

GSCX — Global Supply Chain Exchange

A fully-integrated, regulated digital exchange platform connecting importers, exporters, financiers, logistics providers, insurers and compliance officials across global trade corridors. Built on Node.js + Express + MariaDB with a zero-dependency security core and purpose-built infrastructure for payment abstraction, route optimisation, ledger reconciliation and compliance enforcement.

Version	1.0.0	Runtime	Node.js 22 / Express 4	Database	MariaDB	Member Roles	8 entity types	Crypto Settlement	MooChedda (secp256k1)	DB Tables	30 tables
Classification	Investor / Executive			Cybersecurity	Beezifi IDS + BC3 + AI Agents						

NAVIGATION

Table of Contents

Platform at a Glance

GSCX orchestrates the complete lifecycle of cross-border trade — from product listing and import/export order management through logistics, insurance, inspection and multi-rail payment settlement — all within a single compliance-enforced platform.

MEMBER ROLES 8 entity types Admin · Remitter · Importer · Exporter Transport · Insurance · Bank · Inspector	DATABASE TABLES 30 tables Full relational schema with FK constraints + AI layer	API ENDPOINTS 120+ REST routes CRUD + workflow + crypto + AI + infrastructure layers
PAYMENT RAILS 6 rails ACH · SWIFT · SEPA · WIRE · INTERNAL · CRYPTO	INFRASTRUCTURE SERVICES 6 layers Abstraction · Routing · Reconciliation · Compliance · Crypto · AI	SECURITY FEATURES 9 mechanisms Passwords · TOTP · OTP · Sessions · OFAC Beezifi IDS · IDS Endpoint · BC3 · AI Agents
TRADE DOCUMENTS 10+ document types AWB · BOL · LC · Cert · POD · Inspection Reports	COMPLIANCE CHECKS Real-time Every payment gated by compliance middleware	CRYPTO SETTLEMENT MooChedda Self-custody wallets · USDC/USDT · secp256k1 signing Hosted invoices · ACH/Wire on-ramp · Live pricing

Eight Specialised Member Roles

Each role type has dedicated onboarding workflows, purpose-built data structures, compliance checks and a full-featured operational center. Members can hold multiple roles simultaneously.



Remitter

Initiates cross-border money transfers with full beneficiary management. Supports bank, crypto and internal recipients. Every transfer passes OFAC screening and is gated by the compliance engine before processing.

Beneficiary management OFAC screening

Multi-rail payout Purpose codes

Source of funds



Importer

Manages the full inbound goods lifecycle: HS code classification, customs review, IOR designation, duty payment and regulatory declarations (FDA, FCC, USDA). Orders progress through a structured DRAFT → CLEARED status workflow.

HS codes & classification IOR designation

Customs workflow Duty payer config

Incoterms FDA/FCC/USDA flags



Exporter

KYB-verified entity profile (legal name, registration, tax ID, beneficial owners) with shipment creation covering ECCN dual-use controls, export license tracking and payout account management for multi-currency disbursement.

KYB profile ECCN / dual-use

Export licenses Payout accounts

OFAC screening Sanctions confirmed



Transport Provider

Full logistics tracking from label creation to proof of delivery. Supports AIR/SEA/COURIER/RAIL/ROAD modes with AWB, BOL, customs status tracking, shipment event timeline, charges/duties management and POD capture (recipient, signature, photo).

AWB / BOL Event timeline Customs status

Charges & duties Proof of delivery

Multi-mode



Insurance Provider

End-to-end cargo risk coverage: quote generation with premium calculation, policy issuance with PDF certificate URLs, risk level monitoring (LOW/MEDIUM/HIGH/FLAGGED) and structured claims processing with financial payout tracking.

Quote generation Policy issuance

Certificates Risk monitoring

Claims processing ALL_RISK / NAMED_PERILS



Bank

Full-stack banking operations: multi-type account management (Operating/Custodial/Escrow/Trust), multi-rail transaction processing, FX quote and execution, compliance flag issuance with AML/sanctions controls and account freeze/closure.

Account management SWIFT/ACH/SEPA/WIRE

FX quotes Compliance flags Escrow/Trust

Balance ledger



Inspector

Provides structured verification data used to gate payment release. Submits inspection reports (PASS/FAIL/CONDITIONAL_PASS), uploads photo/video evidence, logs typed defects with severity levels and issues approval signals that directly trigger or block fund release.

Inspection reports PASS / FAIL signal

Photo/video evidence Defect classification

Approval gating Severity tiers



Administrator

Platform governance and operations. Manages member onboarding, KYC/KYB review and approval, OFAC screening, bilateral trade matching, bond/collateral management, reconciliation runs and payment route execution.

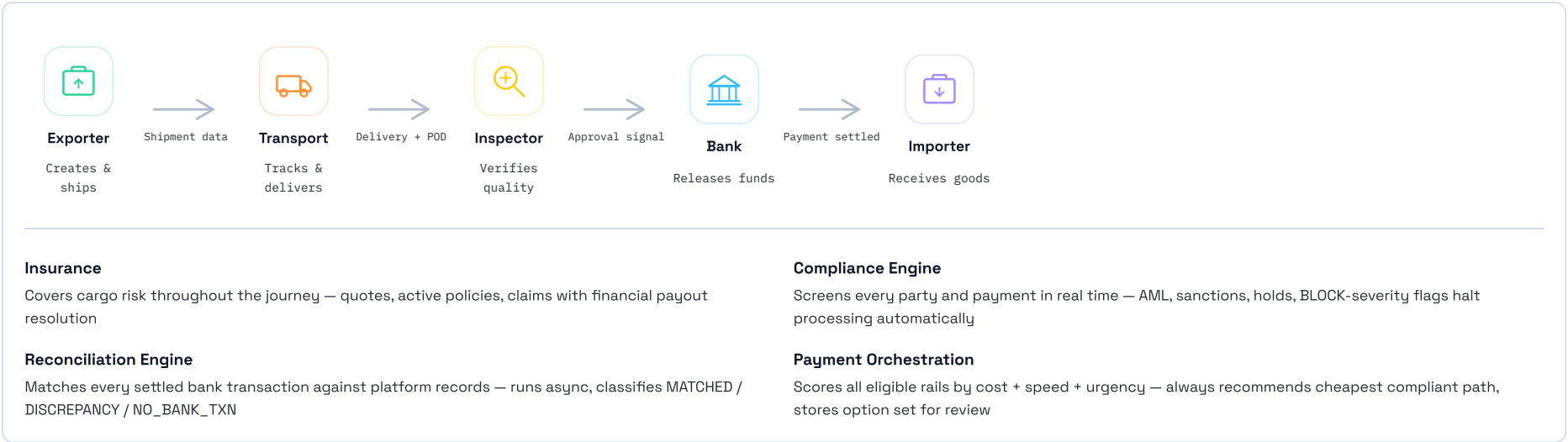
KYC/KYB review OFAC screening

Matching engine Reconciliation

Bond management Full access

How Entities Interact

A complete trade transaction moves through six interconnected role types. Four cross-cutting infrastructure services operate continuously beneath the flow to ensure compliance, optimise payments, cover risk and maintain ledger integrity.



What GSCX Does

Every major feature available on the platform, organised by functional domain.

Member Onboarding & KYC/KYB

Self-registration for all 8 role types, document upload, admin KYC/KYB review workflow, membership fee tracking, OFAC/sanctions status and license verification per entity type.

Import Order Management

Full import lifecycle: product details, HS codes, HS tariff classification, IOR designation, multi-modal shipping, port of entry, customs review workflow, regulatory declarations (FDA/FCC/USDA), duty payer configuration and payment method selection.

Export Shipment Management

KYB-verified exporter profile, shipment creation with ECCN dual-use export controls, export license management, restricted destination checks, sanctions confirmation and payout account assignment for proceeds disbursement.

Logistics & Transport Tracking

Shipment creation across AIR/SEA/COURIER/RAIL/ROAD with AWB and BOL numbers, real-time event timeline, customs status (PENDING/CLEARED/HELD), charge management for duties and brokerage, and full proof-of-delivery capture with recipient name, signature URL and photo URL.

Cargo Insurance

Quote generation with premium calculation, policy issuance (ALL_RISK / NAMED_PERILS / TOTAL_LOSS) with certificate URLs, risk level monitoring per policy (LOW/MEDIUM/HIGH/FLAGGED), and full claims processing with financial approval amounts, payout recipient designation and payout status tracking.

Pre-Shipment & Arrival Inspection

Structured inspection reports with PASS / FAIL / CONDITIONAL_PASS outcomes and SCHEDULED/IN_PROGRESS/COMPLETED status, photo and video evidence upload, typed defect logs (COSMETIC/FUNCTIONAL/CRITICAL) with percentage affected and severity classification, and approval signals that directly control payment release.

Banking & Multi-Rail Payments

Account management (OPERATING/CUSTODIAL/ESCROW/TRUST), transaction processing across SWIFT/ACH/SEPA/WIRE/INTERNAL/CRYPTO rails, FX quote and execution with spread/fee tracking, account freeze/closure controls and compliance hold management.

Cheapest-Path Payment Routing

Scores all eligible rails using: $\text{base cost} + \text{fee rate} \times \text{amount} + \text{settlement hours} \times \text{urgency weight}$. Three urgency tiers (STANDARD/EXPRESS/URGENT) penalise slow rails when time matters. Stores full scored option set for operational review before execution.

Ledger Reconciliation Engine

Full or scoped runs against Remittances, Import Orders, Export Shipments and Account Balances. Each record classified as MATCHED, NO_BANK_TXN or DISCREPANCY with sub-cent (\$0.01) tolerance. Async processing — responds 202 immediately, maintains permanent audit history per run.

Real-Time Compliance Engine

Four entity scopes (MEMBER/ACCOUNT/TRANSACTION/PAYMENT) with severity tiers LOW/MEDIUM/HIGH/BLOCK. BLOCK-severity flags reject remittances and bank transactions via Express middleware before processing. AML, SANCTIONS, HIGH_RISK, HOLD and ADDITIONAL_INFO_REQUIRED flag types with required-action fields and resolution workflow.

Product Hub & Marketplace

Exporter product listings with HS codes, ECCN, incoterms, country of origin, dual-use flags, MOQ, certifications, lead times, brand and model data. OFAC screening per product. Importer browsing and discovery with category and keyword search.

Matching Engine & Bond Management

Admin-controlled bilateral trade matching between any two platform entities with full transaction audit trail. Bond and collateral management for both GSCX-issued and member-submitted instruments, with compensation amounts and expiry tracking.

Crypto Center — MooChedda Integration

Any logged-in member can create or recover secp256k1 self-custody wallets, send USDC/USDT directly to any address, generate hosted payment invoices with line items and tax, and poll live MooChedda market prices. ACH/Wire on-ramp provides fiat-to-USDC deposit instructions. All transfers linked to platform orders (remittances, imports, invoices) for full audit trail.

What It's Built On

Deliberately minimal dependencies — the security and authentication core uses only Node.js built-ins.

BACKEND

Node.js 22 + Express 4

REST API, session management, middleware chain

MariaDB / mysql2

Relational store with FK-constrained schema, JSON columns

Native crypto module

PBKDF2 passwords, TOTP (RFC 6238), session tokens, IDs

Multer

KYC document upload handling

FRONTEND

Vanilla JS (ES2022)

Zero framework — state object + render() + event delegation

CSS Custom Properties

Dark/light theme switching, font scale, design tokens

Space Grotesk + IBM Plex Mono

Typography system loaded via Google Fonts

QRCode.js

Client-side TOTP QR code generation for 2FA setup

INFRASTRUCTURE

dotenv

Environment config: DB credentials, host, port

Content Security Policy

Zero inline styles — all styling via external CSS classes

setImmediate async processing

202 Accepted pattern for long-running reconciliation jobs

Schema auto-migration

ALTER TABLE IF NOT EXISTS — safe re-run on every startup

MooChedda SDK (built-in only)

secp256k1 ECDSA signing, BIP39 wallet creation/recovery, token transfers, hosted invoices — zero npm dependencies

Four Purpose-Built Services

These layers abstract payment complexity, optimise cost, enforce regulatory compliance and maintain ledger integrity — operating invisibly beneath every transaction.

Bank Abstraction Layer — Payment Rail Normalisation

- Normalises ACH, SWIFT, SEPA, WIRE, INTERNAL and CRYPTO into a single canonical payload structure
- Per-rail required field validation: `counterpartySwift` (SWIFT/SEPA), `counterpartyBank` (ACH/WIRE), `counterpartyAccount` (all)
- Currency constraints enforced: ACH USD-only, SEPA EUR-only, others multi-currency
- Amount ceiling enforcement: ACH capped at \$25M — auto-suggests WIRE or SWIFT for larger amounts
- Rail-specific metadata: SEC codes (ACH), MT103/MT202/MT202COV message types (SWIFT), SCT/SCT_Inst scheme (SEPA), wallet network (CRYPTO)
- Exposes `validate-only` endpoint for pre-flight checks without persisting a transaction

Payment Orchestration — Cheapest-Path Route Scoring

- Scores all eligible rails: $\text{baseCost} + \text{feeRate} \times \text{amount} + \text{settlementHours} \times \text{urgencyWeight}$
- Urgency tiers: STANDARD (0.5×), EXPRESS (1.5×), URGENT (4.0×) — slow rails penalised when time is critical
- Eligibility filters: currency compatibility, recipient type (BANK/CRYPTO/INTERNAL), rail-specific constraints
- Compliance check integrated into every route request — BLOCK-severity flags halt routing automatically
- Stores full scored option set so operations can review ranked alternatives before committing
- ROUTED → EXECUTED state transition with linked transaction ID for audit traceability

Ledger Reconciliation Engine

- Full or scoped runs: REMITTANCES, IMPORTS, EXPORTS, ACCOUNTS, or FULL covering all four
- Matches completed platform records against settled bank transactions per entity
- Three-outcome classification: MATCHED, NO_BANK_TXN, DISCREPANCY — with notes per entry
- Sub-cent tolerance: differences < \$0.01 treated as MATCHED to absorb rounding
- Account balance reconciliation: computes $\text{SUM}(\text{CREDIT}) - \text{SUM}(\text{DEBIT})$ vs `ledger_balance` field
- Async 202 pattern — responds immediately, updates run record on completion; full history retained indefinitely

Compliance Engine — Holds, Flags & Rejections

- Four entity scopes: MEMBER, ACCOUNT, TRANSACTION, PAYMENT — each independently flaggable
- Severity tiers: LOW, MEDIUM, HIGH, BLOCK — BLOCK automatically rejects the associated request
- Flag types: AML, SANCTIONS, HIGH_RISK, HOLD, ADDITIONAL_INFO_REQUIRED with required-action text fields
- Express middleware factory — wraps any route: `requireCompliance(getMemberId, getAccountId)`
- Currently gating: POST /remittances and POST /bank-transactions
- On pass: attaches `req.complianceResult` to the request for downstream inspection without re-querying
- Flags have resolution workflow: OPEN → UNDER_REVIEW → RESOLVED / ESCALATED

Crypto Settlement Layer — MooChedda

- Wallet creation via MooChedda API — returns secp256k1 keypair (130-char public address, 64-char private key hex, BIP39 mnemonic)
- Self-custody signing: platform builds DER-encoded SEC1 key from raw hex and signs with Node `crypto.createSign('SHA256')` — no secp256k1 npm package
- Token transfers: SHA-256 hash of `fromAddress + toAddress + amount + tokenSymbol` signed and submitted with timestamp
- Hosted invoices: line-item invoices with configurable tax rate, token preference and expiry — MooChedda returns a hosted payment URL
- Live market data: real-time USDT-denominated pricing updated from on-chain swap activity; registered token registry
- Fiat on-ramp: ACH and wire deposit instructions that credit USDC 1:1 with zero fees
- All transfers linked to platform records (remittances, imports, exports) via `linked_type / linked_id` for cross-ledger traceability

AI Platform Layer — Copilots & Intelligent Assistants

- **Form Copilot:** Converts plain-language descriptions into structured API payloads (remittance, import order, export shipment) with confidence scoring and missing-field highlighting
- **Compliance Copilot:** Summarises active compliance flags into risk assessments (LOW → CRITICAL), extracts required documents, and generates recommended analyst actions (hold, escalate, request info)
- **Reconciliation Copilot:** Analyses discrepancy reports — assesses match quality, performs root-cause analysis, suggests matching bank transactions, and recommends resolution steps
- **Payment Route Advisor:** Recommends optimal payment rail by scoring all eligible options against cost, settlement time, compliance status and risk — provides ranked alternatives with rationale
- Pluggable AI provider system — mock heuristic engine ships out-of-the-box; swappable with any external LLM via `AI_PROVIDER` env var
- All jobs tracked in `ai_jobs` (QUEUED → RUNNING → COMPLETED/FAILED) with full input/output JSON and model metadata retained indefinitely
- Artifacts stored with confidence scores (0.0–1.0) and an approval workflow — artifacts can be approved or rejected by a human reviewer before being acted upon
- Document indexing table (`ai_document_index`) supports chunked RAG retrieval for future semantic search over platform records

Defence in Depth

Nine distinct security mechanisms span application-layer authentication through host-based intrusion detection, network telemetry, and AI-driven threat response — forming a continuous security envelope from client to database.

Transport & Session Layer Cryptographically random 64-byte hex session tokens stored in an in-memory Map with explicit logout invalidation. Every protected route calls <code>requireSession()</code> before processing.
Password Hashing PBKDF2-SHA512 with 210,000 iterations and a 16-byte random salt per credential — implemented entirely via <code>crypto.pbkdf2</code>. No bcrypt or argon2 dependency.
TOTP Two-Factor Authentication RFC 6238-compliant TOTP implemented from scratch using <code>crypto.createHmac</code>. Generates Base32-encoded secrets, produces <code>otpauth://</code> URLs for authenticator apps, verifies with ± 1 step window for clock drift tolerance.
Email / SMS OTP Fallback Per-member OTP type configuration (NONE / EMAIL / SMS / TOTP). Short-lived numeric OTP codes stored on the member record. Configurable requirement flag per account — can be enforced after initial setup.
OFAC / Sanctions Screening OFAC status tracked on members, products and remittances (CLEARED / FLAGGED / NOT_CHECKED). Sanctions confirmation required on remittances and export shipments. Compliance flags at transaction level enforce hard blocks. KYC document upload with admin review and license status workflow.
Beezifi Intrusion Detection System (IDS) On-host agent deployed on every web server and database server node. Performs deep packet inspection against known attack signatures — SQL injection probes, brute-force attempts, port scans, and exploit kits. Automatically injects DROP firewall rules for flagged source IPs in under 100 ms. Continuously syncs with curated global threat intelligence feeds for pre-emptive blocking.
Beezifi IDS Endpoint — IP Telemetry Pipeline Per-host agent that captures every inbound source IP and outbound destination IP processed by the host and streams the data in real time to the BC3 Command Center over an encrypted telemetry channel. Block events and anomaly alerts are pushed immediately. Host health metrics are reported every 30 seconds. Four agents run in total — one on each web server and each database server — providing unified cross-node visibility.
BC3 — Beezifi Cybersecurity Command Center Centralised security operations platform that aggregates telemetry from all IDS Endpoint agents. Provides a SOC analyst dashboard with live network maps, alert timelines, IP geolocation overlays and drill-down incident views. Maintains a master blocklist pushed simultaneously to all server nodes when a bad actor is identified. Retains all IP records and events for 90 days hot storage and 1 year cold archival for forensic investigation and compliance reporting.
AI Security Agents — Autonomous Threat Response AI agents embedded in BC3 build statistical baselines of normal traffic per endpoint, per hour, and per user cohort. They correlate events across all four server nodes to detect distributed attack campaigns invisible from any single host. High-confidence threats (>95%) trigger autonomous block-pushes to the entire fleet; medium-confidence findings are escalated to the human analyst queue; novel or unknown patterns are captured, sandboxed, and immediately escalated. Analyst decisions feed back as labelled ground-truth to continuously improve model accuracy.

30-Table Relational Schema

All tables use VARCHAR(32) primary keys generated by `crypto.randomBytes` with role-prefixed IDs (e.g. `RMT_`, `IMP_`, `EXP_`, `AIJ_`). All monetary amounts use DECIMAL(15,2) or DECIMAL(18,2). Three crypto tables and four AI platform tables added in v1.1–v1.2. Foreign key constraints enforced at the DB level.

members

Central identity table. Multi-value category as JSON array. Supports 8 role types per member.

id category (JSON) kyc_status ofac_status
totp_secret otp_type

import_orders

Full import lifecycle with 30+ fields covering commercial, customs, regulatory and payment dimensions.

hs_code ior_designation incoterms fda_required
duties_payer status

export_shipments

Export order with ECCN dual-use classification, export license fields and full shipping details.

eccn dual_use export_license_number hs_code
incoterms

transport_shipments

Complete logistics record with tracking numbers, documents, addresses, timeline, customs status and POD.

tracking_number awb_number bol_number
customs_status pod_signature_url

shipment_events

Immutable event log per shipment. 10 event types from LABEL_CREATED through DELIVERED and EXCEPTION.

event_type (10 values) location occurred_at

insurance_policies

Active coverage with certificate URL, risk monitoring level and linked quote reference.

policy_number coverage_type risk_level
covered_from covered_until

bank_accounts

Multi-type accounts with separate available and ledger balance columns for real-time vs settled tracking.

account_type available_balance ledger_balance
status (ACTIVE/FROZEN/CLOSED)

bank_transactions

Full payment record with rail, counterparty, rail-specific IDs and optional platform entity link.

payment_rail counterparty_swift compliance_hold
linked_type settled_at

compliance_flags

Multi-scope compliance record covering members, accounts, transactions and payments.

reference_type flag_type severity (LOW-BLOCK)
required_action status

inspection_reports

Structured inspection output with result, status and approval signal that gates payment release.

result (PASS/FAIL/CONDITIONAL) approval_signal
status location

reconciliation_entries

One row per entity checked per run. Four entity types, three outcomes, with expected vs actual amounts.

entity_type result (MATCHED/DISCREPANCY/NO_BANK_TXN)
expected_amount actual_amount

payment_routes

Stored routing decision with full scored option set, compliance clearance flag and execution status.

route_options (JSON) recommended_rail
compliance_cleared status

crypto_wallets

Platform-managed and self-custody secp256k1 wallets per member. Stores address, encrypted private key, BIP39 mnemonic, and cached token balances (JSON).

address (130 char) private_key mnemonic
token_balances (JSON) wallet_type

crypto_transfers

On-chain token transfer record. Linked to platform orders via linked_type / linked_id. Stores MooChedda transaction ID on completion.

from_address to_address token_symbol
moochedda_tx_id linked_type / linked_id

crypto_invoices

Hosted payment invoices with line items (JSON), tax rate, expiry, and MooChedda payment URL. Status synced via poll endpoint.

moochedda_invoice_id payment_url line_items (JSON)
status (PENDING/PAID/EXPIRED)

ai_jobs

Tracks every AI Copilot task from submission to completion. Stores input, output, model metadata, and timing. Retained indefinitely for audit.

job_type	status (QUEUED/RUNNING/COMPLETED/FAILED)		
input_json	output_json	ai_provider	ai_model

ai_artifacts

Structured output produced by a completed AI job (form drafts, compliance summaries, reconciliation analyses). Includes confidence score and human approval workflow.

artifact_type	confidence_score	approval_status
approved_by	content_json	source_ref

ai_audit_log

Immutable record of every AI action, including the actor, action type, and contextual notes. Used for explainability and compliance reporting.

action_type	actor_id	job_id (FK)	artifact_id (FK)
notes			

ai_document_index

Chunked document store for Retrieval-Augmented Generation (RAG). Platform records are split into ordered chunks with metadata for semantic search queries.

doc_type	doc_ref_id	chunk_index	chunk_text
metadata_json			

REST Endpoints by Domain

All routes are under /api. Standard JSON request/response. Session token required on all authenticated routes.

DOMAIN	METHOD	ROUTE	DESCRIPTION
Auth	POST	/auth/register	Register new member with multi-role category array
Auth	POST	/auth/login	Login with password + optional TOTP/OTP second factor
Auth	POST	/auth/totp/setup	Generate TOTP secret and QR code for authenticator apps
Members	GET	/members	List all members with full profile
Members	PATCH	/members/:id	Update KYC status, OFAC status, approval, license
Remittances	POST	/remittances	Submit transfer — compliance middleware gated
Imports	POST	/import-orders	Create import order with regulatory declarations
Imports	PATCH	/import-orders/:id/status	Advance customs workflow status
Exports	POST	/export-profiles	Upsert KYB exporter profile (idempotent)
Exports	POST	/export-shipments	Create export shipment with ECCN controls
Transport	POST	/transport-shipments	Create logistics shipment record
Transport	POST	/shipment-events	Append tracking event to timeline
Transport	PATCH	/transport-shipments/:id/pod	Record proof of delivery (recipient, signature, photo)
Insurance	POST	/insurance-quotes	Generate cargo coverage quote
Insurance	POST	/insurance-policies	Issue policy from accepted quote
Insurance	POST	/insurance-claims	Submit claim against active policy
Bank	POST	/bank-transactions	Process payment — compliance middleware gated
Bank	POST	/fx-quotes	Create FX quote with rate, spread and fees
Bank	PATCH	/bank-accounts/:id/status	Freeze or close an account
Compliance	POST	/compliance-flags	Issue compliance flag against any entity
Compliance	PATCH	/compliance-flags/:id/status	Advance flag resolution workflow
Inspection	POST	/inspection-reports	Submit structured inspection report
Inspection	POST	/inspection-evidence	Upload photo/video evidence for a report
Inspection	POST	/inspection-defects	Log typed defect with severity and recommended action
Inspection	PATCH	/inspection-reports/:id	Update result or approval signal
Reconciliation	POST	/reconciliation/run	Start async reconciliation run (202 response)
Reconciliation	GET	/reconciliation/entries	Fetch entries for a completed run

DOMAIN	METHOD	ROUTE	DESCRIPTION
Routing	POST	/payment/route	Score all rails, store result, check compliance
Routing	PATCH	/payment/routes/:id/execute	Execute the recommended rail on a stored route
Routing	GET	/payment/rails	Return all rail specs and constraints
Matching	POST	/matching/execute	Admin bilateral trade match between two transactions
Crypto	POST	/crypto/wallets/create	Generate secp256k1 wallet via MooChedda — returns address, private key & mnemonic once
Crypto	POST	/crypto/wallets/recover	Restore wallet from BIP39 12-word mnemonic
Crypto	GET	/crypto/wallets/:id/balance	Fetch live token balances from MooChedda, cache in DB
Crypto	POST	/crypto/transfer	Sign and broadcast token transfer (USDC/USDT) with platform-held private key
Crypto	POST	/crypto/invoices	Create hosted payment invoice with line items, tax and token preference
Crypto	GET	/crypto/invoices/:id/status	Poll MooChedda for payment confirmation, sync status to DB
Crypto	GET	/crypto/prices	Real-time USDT-denominated token prices from MooChedda
Crypto	GET	/crypto/deposit-instructions	ACH/Wire fiat-to-USDC on-ramp routing details
KYC	POST	/kyc/upload	Upload KYC/KYB document for a member (up to 80 MB)
KYC	GET	/kyc/document/:memberId	Retrieve KYC document record for a member
AI	POST	/ai/form-draft	Form Copilot — convert plain-language description to structured payload
AI	POST	/ai/compliance/summary	Compliance Copilot — analyse active flags and generate risk summary with recommended actions
AI	POST	/ai/reconciliation/analyze	Reconciliation Copilot — analyse discrepancy entries and suggest resolution steps
AI	POST	/ai/payment/advise	Payment Route Advisor — score rails and recommend optimal payment path
AI	GET	/ai/jobs/:id	Poll status and retrieve output of any AI Copilot job

Native Crypto Settlement for Every Member

Any authenticated member — regardless of role — can access the Crypto Center. The platform integrates with MooChedda (v1.moochedda.com:3002), a REST-based self-custody payment infrastructure with zero transaction fees and instant settlement.

Wallet Management

Create new secp256k1 wallets or recover existing wallets from a BIP39 12-word mnemonic. Platform-managed wallets store the private key server-side for automated signing. Self-custody wallets store only the address. Live balance refresh pulls all token holdings from MooChedda and caches them.

Token Transfers

Send USDC, USDT, or any registered MooChedda token directly to a recipient wallet address. The platform signs the transfer payload using secp256k1 ECDSA (SHA-256 hash of fromAddress + toAddress + amount + tokenSymbol) without any external signing library. Transfers can be linked to a platform order (remittance, import, export, invoice) for cross-ledger traceability.

Hosted Payment Invoices

Exporters and any member can generate hosted payment invoices with multiple line items, configurable tax rate (e.g. 0.08 for 8%), token preference, and expiry window. MooChedda returns a hosted paymentUrl that the buyer opens to pay. Invoice status (PENDING / PAID / EXPIRED) is polled on demand and synced back to the platform database.

Live Market Data

Real-time USDT-denominated prices for all tokens registered on MooChedda, updated continuously through on-chain swap activity. The token registry endpoint lists every registered token with name, symbol, decimals, total supply and creator address. One-click price refresh from the Crypto Center UI.

Fiat On-Ramp (ACH / Wire)

Members can retrieve MooChedda ACH and wire transfer routing instructions directly from the platform. Fiat deposits via bank transfer credit the member's wallet as USDC at a 1:1 ratio with zero fees, providing a seamless bridge from the traditional banking layer managed in the Bank Center.

Security Architecture

secp256k1 DER key construction is implemented from scratch using ASN.1 byte-level encoding with only the Node.js crypto module — no secp256k1 or elliptic npm packages. Read operations require no authentication. Write operations are authenticated by cryptographic signature, not API keys. Private keys are stored server-side for platform-managed wallets (encryption at rest recommended for production).

Role-Specific Guided Onboarding

Every member sees a personalised Getting Started guide on the platform — tailored to their exact role combination. Members holding multiple roles see all relevant guides stacked in sequence.

8 Role-Specific Guides

- **Admin:** Member approval, KYC review, OFAC screening, compliance flags, reconciliation
- **Remitter:** Beneficiary setup, remittance submission, funding sources, crypto payments
- **Importer:** Marketplace, customs declarations, regulatory flags, payout accounts
- **Exporter:** KYB profile, product listings, shipments, payout accounts, crypto invoices
- **Transport:** Shipment creation, event logging, customs, charges, proof of delivery
- **Insurance:** Quote → Policy → Claim lifecycle, risk monitoring, payout confirmation
- **Bank:** Account opening, transactions, FX, compliance flags, payment routing
- **Inspector:** Reports, evidence, defect logging, approval signal for payment release

Onboarding Flow

- Member registers with selected role(s) — account starts as PENDING
- Admin reviews registration, verifies KYC document, sets status to APPROVED
- Member logs in and navigates to **Getting Started** under Account in the sidebar
- Platform detects roles from `user.category []` array and renders all matching guides
- Each guide shows numbered steps with direct navigation cues to the relevant Center
- Settings page includes password management and TOTP two-factor authentication setup
- First-boot admin setup screen auto-detected — redirects to account creation before login

Running GSCX

The platform is a single Node.js process with a MariaDB backend. The schema is idempotent — safe to re-run on every startup via `CREATE TABLE IF NOT EXISTS` and `ALTER TABLE ADD COLUMN IF NOT EXISTS`.

REQUIREMENTS

Node.js 18+

ES2022 features, native crypto module required

MariaDB 10.5+

JSON column support, `FIELD()` ordering function

.env configuration

DB_HOST, DB_USER, DB_PASS, DB_NAME, PORT

QUICK START

TERMINAL

```
npm install
npm start # NODE_ENV=production
# Server runs on PORT (default 3000)
# Schema auto-applies on startup
# First-run admin setup screen appears
```

On first boot the platform detects no administrator and shows a setup screen to create the initial admin account. All subsequent visits go straight to the login page.

Beezifi IDS & BC3 Command Center

A dedicated cybersecurity stack runs in parallel with the application infrastructure — collecting network telemetry at every node, routing it to a centralised command centre, and acting on threats autonomously through AI Security Agents alongside human analysts.

Beezifi IDS — On-Host Intrusion Detection

Deployed on every web server and database server node. Performs real-time deep packet inspection against known attack signatures — SQL injection probes, brute-force login attempts, port scans, and exploit kits. Automatically blocks malicious IPs via host firewall rules in under 100 ms with zero manual intervention. Continuously syncs with global threat intelligence feeds for pre-emptive blocking before an attack even begins.

Beezifi IDS Endpoint — IP Telemetry Pipeline

A lightweight per-host agent runs alongside Beezifi IDS on each server node. It captures every inbound source IP and every outbound destination IP and streams the data in real time to the BC3 Command Center over an encrypted channel. Block events and anomaly alerts are pushed immediately; host health metrics report every 30 seconds. Four agents provide full east-west and north-south network visibility across the fleet.

BC3 — Beezifi Cybersecurity Command Center

The centralised security operations platform that aggregates telemetry from all four IDS Endpoint agents. Security analysts work from a live SOC dashboard showing network maps, alert timelines, IP geolocation overlays and drill-down incident views. BC3's Blocklist Orchestrator pushes block rules simultaneously to every server node when a threat is confirmed — ensuring fleet-wide protection within seconds of a decision. All events are stored in a SIEM with 90-day hot and 1-year cold retention for forensics and compliance.

AI Security Agents — Behavioral Anomaly Detection

AI agents embedded in BC3 build statistical traffic baselines per endpoint, per hour of day, and per user cohort. Deviations — sudden connection spikes, unusual port access, geographic impossibility — automatically trigger investigation workflows without waiting for human review. Agents also cross-correlate timing, payload similarity, and TTL fingerprints across all four server nodes to detect and block distributed attack campaigns that would evade any single-host view.

AI Security Agents — Autonomous Response

High-confidence threats (>95% classification score) trigger autonomous block-pushes to the entire fleet — compressing response time from minutes to milliseconds. Medium-confidence findings (60–95%) result in a temporary block and immediate escalation to the analyst queue for human review. Low-confidence signals are flagged and watched. Novel or previously unseen patterns are sandboxed and escalated immediately for hands-on forensic investigation.

Human-AI Collaboration Model

Security analysts and AI agents operate in a tiered partnership. Analysts can override, suppress, or confirm any AI-generated block within a 15-minute window. Every analyst decision — confirm, false-positive override, escalate — feeds back into the AI models as labelled ground-truth, continuously improving classification accuracy and reducing false positives over time. All analyst actions are fully audit-logged in BC3.

AI AGENT RESPONSE TIERS

THREAT CONFIDENCE	AI ACTION	ANALYST ROLE
HIGH >95%	Autonomous block pushed fleet-wide instantly	Notified; can override within 15 min
MEDIUM 60-95%	Temporary block + escalate to analyst queue	Reviews and confirms or reverses
LOW <60%	Flag and watch; no block issued	Reviews enriched alert; decides action
NOVEL / UNKNOWN	Capture, sandbox, immediate escalation	Hands-on forensic investigation

IDS NODE COVERAGE

100%

All web + DB server nodes monitored
Zero unmonitored infrastructure

AUTO-BLOCK LATENCY

<100 ms

IP block applied at host firewall
No manual intervention required

FLEET-WIDE BLOCK PUSH

<5 sec

BC3 Blocklist Orchestrator pushes
to all nodes simultaneously

TELEMETRY RETENTION

1 year

90-day hot storage (fast query)
+ 12-month cold archival

Four Built-In AI Copilots

GSCX ships with a pluggable AI platform layer that embeds intelligent assistants directly into trade finance workflows. Each copilot exposes a structured JSON API backed by a swappable provider — a mock heuristic engine runs out-of-the-box; any external LLM can be substituted via the `AI_PROVIDER` environment variable. All jobs are tracked, all outputs are stored as scoreable artifacts, and every AI action is audit-logged.

Form Copilot — POST `/api/ai/form-draft`

Accepts a plain-language description of a trade operation and converts it into a fully structured API payload for remittance creation or import order submission. The copilot detects currency, amounts, beneficiaries, purposes, and incoterms from free text. Missing required fields are identified and surfaced as clarifying questions. Each draft carries a per-field confidence score (0.58–0.91) and a list of warnings for fields that needed assumptions.

Compliance Copilot — POST `/api/ai/compliance/summary`

Analyses all active compliance flags for a member or transaction and produces a structured risk summary. The copilot assigns an overall risk level (LOW / MEDIUM / HIGH / CRITICAL), extracts all required documents from flag data, drafts an analyst narrative, and generates a prioritised list of recommended actions — including whether to hold, escalate, request additional information, or clear the entity. Output is stored as a reviewable artifact before any action is taken.

Reconciliation Copilot — POST `/api/ai/reconciliation/analyze`

Takes a completed reconciliation run and provides intelligent analysis of its discrepancy entries. For each unmatched or discrepant record the copilot performs root-cause analysis (timing mismatch, FX rounding, missing settlement, duplicate posting), identifies likely matching bank transactions, and recommends specific resolution steps — including entries to write off, transactions to investigate, or corrections to submit. Summaries are stored as artifacts for controller review.

Payment Route Advisor — POST `/api/ai/payment/advise`

Supplements the deterministic payment orchestration engine with AI-generated narrative advice. Given the payment parameters and the scored route options, the advisor explains why the recommended rail was chosen, flags any compliance considerations, identifies corridor-specific risks (currency volatility, settlement delays, sanction exposure), and provides ranked alternatives with cost/speed trade-off commentary — all in human-readable form for operations review.

AI Infrastructure & Job Lifecycle

COMPONENT	TABLE	PURPOSE
Job Manager	<code>ai_jobs</code>	Tracks every copilot invocation from QUEUED → RUNNING → COMPLETED / FAILED. Stores full input and output JSON, provider name, model ID, and wall-clock timing. Jobs are retained indefinitely.
Artifact Store	<code>ai_artifacts</code>	Persists structured output of completed jobs with a confidence score (0.0–1.0). Artifacts have a human approval workflow — PENDING → APPROVED / REJECTED — so outputs can be reviewed before being acted upon.
Audit Log	<code>ai_audit_log</code>	Immutable record of every AI action. Captures actor ID, action type (generate, approve, reject, escalate), linked job and artifact, and free-text notes. Supports explainability and regulatory compliance reporting.
Document Index	<code>ai_document_index</code>	Chunked text store for Retrieval-Augmented Generation (RAG). Platform records (contracts, reports, flags) are split into ordered chunks with metadata JSON, enabling semantic search queries against live platform data for future copilot capabilities.

Phase 2–3 Planned Capabilities

TRADE CLASSIFICATION

HS / ECCN Code Suggestion

Auto-classify goods from product description; flag dual-use items and restricted destinations.

Shipment Risk Prediction

Predict delay probability and optimal carrier selection from historical corridor data.

INSURANCE & INSPECTION AI

Insurance Risk Scoring

Score cargo risk and recommend coverage tier from route, cargo type, and historical claims data.

Inspection Image Analysis

Analyse uploaded evidence photos to auto-detect and classify defect types and severity.

INTELLIGENCE & OPTIMISATION

Cross-Entity Case Intelligence

Surface hidden connections between members, transactions, and flags across the full platform.

Counterparty Anomaly Detection

Identify unusual behavioural patterns in payment flows before compliance flags are raised.