Trade Finance Blockchain Explorer

Project Statement:

This project offers transparent, tamper-evident tracking of trade finance artifacts (LoCs, invoices, shipping docs) with a ledger-style explorer and risk insights.

Key Features:

- Document repository with hashing
- Ledger explorer for lifecycle events
- Tamper-proof audit trails
- Counterparty risk scoring
- Trade flow visualizations

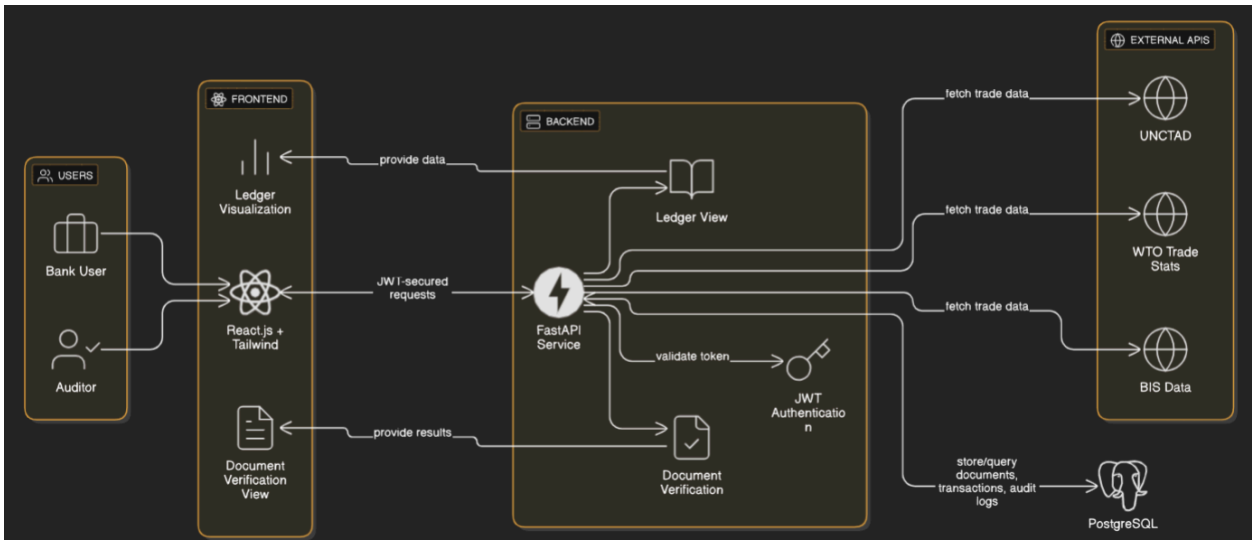
Tech Stack:

- Frontend: React.js + Tailwind CSS
- Backend: FastAPI
- Database: PostgreSQL
- Authentication: JWT (access + refresh)
- **Extras:** Object storage for docs (S3/compatible), scheduled integrity checks; Integrations (UNCTAD, WTO, BIS datasets)

Modules:

- Module A: Auth & Role/Org Management
- Module B: Document Upload, Hash & Storage
- Module C: Ledger Explorer & Verification
- Module D: Trade Transactions & Risk Score
- Module E: Analytics & Reporting

Architecture Diagram:



8-Week Milestone Plan

Milestone 1: Weeks 1–2 – Auth & Org Setup

Week 1: Project skeleton, JWT auth, Users schema with roles/orgs
Week 2: Org scoping, role-based access, base layout

Expected Output:

Secure multi-role access, org context ready.

Milestone 2: Weeks 3–4 – Documents & Ledger

Week 3: Document upload (S3), metadata + hashing (SHA-256)
Week 4: LedgerEntries API + explorer UI, verify hash trail

Expected Output:

Documents stored with hashes; ledger timeline view.

Milestone 3: Weeks 5–6 – Transactions & Integrity

Week 5: Trade Transactions flow (buyer/seller, statuses)
Week 6: Integrity check job (Celery) + alerts on mismatches

Expected Output:

End-to-end trade flow; automated integrity checks.

Milestone 4: Weeks 7–8 – Risk & Analytics

Week 7: Risk scoring (combine internal events + external stats)
Week 8: Dashboards, exports (CSV/PDF), QA & deployment

Expected Output:

Risk dashboards, exportable analytics, production readiness.

Expected Project Outcome:

By Week 8, auditors and parties can verify documents, trace events on a ledger, assess risk, and export compliance-friendly reports.

Database Schema:

- **Users:** id (INT, PK), name (VARCHAR), email (VARCHAR, UNIQUE), password (VARCHAR), role (ENUM: 'bank', 'corporate', 'auditor', 'admin'), org_name (VARCHAR), created_at (TIMESTAMP)

- **Documents:** id (INT, PK), owner_id (FK to Users.id), doc_type (ENUM: 'LOC', 'INVOICE', 'BILL_OF_LADING', 'PO', 'COO', 'INSURANCE_CERT'), doc_number (VARCHAR), file_url (VARCHAR), hash (VARCHAR), issued_at (TIMESTAMP), created_at (TIMESTAMP)

- **LedgerEntries:** id (INT, PK), document_id (FK to Documents.id), action (ENUM: 'ISSUED', 'AMENDED', 'SHIPPED', 'RECEIVED', 'PAID', 'CANCELLED', 'VERIFIED'), actor_id (FK to Users.id), metadata (JSONB), created_at (TIMESTAMP)

- **TradeTransactions:** id (INT, PK), buyer_id (FK to Users.id), seller_id (FK to Users.id), amount (NUMERIC), currency (CHAR(3)), status (ENUM: 'pending', 'in_progress', 'completed', 'disputed'), created_at (TIMESTAMP), updated_at (TIMESTAMP)

- **RiskScores:** id (INT, PK), user_id (FK to Users.id), score (NUMERIC), rationale (TEXT), last_updated (TIMESTAMP)

- **AuditLogs:** id (INT, PK), admin_id (FK to Users.id), action (TEXT), target_type (VARCHAR), target_id (INT), timestamp (TIMESTAMP)