - that each solve a narrow slice of the problem but do not interconnect. A Ghanaian exporter might gain access to an electronic certificate of origin through one platform, an invoice discounting facility through another, and an eBL through a third, yet still find that no single workflow can carry a transaction from purchase order to settlement in a continuous, compliant, auditable chain. The insight from analysis undertaken by a prominent consulting entity, BCG, of the trade finance ecosystem has remained stubbornly current: vertical point solutions, however sophisticated, do not aggregate into a horizontal solution. The orchestration layer is missing.

## 2.2 What Existing Solutions Leave Unresolved

Various assessments of digital trade finance adoption, and of contemporary trade-related technology stacks, all converge on a diagnosis: the legal frameworks are increasingly supportive (e.g. ETDA 2023 & MLETR, eUCP 2.1), the messaging standards are maturing (e.g. ISO 20022 & SWIFT's gpi), and the component technologies are available (AI, distributed ledgers, API gateways, & OCR). Yet adoption remains low, and the trade finance gap continues to widen.

The reason, from this paper's standpoint, is mostly architectural. Each of these analyses identifies interoperability as the central unsolved challenge - the ability to connect front-end innovation (digital interfaces, mobile access) with back-end processing (risk engines, compliance checks, settlement rails) across jurisdictional, institutional, and technological boundaries. The Neofingo protocol is designed precisely to occupy that architectural gap in a step-by-step scalable fashion that is practical, measured, and acutely aware of the coordination overhead.

# 3. Protocol Architecture: The Five-Layer Stack

The Neofingo protocol is organised as a five-layer stack, each layer performing a distinct function whilst maintaining clearly defined interfaces with the layers above and below it. The architecture is also designed to be relatively modular and reducible so that proofs of concept can proliferate, interweave, and build momentum.

The layered architecture itself serves three strategic objectives: it allows different participants to engage at different layers depending on their capabilities and regulatory posture; it permits incremental deployment (the protocol can go live with minimal infrastructure and deepen over time); and it isolates failures, so that a disruption at one layer does not cascade through the system.

> *Design Principle: Neofingo is an orchestration protocol rather than a definitive platform. It does not hold funds, issue guarantees, or take credit risk. It provides the connective logic through which licensed actors perform these functions within the terms of their existing authorisations.*

## 3.1 Layer 1: Connectivity and Messaging

The foundation layer handles all message transport between participants. The Neofingo API Gateway operates as a hub-and-spoke routing engine, enforcing ISO 20022 message formats for all trade finance events. This is strategic choice. ISO 20022 is now the mandatory messaging standard for SWIFT's cross-border payments, the EU's TARGET2, and the Bank of England's RTGS renewal. By adopting it from inception, Neofingo ensures that data generated by a Ghanaian SME is natively readable by any major global financial institution without manual re-keying or format conversion.

The gateway supports both synchronous REST API calls (for real-time events such as issuance confirmations) and asynchronous message queuing (for batch processes such as end-of-day reconciliation). Authentication uses OAuth 2.0 with OpenID Connect, providing federated identity management across jurisdictions. Every message transiting the gateway is assigned a unique correlation identifier, time-stamped with a trusted time-stamp authority, and logged to the Neofingo Hash-Chain (Section 7).

### 3.1.1 Resilience and Low-Bandwidth Adaptation

Given uneven internet infrastructure across African markets, the connectivity layer incorporates graceful degradation. Where broadband connectivity is available, the full API suite operates in real time. Where connectivity is intermittent or bandwidth-constrained, the protocol supports store-and-forward messaging using compressed JSON payloads, with automatic retry logic and conflict resolution upon reconnection. A lightweight USSD interface provides basic transaction status and approval functions for participants operating from feature phones - a critical inclusion for agricultural cooperatives in rural regions.

## 3.2 Layer 2: Identity, KYB, and Trust Resolution

The identity layer aggregates, validates, and maintains the trust profiles of all entities participating in a Neofingo-mediated transaction. Rather than building a proprietary identity system, the protocol acts as an identity broker - ingesting verified credentials from national identity systems, credit bureaux, and international utilities, then presenting a normalised trust profile to downstream layers.

For International/European/UK-side participants, identity verification aligns with the Digital Identity and Attributes Trust Framework (DIATF) and draws on FCA-regulated identity providers. For Ghanaian participants, the protocol aligns with the formatting of the Ghana Card (national identity) where necessary, the Registrar General's Department (business registration), and local credit reference bureaux. At the pan-African level, alignment is anticipated with Afreximbank's MANSA repository to bolster the AfCFTA Hub corroborative KYC layer, and with Legal Entity Identifiers (LEIs) issued by the Global LEI Foundation to resolve corporate identities unambiguously across jurisdictions.

The identity layer also manages consent. Under the Neofingo Consent Protocol (NCP), every data-sharing action requires explicit, purpose-limited, revocable consent from the data subject, recorded immutably on the Hash-Chain. This aligns with Ghana's Data Protection Act 2012 (Act 843), the UK GDPR, and emerging pan-African data governance frameworks.

## 3.3 Layer 3: Trade Document Processing and Compliance

This is the operational core of the protocol - the layer where trade documents are ingested, validated, classified, and matched against the terms of the neo-LC. The processing engine operates in three phases.

**Phase 1 - Document Ingestion:** Documents enter the system through multiple channels: direct API submission from integrated ERP or accounting systems, manual upload via the Nomi mobile interface, or OCR-assisted capture from scanned paper documents. Each document is immediately assigned a cryptographic hash (SHA-256) and registered on the Hash-Chain, creating an immutable record of the document's state at the point of submission.

**Phase 2 - AI-Assisted Validation:** The Nomi compliance engine (Section 10) performs automated checks against eUCP 2.1 presentation rules, cross-referencing each document field against the terms of the issued neo-LC. The engine verifies consistency across the document set - matching goods descriptions, quantities, values, and shipping details across invoice, bill of lading, packing list, and certificate of origin. Discrepancies are flagged with plain-language explanations and suggested corrections, enabling the SME to cure defects before formal presentation rather than after rejection.

**Phase 3 - Compliance Screening:** Documents and counterparty data are screened against sanctions lists (OFAC, EU, UN consolidated), adverse media databases, and trade-based money laundering (TBML) typology indicators. The screening uses a risk-scoring model aligned with JMLSG guidance and the UK Money Laundering Regulations 2017, with human-

in-the-loop oversight mandated for all transactions exceeding configurable thresholds. PRA Supervisory Statement SS1/23 governs the model risk framework, including validation, backtesting, data lineage, and drift monitoring.

## 3.4 Layer 4: Settlement and Liquidity Management

The settlement layer manages the movement of funds across the corridor, connecting African local-currency payment rails with UK hard-currency settlement systems. The architecture is designed around the Nostro-Lite model - a Neofingo innovation that dramatically reduces the collateral requirements for African fintechs maintaining settlement accounts with London neobanks.

In a traditional correspondent banking arrangement, the African bank must maintain large cash deposits in a nostro account to cover potential settlement obligations. The Nostro-Lite model substitutes a portion of that cash collateral with data collateral - the real-time, cryptographically verified visibility into the underlying trade assets provided by the Neofingo protocol. Because the London neobank can see, in real time, the status of every document, every compliance check, and every shipment milestone, its exposure uncertainty decreases, and the cash collateral required decreases proportionally.

Settlement rails include all the popular channels: UK Faster Payments Service and CHAPS for sterling legs, SWIFT gpi for hard-currency cross-border transfers, and national interbank networks, big card networks, and PAPSS (Pan-African Payment and Settlement System) for intra-Africa local-currency legs. The protocol supports configurable netting windows (intraday, T+1, or bilateral) and programme-governed FX hedging with pre-set tolerance bands. To be clear, Neofingo does not impose new payment protocols and settlement rules on the incumbent arrangements. It simply documents activity.

## 3.5 Layer 5: Observability, Analytics, and Governance

The top layer provides real-time dashboards, anomaly detection, and post-trade analytics for all programme participants and regulators. Dashboards are role-segmented: an SME exporter sees the status of their transaction; a neobank risk officer sees portfolio-level exposure; a central bank supervisor sees aggregate corridor volumes, default rates, and compliance metrics.

Anomaly detection algorithms monitor document submission patterns, payment behaviours, and counterparty risk signals, flagging deviations that may indicate fraud, money laundering, or operational failure. All analytics outputs are audit-logged and available to the Neofingo Committee serving as the Programme Governance Board, which comprises representatives of UK issuing institutions, African fintech partners, DFI stakeholders, legal counsel, and an independent risk chair.

# 4. The neo-LC Instrument: Structure and Lifecycle

The neo-LC is the programmable, digital successor to the traditional paper letter of credit. It preserves the legal framework and commercial logic of the LC - the buyer's bank's undertaking to pay the seller upon compliant presentation of specified documents - whilst eliminating the documentary friction, error cascades, and access barriers that render the traditional instrument unusable for the vast majority of African SME exporters.

## 4.1 Legal Foundation

The neo-LC operates under dual legal anchoring. On the UK side, the Electronic Trade Documents Act 2023 provides the statutory basis for treating electronic trade documents as legally equivalent to their paper counterparts, including the critical concept of 'possession' of an electronic document. On the international trade law side, the neo-LC conforms to ICC Uniform Customs and Practice for Documentary Credits (UCP 600) as supplemented by the electronic supplement eUCP Version 2.1 (2023), which governs the electronic presentation of documents under a credit. Where UNCITRAL's Model Law on Electronic Transferable Records (MLETR) has been adopted or is in progress in a participating jurisdiction, the protocol aligns with its provisions on functional equivalence and technological neutrality.

## 4.2 The neo-LC Data Structure

Each neo-LC is a structured digital object encoded in ISO 20022-compliant XML, comprising the following core fields:

| Field | Content and Standard |
|---|---|
| Instrument Identifier | Unique neo-LC reference (UUID v4) plus LEI of issuing institution |
| Applicant (Importer) | LEI, registered name, jurisdiction, DIATF or equivalent identity attestation |
| Beneficiary (Exporter) | LEI or national business ID, registered name, jurisdiction, MANSA profile reference |
| Issuing Institution | LEI, FCA/PRA authorisation reference, SWIFT BIC |
| Confirming/Advising Institution | LEI, local regulatory authorisation, SWIFT BIC or Neofingo network ID |
| Amount and Currency | Face value, settlement currency (GBP, USD, EUR), applicable FX rate lock mechanism |
| Document Requirements | Machine-readable list of required documents per eUCP Article e5, with hash references to template specifications |
| Shipment Terms | Incoterms reference, latest shipment date, port/airport of loading and discharge |

| | |
|---|---|
| Expiry and Presentation Period | Expiry date, presentation deadline (days after shipment), eUCP time-stamp validation rules |
| Conditions and Clauses | Programmatic conditions: partial shipment, transhipment, insurance requirements, inspection clauses |
| Settlement Instructions | Nominated settlement rails, netting window, Nostro-Lite account references |
| Hash-Chain Anchors | Root hash of the neo-LC record, linking to the Neofingo Hash-Chain for integrity verification |

## 4.3 Lifecycle Stages

The neo-LC moves through a defined lifecycle, with each transition recorded on the Hash-Chain and triggering downstream events through the API Orchestration Suite.

**Stage 1 - Application and Origination:** The exporter, guided by the Nomi AI interface, provides trade details: goods description, value, shipment schedule, and buyer information. The African fintech distributor ingests this data, performs local KYB verification, and packages it as an ISO 20022 trade initiation message (tsmt.019). This is transmitted to the Neofingo Gateway, which routes it to the nominated issuing institution in London.

**Stage 2 - Risk Assessment and Issuance:** The issuing neobank's risk engine evaluates the application against its own proprietary models but is welcome to leverage the Neofingo Hybrid Risk Score (NHYRS). The NHYRS composite metric combines the exporter's transaction history on the network, behavioural signals, buyer credit quality, sectoral and sovereign risk, and document integrity indicators. The model operates under PRA SS1/23 governance: it is inventoried, validated, subject to backtesting, and incorporates a mandatory human override capability. If approved, the neobank issues the neo-LC as a digitally signed ISO 20022 message, which is registered on the Hash-Chain with a time-stamped issuance event.

**Stage 3 - Advising and Confirmation:** The neo-LC is transmitted to the advising or confirming institution in the exporter's jurisdiction. Advising adds a layer of authentication (the advising bank verifies the issuing bank's digital signature). Confirmation adds a payment undertaking from the local institution - particularly valuable for exporters who need certainty of payment irrespective of the issuing bank's condition.

**Stage 4 - Fulfilment and Presentation:** The exporter ships the goods and assembles the document set specified in the neo-LC. Each document is digitised (if not already born-digital), hashed, and submitted through the Nomi interface. The AI compliance engine validates the presentation against eUCP rules, flags discrepancies for correction, and - once the exporter confirms the presentation - transmits it as an eUCP-compliant electronic presentation to the issuing bank, with all hash references anchored on the Hash-Chain.

**Stage 5 - Examination and Acceptance:** The issuing bank examines the presentation within the eUCP Article e5 timeframe (maximum five banking days). The Nomi engine pre-screens the presentation on both sides, so that by the time it reaches the bank's trade desk, the probability of discrepancy has been reduced from the industry-standard 70-80 per cent to a target of under 10 per cent. Acceptance triggers a settlement instruction to the nominated payment rail.

**Stage 6 - Settlement:** Funds move through the settlement layer - Nostro-Lite accounts for the corridor legs, Faster Payments or CHAPS for sterling settlement, or other preferred payment channel for local-currency disbursement to the exporter. **The entire chain - from issuance to settlement - is designed to compress from a legacy timeline of 14-21 days to a target of 48-72 hours for standard flows.**

**Stage 7 - Archival and Data Enrichment:** Upon settlement, the complete transaction record - including all documents, compliance logs, hash-chain entries, and settlement confirmations - is archived as an Evidence Bundle. This bundle serves three purposes: dispute resolution (it is designed to be court-admissible), regulatory audit (available to supervisors upon request), and credit history enrichment (with the exporter's consent, the transaction record feeds into their portable credit profile, reducing the cost and friction of future applications).

# 5. The API Orchestration Suite

The Neofingo API Orchestration Suite is the nervous system of the protocol - the mechanism through which all participants interact, all events are sequenced, and all data flows are governed. The suite is designed on three architectural principles: event-driven choreography (participants respond to events rather than following a rigid, centrally orchestrated sequence); API-first design (every protocol function is exposed as a versioned, documented API endpoint); and consent-gated access (no data traverses any API without a recorded, purpose-limited consent from the data subject).

## 5.1 Core API Domains

The orchestration suite is organised into six functional domains, each comprising a cluster of related endpoints.

| Domain | Key Endpoints | Function |
|---|---|---|
| Issuance Domain | /neo-lc/issue, /neo-lc/amend, /neo-lc/cancel | Creation, modification, and cancellation of neo-LC instruments. Handles multi-party digital signatures and Hash-Chain registration. |
| Presentation Domain | /presentation/submit, /presentation/validate, /presentation/status | Document submission, AI-assisted pre-screening, eUCP compliance validation, and presentation status tracking. |
| Identity Domain | /identity/kyb, /identity/verify, /identity/consent | KYB verification requests, identity attestation queries (Ghana Card, DIATF, LEI, MANSA), and consent record management. |
| Compliance Domain | /compliance/screen, /compliance/score, /compliance/override | Sanctions screening, risk scoring, TBML pattern detection, and human-in-the-loop override management. |
| Settlement Domain | /settlement/instruct, /settlement/confirm, /settlement/reconcile | Payment instruction routing, settlement confirmation, Nostro-Lite balance management, and end-of-day reconciliation. |
| Observability Domain | /observe/dashboard, /observe/alert, /observe/audit | Real-time dashboards, anomaly alerts, and audit-trail queries for participants, programme governance, and regulators. |

## 5.2 Event-Driven Choreography

Rather than imposing a rigid, centrally controlled workflow, the Neofingo orchestration model uses event-driven choreography. Each significant action - neo-LC issuance, document submission, compliance flag, settlement instruction - emits an event to a message broker. Subscribed participants receive only the events relevant to their role and their consent-gated data access rights.

This approach confers three advantages. First, it is resilient: if one participant's system is temporarily offline, events queue and replay upon reconnection without corrupting the transaction state. Second, it is extensible: new participants or services can subscribe to the event stream without requiring changes to existing integrations. Third, it respects data sovereignty: events carry only the metadata needed for routing; the underlying data is accessed through authenticated API calls governed by the consent framework.

## 5.3 API Versioning and Backward Compatibility

All Neofingo APIs follow semantic versioning (major.minor.patch). Non-breaking changes (new optional fields, additional response metadata) increment the minor version. Breaking changes (field removal, structural changes) increment the major version. The gateway maintains parallel support for at least two major versions at all times, providing a minimum 12-month deprecation window to allow participants to migrate. This is critical for a multi-jurisdictional protocol: different institutions will upgrade their integrations at different speeds, and the orchestration layer must accommodate that variance without forcing synchronised deployments.

# 6. Data Sharing Framework: Who Shares What, When, and With Whom

The viability of the Neofingo protocol depends on the willingness and ability of diverse actors - across jurisdictions, institutional types, and regulatory regimes - to share data in structured, timely, and legally compliant ways. This section specifies the data sharing rules with the granularity required for implementation, drawing on best practice from digital public infrastructure worldwide.

> *Governing Principle: Data sharing under Neofingo follows the doctrine of minimum necessary disclosure. No actor receives more data than is required to perform their specific role at their specific stage of the transaction lifecycle. Consent is explicit, purpose-limited, and revocable. Cross-border transfers are governed by Standard Contractual Clauses (SCCs) embedded in participant agreements.*

## 6.1 Data Categories

All data flowing through the Neofingo protocol falls into one of six categories, each with distinct sensitivity levels, consent requirements, and access rules.

| Category | Examples | Sensitivity | Default Sharing Rule |
|---|---|---|---|
| Trade Data | Goods description, quantity, value, Incoterms, shipment schedule, purchase order details | Standard | Shared with all transaction counterparties upon neo-LC issuance |
| Identity Data | Entity name, LEI, national ID references, beneficial ownership, registered address | Enhanced | Shared only with parties performing KYC/KYB functions under explicit consent |
| Financial Data | Credit scores, account balances, transaction history, risk assessments | Restricted | Shared only with issuing/confirming institutions and DFI guarantee providers under separate financial data consent |
| Compliance Data | Sanctions screening results, PEP flags, adverse media hits, TBML indicators | Restricted | Shared only with compliance functions of regulated participants; aggregate (anonymised) data available to programme governance |
| Document Data | Invoices, bills of lading, certificates of origin, inspection reports, insurance certificates | Standard | Shared with all transaction counterparties as part of eUCP presentation; hash references shared with all network participants |
| Operational Data | API logs, latency metrics, error rates, system health indicators | Internal | Shared only with Neofingo network operations and, in aggregate, with the Programme Governance Board |

## 6.2 Data Flows by Transaction Stage

The following specifies, for each stage of the neo-LC lifecycle, exactly which data flows between which actors, under which consent basis, and via which API domain.

### 6.2.1 Stage 1: Application and Origination

**From Exporter to African Fintech Distributor:** The exporter provides trade data (e.g. goods, value, & buyer details) and identity data (e.g. business registration, Ghana Card, & beneficial ownership). Consent basis: contractual necessity for trade finance application. The fintech ingests this data, performs initial KYB verification against local registers, and structures it into an ISO 20022 trade initiation message.

**From African Fintech to Neofingo Gateway:** The fintech transmits the structured trade initiation message via the Issuance Domain API (/neo-lc/issue). The message includes trade data, a hash reference to the exporter's identity attestation (not the raw identity data itself), and the fintech's own attestation that local KYB has been completed to the standard specified in the programme's bilateral Data Processing Agreement.

**From Neofingo Gateway to Issuing Neobank (UK):** The gateway routes the issuance request to the nominated UK institution. The neobank receives the full trade data and the fintech's KYB attestation. If the neobank's risk engine requires additional identity or financial data to complete its own KYC/AML assessment, it requests that data through the Identity Domain API, triggering a consent request to the exporter via the Nomi interface. The exporter may grant or withhold consent for each specific data field.

### 6.2.2 Stage 2: Risk Assessment and Issuance

**From Issuing Neobank to Compliance Services:** The neobank submits counterparty identifiers to the Compliance Domain API (/compliance/screen) for sanctions and PEP screening. The compliance service returns pass/fail/review results. Underlying screening data (the specific watchlist entries matched) is retained in the compliance service and shared with the neobank's compliance officer only; it does not flow to other transaction parties.

**From MANSA/Credit Bureaux to Issuing Neobank (via Gateway):** Where the exporter has consented, the gateway retrieves corroborative identity and creditworthiness data from participating identity and integrity repositories, such as the AfCFTA Hub, and relevant credit reference bureaux. This data is shared with the issuing neobank under a Financial Data Consent and is used solely for the purpose of risk-pricing the neo-LC. It is not stored by the gateway beyond the life of the transaction.

**From Issuing Neobank to All Parties:** Upon approval, the neobank issues the neo-LC and transmits it through the gateway to the advising/confirming institution and the exporter. The issued neo-LC (trade data and instrument terms) is shared with all transaction counterparties. The underlying risk assessment is not shared; only the binary issuance decision and the instrument terms are visible to the beneficiary.

### 6.2.3 Stage 3: Document Presentation

**From Exporter to Nomi/Gateway:** The exporter uploads trade documents through the Nomi interface. Each document is hashed at the point of upload and registered on the Hash-Chain. The Nomi AI engine validates the document set against the neo-LC terms (Presentation Domain API). Document data (the actual content of invoices, bills of lading, etc.) is shared with the issuing and confirming institutions as part of the eUCP presentation. Hash references are shared with all network participants for integrity verification, but the document content itself is accessible only to the parties specified in the neo-LC.

**From Nomi to Exporter (Feedback Loop):** Where the AI engine detects discrepancies, it returns plain-language explanations and suggested corrections to the exporter through the Nomi interface. This data is private to the exporter and their nominated fintech advisor; it is not shared with the issuing bank or any other party until the exporter formally submits the corrected presentation.

### 6.2.4 Stage 4: Settlement

**From Issuing Neobank to Settlement Rails:** Upon acceptance of the presentation, the neobank transmits a settlement instruction through the Settlement Domain API. The instruction includes payment amount, currency, beneficiary account details (Nostro-Lite account reference for the African fintech, or direct account for the exporter), and the settlement rail to be used. Account details are shared only between the settlement counterparties and the payment rail operator; they are not visible to other transaction participants.

**From Settlement Rails to All Parties (Confirmation):** Settlement confirmation events are broadcast to all transaction counterparties, confirming that funds have moved. The confirmation includes the amount, currency, and timestamp, but not the underlying account details of the receiving party.

### 6.2.5 Stage 5: Post-Trade and Credit Enrichment

**From Neofingo Archive to Exporter's Portable Credit Profile:** With the exporter's explicit consent (separate from the transaction consent), the completed transaction record - outcome, value, settlement time, discrepancy rate, compliance status - is distilled into a structured credit data point and added to the exporter's portable credit profile within the Neofingo network. This profile is owned by the exporter and can be shared, at their discretion, with any future lender or trade finance provider on the network. The mechanism draws direct inspiration from the credit portability partnership between Nova (US) and XDSData (Ghana), extending the principle from consumer credit to trade finance.

## 6.3 Cross-Border Data Transfer Mechanisms

All cross-border data transfers within the Neofingo protocol are governed by a library of Standard Contractual Clauses (SCCs) embedded in the bilateral Data Processing Agreements that each participant signs upon network accession. The SCCs align with UK adequacy

requirements (for UK-Ghana data flows), the EU Standard Contractual Clauses (where EU-based participants are involved), and the emerging African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).

Data residency requirements are respected through a distributed architecture: the Neofingo Gateway does not centralise raw data. Instead, it holds hash references, routing metadata, and consent records. The underlying data remains in the jurisdiction of the institution that generated it, accessible to authorised counterparties via authenticated API calls. This architecture means that a Ghanaian exporter's identity data never leaves Ghana; the UK neobank accesses a verified attestation of that data, not the data itself. Similarly, the UK neobank's risk assessment never leaves the UK; the exporter receives an issuance decision, not the underlying credit model output.

## 6.4 Lessons from Global Digital Public Infrastructure

The Neofingo data sharing framework draws on four international precedents.

**India's Unified Payments Interface (UPI) and Account Aggregator Framework:** UPI demonstrated that a thin, interoperable protocol layer can unlock massive transaction volumes without centralising data. The Account Aggregator framework extended this principle to financial data sharing, establishing a consent-based architecture in which data flows between Financial Information Providers and Financial Information Users through licensed intermediaries. Neofingo adopts the same structural logic: the protocol orchestrates; the data remains distributed.

**UK Open Banking (JROC/Future Entity):** The UK's Open Banking framework proved that API-based, consent-gated data sharing between regulated institutions can function at scale. Neofingo extends this model from domestic retail banking to cross-border trade finance, inheriting the API standards (RESTful, OAuth 2.0) and the consent management architecture whilst adding the multi-jurisdictional and multi-currency dimensions that trade finance requires.

**Estonia's X-Road:** X-Road's principle of 'once only' data provision - where an entity provides a data point to one registry, and all authorised consumers query that single source rather than requiring the entity to re-submit - informs the Neofingo identity layer. An exporter registers their business details once; all subsequent verifications query that registration rather than demanding fresh documentation.

**Singapore's Trade Data Exchange (SGTraDex):** SGTraDex demonstrated that trade-specific data sharing infrastructure can reduce cargo dwell times and documentation costs by connecting supply chain actors through standardised data protocols. Neofingo extends this logic from a single-jurisdiction trade facilitation platform to a cross-border corridor connecting two distinct regulatory environments.

# 7. The Neofingo Hash-Chain: Cryptographic Integrity Without Blockchain Dependency

One of the most common misconceptions in digital trade finance discourse is that document integrity and audit-trail immutability require a blockchain or distributed ledger. They do not. What they require is a cryptographic mechanism that makes tampering detectable. The Neofingo Hash-Chain provides exactly that, using a straightforward construction that is well-understood, computationally efficient, and deployable without the operational complexity, latency overhead, or governance challenges of a blockchain network.

## 7.1 Construction

The Neofingo Hash-Chain operates as follows. Every event in the protocol - document submission, neo-LC issuance, compliance screening result, settlement instruction, consent grant or revocation - generates a record. That record is hashed using SHA-256, producing a 256-bit digest. The hash of each new record incorporates the hash of the immediately preceding record, creating a sequential chain in which any alteration to any historical record would produce a cascade of hash mismatches detectable by any party that simply invokes their right to inspect the chain.

Formally: for each event E at position n, the hash H(n) is computed as H(n) = SHA-256(E(n) || H(n-1)), where || denotes concatenation and H(0) is a genesis value published at protocol initialisation. This is, in essence, the same mathematical construction that underpins blockchain technology, but implemented without the consensus mechanism, distributed replication, and tokenisation apparatus that blockchains add. The chain is maintained by the Neofingo Gateway and rendered visible on demand to participating institutions, each of which independently verifies the chain's integrity using an innovative *integrity inspection mechanism*.

## 7.2 Tamper Evidence and Dispute Resolution

If any actor attempts to alter a historical record - modifying an invoice amount after submission, backdating a compliance check, or editing a shipment date - the hash of the altered record will no longer match its stored value, and every subsequent hash in the chain will also fail verification. This property means that tampering is not prevented (no system can prevent a determined actor from modifying their own records) but is rendered cryptographically provable and operationally worthless. Any discrepancy between a party's claimed record and the Hash-Chain reference is detectable and evidentiarily significant.

In the event of a dispute, the Neofingo system generates an Evidence Bundle - a self-contained, cryptographically signed package containing the complete transaction record, all associated hashes, and the relevant segment of the Hash-Chain. This bundle is designed to be court-admissible under the UK's Civil Evidence Act 1995 and equivalent statutes in participating African jurisdictions.

## 7.3 Time-Stamping and Non-Repudiation

Each Hash-Chain entry is time-stamped by a trusted Time-Stamping Authority (TSA) conforming to RFC 3161 and the ETSI EN 319 422 standard. The TSA is operated independently of the Neofingo Gateway, ensuring that time-stamps cannot be manipulated by any network participant, including the protocol operator. This provides non-repudiation: a party cannot deny having submitted a document or made a decision at the time recorded by the Hash-Chain.

## 7.4 Multi-Party Verification

The Hash-Chain is not a single, centrally held ledger. Replicas are maintained by specified trust nodes of the key regulated participants. TrustNodes include networks of issuing neobanks, confirming African institutions, and any DFI guarantee providers. Each TrustNode periodically confirms chain integrity. If any replica diverges, the discrepancy can be flagged during an integrity inspection event, and the affected transactions, if under dispute, are quarantined. The Programme Governance Board adjudicates in such disputes. This multi-party verification provides good enough immutability and practical system integrity without the overhead of a blockchain consensus protocol.

## 7.5 Relationship to Distributed Ledger Technology

The Neofingo Hash-Chain is designed to function entirely without a distributed ledger. No permissioned or permissionless blockchain is required for the protocol to deliver document integrity, tamper evidence, or audit-trail immutability.

Where participants choose to deploy a permissioned ledger - such as Hyperledger Fabric or R3 Corda - the Hash-Chain can be anchored to the ledger's blocks at configurable intervals (e.g., every 100 events or every hour), providing an additional layer of immutability backed by the ledger's own consensus mechanism. This is particularly valuable for two use cases: constructive possession of electronic bills of lading under ETDA 2023 (where the distributed ledger provides the 'reliable system' required by the Act's possession requirements); and multi-corridor deployment (where anchoring to a shared ledger provides cross-corridor integrity verification without requiring bilateral trust between gateway operators in different corridors).

The key design principle is optionality. Permissioned ledger integration enhances the protocol where the context warrants it. It never constrains the protocol where the context does not.

# 8. Optional Permissioned Ledger Integration

This section specifies how permissioned distributed ledger technology may be integrated with the Neofingo protocol where participants determine that it adds value beyond what the Hash-Chain alone provides.

## 8.1 Applicable Use Cases

**Constructive Possession under ETDA 2023:** The UK's Electronic Trade Documents Act requires that, for an electronic trade document to be 'possessed', the document must be held on a 'reliable system' that prevents more than one person from exercising control over the document at any one time. A permissioned ledger, with its inherent single-state consensus, provides a natural implementation of this requirement. When a neo-LC includes an electronic bill of lading, the eBL's control token can be tracked on the permissioned ledger, ensuring that constructive possession transfers are atomic and verifiable.

**Multi-Corridor Anchoring:** As Neofingo expands beyond the UK-Ghana corridor to additional country pairs, a shared permissioned ledger provides a common integrity anchor across corridors. Each corridor's Hash-Chain periodically anchors its state to the shared ledger, enabling cross-corridor audit and verification without requiring each corridor to trust the other's gateway operator bilaterally.

**Tokenised Trade Finance Assets:** In future iterations, neo-LCs or fractions thereof may be tokenised for secondary market distribution - enabling institutional investors to purchase trade finance exposure as a liquid asset class, a trajectory identified by the ITFA Trade Finance Investment Ecosystem group. A permissioned ledger provides the infrastructure for tracking token issuance, transfer, and redemption with regulatory-grade auditability.

## 8.2 Integration Architecture

Permissioned ledger integration is implemented as a sidecar service, not as a replacement for the Hash-Chain. The Hash-Chain remains the primary integrity mechanism. The ledger sidecar subscribes to the Hash-Chain's event stream and periodically writes anchor points (batch hashes) to the ledger. Participants who do not operate ledger nodes continue to verify integrity through the Hash-Chain alone; participants who do operate nodes gain the additional assurance of ledger-backed immutability.

This sidecar architecture means that the core protocol is entirely ledger-agnostic. The sidecar can connect to Hyperledger Fabric, R3 Corda, or any other permissioned ledger that supports the required hash-anchoring API. The choice of ledger technology is a deployment decision, not a protocol decision.

# 9. Cybersecurity Architecture and Guardrails

A cross-border trade finance protocol connecting European capital pools with African SME ecosystems presents a substantial attack surface. The Neofingo cybersecurity architecture is designed in depth, applying the principle of defence at every layer.

## 9.1 Threat Model

The protocol's threat model identifies five primary adversary categories: external attackers seeking to exploit API vulnerabilities or intercept data in transit; insider threats from compromised participants or rogue employees; state-affiliated actors targeting the corridor for intelligence or disruption; fraud rings exploiting the trade finance workflow to submit fictitious invoices or inflate values; and supply chain attacks targeting the software dependencies of the protocol's infrastructure. Each category is addressed through a layered control set.

## 9.2 Transport Security

All data in transit is encrypted using TLS 1.3 with forward secrecy. Mutual TLS (mTLS) is required for all API communications between the Neofingo Gateway and participant systems, ensuring that both sides of every connection are cryptographically authenticated. API requests are signed using RSA-2048 or ECDSA P-256 digital signatures, providing non-repudiation at the message level in addition to the transport-level encryption.

## 9.3 Data-at-Rest Protection

All persistent data stores within the protocol infrastructure are encrypted using AES-256 with keys managed through a Hardware Security Module (HSM) conforming to FIPS 140-2 Level 3. Key rotation occurs on a quarterly cycle, with emergency rotation capability for incident response. The Hash-Chain's cryptographic keys are air-gapped from application keys, ensuring that a compromise of the application layer does not expose the integrity mechanism.

## 9.4 API Security

Beyond OAuth 2.0 and mTLS authentication, the API gateway enforces rate limiting, payload validation, and anomaly detection on every endpoint. Input validation rejects malformed requests before they reach application logic, mitigating injection attacks. API keys and tokens are rotated on configurable schedules and are scoped to specific domains and operations - a participant's identity verification token cannot be used to invoke settlement endpoints.

## 9.5 Fraud Detection and TBML Controls

Trade-based money laundering (TBML) presents a specific threat to any digital trade finance corridor. The Neofingo protocol incorporates pattern recognition algorithms trained on known TBML typologies: over- and under-invoicing, multiple invoicing of the same shipment, carousel fraud, and fictitious trade transactions. These algorithms operate at the Compliance

Domain layer and generate risk flags that are routed to the human-in-the-loop compliance function. False positive management is a critical design consideration: the algorithms are tuned to minimise false positives that would disproportionately affect SME exporters while maintaining high detection sensitivity for genuine TBML patterns.

## 9.6 Incident Response and Business Continuity

The protocol's incident response framework follows the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) and is supplemented by specific playbooks for each identified threat category. A cyber incident affecting any participant triggers a mandatory notification to the Programme Governance Board within four hours, with concurrent notification to relevant regulators (Bank of Ghana, FCA, & PRA, for instance) as applicable. Business continuity provisions include geographic redundancy for gateway infrastructure, automated failover, and the ability to operate in degraded mode (store-and-forward messaging with delayed settlement) during disruptions.

# 10. The Nomi AI Interface: Compliance Automation and User Guidance

Nomi is the AI-enabled interface through which SME exporters, fintech distributors, and other non-specialist participants interact with the Neofingo protocol. Its design philosophy is radical simplification: Nomi translates the dense, specialist language of international trade finance into guided, conversational workflows that require no prior expertise from the user.

## 10.1 Functional Architecture

Nomi operates as a modular AI service comprising three components. The Conversational Guide uses natural language processing to walk users through LC creation, document preparation, and submission in plain English (with French and local language support planned). The Compliance Engine performs automated document validation against eUCP 2.1 rules, cross-document consistency checks, and pre-submission discrepancy detection. The Knowledge Base maintains an up-to-date repository of trade finance rules, commodity-specific documentation requirements, and jurisdiction-specific regulatory guidance, enabling Nomi to provide contextually relevant advice in real time.

## 10.2 Model Governance Under PRA SS1/23

The AI models powering Nomi are subject to the full rigour of the PRA's model risk management framework. Each model is inventoried with a documented purpose statement, input data specification, and performance benchmark. Validation is performed by an independent function (not the development team) on a quarterly cycle and upon any material change to model inputs or architecture. Backtesting against historical transaction data verifies that the model's discrepancy detection rates and risk scores remain within tolerance bands. Data lineage is tracked end to end, from source data through feature engineering to model output.

Crucially, Nomi never makes a final decision. Every compliance determination, risk score, and document validation output can be overridden by a human operator at the issuing institution. Nomi's role is to compress the 70-80 per cent discrepancy rate of paper presentations to under 10 per cent, allowing human attention to concentrate on the genuinely ambiguous cases rather than being consumed by routine clerical errors.

## 10.3 Accessibility and Inclusion Design

Nomi's interface is designed for the conditions in which most African SME exporters actually operate. The mobile-first interface runs efficiently on low-bandwidth connections and mid-range Android devices. A lightweight USSD fallback supports basic status queries and approval functions from feature phones. Document upload supports camera capture with automatic orientation correction and OCR enhancement for hand-written or poor-quality printed documents. Language support prioritises English and French, with Twi, Hausa, and Krio planned for subsequent phases.

# 11. Regulatory Navigation: Operating Within Existing Licence Perimeters

A defining design choice of the Neofingo protocol is that it does not require a licence in any jurisdiction to operate. Neofingo itself does not hold client funds, issue credit instruments, or take deposit or insurance risk. It is an orchestration protocol - a set of data standards, API specifications, and process rules - that enables already-licensed institutions to interoperate more effectively.

## 11.1 The Regulatory Positioning

In UK regulatory terms, the Neofingo protocol is best understood as a technology infrastructure provider to regulated firms, analogous to SWIFT in the messaging domain or CLS in the settlement domain. The regulated activities - issuing letters of credit, holding deposits, processing payments, performing credit intermediation - are performed by FCA- and PRA-authorised institutions (banks, neobanks, EMIs) using their existing permissions. Neofingo provides the technical rails on which those activities run, but it does not itself perform them.

In Ghanaian regulatory terms, the protocol operates within a prospective Bank of Ghana's policy sandbox - a supervised, controlled governance environment in which the technology, processes, and commercial arrangements can be tested and refined with full regulatory visibility. This is a deliberate choice of a policy sandbox over a regulatory sandbox: the distinction matters materially. A regulatory sandbox typically implies that the participant is operating under a temporary, limited licence for activities it would otherwise be unable to perform. A policy sandbox, by contrast, implies that the participant is operating within existing regulatory perimeters, and the sandbox provides a structured framework for the regulator to observe, learn from, and refine the policy environment around an activity that is already lawful but novel in its application.

## 11.2 How Neofingo Supports Regulatory Objectives

For central banks and financial regulators, the protocol provides several direct benefits. It creates a structured, observable channel through which cross-border trade finance activity can be monitored in real time - a significant improvement over the opacity of bilateral correspondent relationships. It generates granular data on SME trade finance demand, approval rates, discrepancy patterns, and settlement performance, equipping regulators with the empirical basis for evidence-led policy development. And it enables regulators to steer regulated entities toward developmental objectives - accelerating SME export finance, deepening local-currency settlement, building credit histories for underserved segments - without those entities departing from their existing compliance obligations.

## 11.3 Licence-Holder Interoperability Matrix

The following matrix maps each participant type to their existing licence, the activities they perform within the Neofingo protocol, and the regulatory regime under which those activities fall.

| Participant | Licence Held | Activities in Neofingo | Regulatory Regime |
|---|---|---|---|
| UK Neobank / Authorised Bank | FCA/PRA Full Authorisation | Issue/confirm neo-LCs, hold settlement accounts, screen for AML/sanctions | PRA Rulebook, UK MLR 2017, JMLSG, SS1/23 |
| UK EMI | FCA EMI Authorisation | Process payments, hold e-money, manage FX conversion | EMRs 2011, PSRs 2017, FCA AML guidance |
| Ghanaian Bank | BoG Banking Licence | Advise/confirm neo-LCs, perform local KYB, manage cedis settlement | Banks and SDIs Act 2016, BoG AML/CFT Directive |
| African Fintech (PSP/Lender) | BoG or relevant national licence | Originate exporters, ingest trade data, operate local payment rails | Payment Systems and Services Act 2019, BoG sandbox terms |
| Neofingo Protocol | None required | Orchestrate data flows, maintain Hash-Chain, operate API Gateway | Technology infrastructure provider; contractual governance |

# 12. Interoperability with Global Digital Public Infrastructure

Neofingo is designed from the outset as one corridor within a larger, emerging global architecture of digital public infrastructure for trade. Its standards choices, data formats, and protocol design are intended to ensure that any Neofingo corridor can interoperate with other DPI initiatives without bespoke integration work.

## 12.1 AfCFTA Hub Integration

The AfCFTA Hub, hosted by the AfCFTA Secretariat in Accra, serves as the continental conductor for intra-African trade facilitation. Neofingo integrates with the Hub at multiple levels: rules-of-origin verification (enabling diagonal accumulation across AfCFTA member states), tariff schedule queries, and trade data exchange for regulatory reporting. Transactions passing through the Neofingo corridor and routed via the AfCFTA Hub demonstrate, within a real-world operational context, that the architecture works - providing the AfCFTA Secretariat with a reference implementation for digital trade facilitation that other corridors can adopt.

## 12.2 PAPSS Connectivity

The Pan-African Payment and Settlement System, operated by Afreximbank, provides the local-currency settlement rail for intra-African payment legs. Neofingo's settlement layer can interface with PAPSS through ISO 20022-compliant payment initiation messages, enabling the Ghanaian exporter to receive payment in Ghana cedis without the neobank needing to maintain a cedis nostro account. This is a critical enabler for multi-country triangular trade - a Ghanaian processor importing raw materials from Côte d'Ivoire for re-export to the UK can settle both legs through the corridor.

## 12.3 SWIFT and gpi Compatibility

The protocol's messaging layer is fully compatible with SWIFT's global payments innovation (gpi) framework. Where participants prefer to use SWIFT for cross-border payment legs, the Neofingo Gateway translates ISO 20022 settlement instructions into gpi-compliant payment orders and tracks their status through SWIFT's tracking service. This ensures that Neofingo does not require participants to abandon existing payment infrastructure - it enhances and orchestrates what already exists.

## 12.4 Open Banking APIs and Future Entity (UK)

The UK's Open Banking architecture, now evolving under the JROC Future Entity, provides a precedent and a technical foundation for consent-based data sharing between regulated institutions. Neofingo's consent management protocols are designed to be compatible with Open Banking consent flows, enabling UK neobanks to re-use their existing Open Banking API infrastructure for Neofingo data sharing without building parallel systems.

# 13. Implementation Sequencing and Technical Roadmap

## 13.1 Phase 1: Foundation (Months 1 - 6)

Deploy the Neofingo Gateway with core API domains (e.g. Issuance, Presentation, & Identity). Establish the Hash-Chain with genesis *trigger* and initial TSA integration. Onboard two to three UK neobanks and three to five Ghanaian fintech distributors as pilot participants. Launch the Nomi AI interface in English with basic document validation capabilities. Operate within the Bank of Ghana's policy sandbox with full supervisory reporting.

## 13.2 Phase 2: Deepening (Months 7 - 12)

Add Compliance and Settlement Domain APIs. Integrate AfCFTA Hub, Identity Service Framework, and interbank/interfintech payments network connections. Deploy the Nostro-Lite settlement model with initial DFI guarantee backing. Expand Nomi's validation coverage to include commodity-specific document sets (e.g. cocoa, shea, & cashew). Begin credit enrichment data collection for exporter portable profiles.

## 13.3 Phase 3: Scaling (Months 13 - 24)

Extend the corridor to Nigeria and Sierra Leone. Deploy optional permissioned ledger sidecar for eBL constructive possession. Launch secondary market capabilities for neo-LC distribution. Integrate additional identity providers and credit bureaux. Target: 2,000 SMEs onboarded, $200 million annualised corridor volume, processing time compressed to 48-72 hours for standard flows.

## 13.4 Phase 4: Continental Integration (Months 25 - 36)

Extend to Kenya and East African corridors. Anchor multi-corridor Hash-Chain to shared permissioned ledger. Enable triangular trade flows (e.g., UK buyer, Ghanaian processor, Ivoirian raw material supplier) with diagonal accumulation under AfCFTA rules. Begin engagement with Gulf and East Asian import markets. Target: five active corridors, 10,000 SMEs onboarded, $1 billion annualised corridor volume.

# Appendix A: API Endpoint Reference Schema

The following provides a representative schema for the core API endpoints. Full OpenAPI 3.0 specifications will be published as a separate technical document upon protocol launch.

| Endpoint | Request Body (simplified) | Response (simplified) |
|---|---|---|
| POST /neo-lc/issue | { applicant_lei, beneficiary_id, amount, currency, documents_required[], shipment_terms, expiry_date, conditions[] } | { neo_lc_id, status, hash_chain_ref, issued_at } |
| POST /presentation/submit | { neo_lc_id, documents[{ type, hash, content_ref }], submitter_id } | { presentation_id, validation_result, discrepancies[], hash_chain_ref } |
| GET /identity/verify | { entity_id, verification_sources[] } | { entity_id, verification_status, attestations[], consent_ref } |
| POST /compliance/screen | { entity_ids[], transaction_ref } | { screening_results[{ entity_id, status, flags[] }], timestamp } |
| POST /settlement/instruct | { neo_lc_id, amount, currency, beneficiary_account, rail } | { instruction_id, status, estimated_settlement, hash_chain_ref } |

# Appendix B: Data Dictionary and ISO 20022 Mapping

| Data Element | ISO 20022 Identifier | Usage in Neofingo |
|---|---|---|
| Trade Initiation | tsmt.019 | Purchase order data from buyer, initiating the neo-LC application flow |
| Credit Transfer | pain.001 / pacs.008 | Fund movement instructions for settlement legs |
| Trade Status | tsmt.025 | Notification of trade lifecycle events (issuance, presentation, acceptance, settlement) |
| Bank Statement | camt.053 | Nostro-Lite account reconciliation and balance reporting |
| Invoice | remt.001 | Structured invoice data for document validation and presentation |
| Entity Identity | acmt.023 | Corporate identity verification requests and responses |

# Appendix C: Glossary of Technical Terms

| Term | Definition |
|---|---|
| AfCFTA | African Continental Free Trade Area - the continent-wide trade agreement creating a single market of 1.4 billion people |
| DPI | Digital Public Infrastructure - shared, open, interoperable technology systems that underpin societal functions at population scale |
| ETDA 2023 | Electronic Trade Documents Act 2023 (UK) - statute conferring legal equivalence to electronic trade documents |
| eUCP 2.1 | Electronic Uniform Customs and Practice - ICC supplement to UCP 600 governing electronic presentation under documentary credits |
| Hash-Chain | A sequential cryptographic structure in which each record's hash incorporates the previous record's hash, creating tamper-evident continuity |
| ISO 20022 | The international standard for financial messaging, providing rich, structured data formats for payments and trade finance |
| LEI | Legal Entity Identifier - a 20-character alphanumeric code that uniquely identifies entities engaged in financial transactions globally |
| MANSA | Afreximbank's centralised KYC repository for African entities, reducing duplicative due diligence |
| MLETR | UNCITRAL Model Law on Electronic Transferable Records - international framework for legal recognition of electronic negotiable instruments |
| neo-LC | Neofingo's programmable digital letter of credit, conforming to UCP 600, eUCP 2.1, and ETDA 2023 |
| Nomi | Neofingo's AI-enabled interface for user guidance, document validation, and compliance automation |
| Nostro-Lite | Neofingo's reduced-collateral settlement model, substituting data transparency for a portion of traditional cash collateral |
| PAPSS | Pan-African Payment and Settlement System - Afreximbank's infrastructure for instant, local-currency cross-border payments in Africa |
| SS1/23 | PRA Supervisory Statement 1/23 - model risk management principles for banks, governing AI and algorithmic decision-making |
| TBML | Trade-Based Money Laundering - the use of trade transactions to disguise the proceeds of crime |
| TSA | Time-Stamping Authority - an independent service providing cryptographically verifiable timestamps per RFC 3161 |
| UCP 600 | Uniform Customs and Practice for Documentary Credits - the ICC's globally adopted rules governing letters of credit |

**neofingo**

*Smart Finance. Shared Governance.*