

Fibre, yarn and dye origin assurance

COTO design extension, not a PPT extract or activated feature. Synthetic pilots only. No Everledger partnership, integration or certification is claimed. Blockchain preserves a record of an assertion; it cannot make an inaccurate source true.

Intended outcome

Explain which material lots entered a rug and what evidence supports composition, sourcing and processing claims, with explicit limits where materials were mixed.

Accountable roles

Supplier attests its source lot; dyer/mill records transformation; manufacturer reconciles consumption; a competent reviewer/laboratory checks the specific claim scope.

Required evidence

Supplier and batch references; material species/composition; purchase and processing documents; quantity/unit; process losses; segregated versus mass-balance accounting method; test method/sample chain; issuer/site/scope/expiry; input-output links.

Six accountable steps

1. Register the source lot / Supplier + source reviewer

Record the declared origin and material composition against an actual batch and invoice. Document how the claim was checked. A fibre test can support composition within its method, but does not automatically prove a geographic origin.

2. Track the transformations / Mill/dyer + receiving site

Link yarn preparation and dye batches to their inputs, outputs, sites and documented process losses. Require the receiver to confirm quantity. Mixed inputs need an explicit transformation event rather than a false single-source identity.

3. Reconcile physical and accounting claims / Manufacturer + stock reviewer

Keep segregated/identity-preserved material separate from any mass-balance accounting claim. Check units, yield and declared waste. Allocated certified quantity cannot exceed the verified eligible input adjusted for the applicable scheme; mass balance must not be described as proof of physical content in every rug.

4. Assist document checking / AI operator + reviewer

Extract material, date, batch, quantity and issuer fields from permitted documents into a draft; compare them to the register. Low-confidence extraction or contradictory country/batch data goes to a person, not a guessed replacement.

5. Approve the product claim / Claim owner + competent reviewer

State exactly what is supported: composition, declared source, tested sample or scheme allocation. Record reviewer competence, evidence scope and uncertainty. A disputed source cannot receive an unconditional origin badge.

6. Publish a limited lineage view / Passport administrator

Show approved lot relationships, declared versus reviewed claim status and review date to the permitted audience. Append corrections and expiry changes; do not disclose private supplier prices or individual worker details.

Separate evidence, AI and blockchain

Blockchain role

A future approved ledger records opaque source/transformation references, approved-event digests, issuer/reviewer attestations and correction/revocation links. Full invoices, lab reports and identities remain private. A laboratory signature attests only the tested scope; the ledger cannot turn a supplier declaration into scientific proof.

AI role

OCR and entity matching identify inconsistencies and missing links. Begin with deterministic stock/mass calculations as the baseline. Do not infer origin from rug appearance, nationality or an unsupported model score. Evaluate extraction error on representative documents and keep the original evidence available to the reviewer.

Exceptions and safeguards

Unknown source, missing document, mixed batch, impossible yield or a revoked scheme certificate triggers a visible claim hold. An accredited test or issuer confirmation is needed only for the claim actually relied on. A corrected declaration is versioned; it does not silently rewrite the batch journey.

Current / manual route

Start with the existing lot evidence description/digest and an approved manual material-lineage register. No source-laboratory network, raw-material token or mass-balance service is currently active.

Additional work required

Structured input-output batches, unit/yield rules, evidence vault, issuer/claim status, reviewer permissions and the passport visibility view. Laboratory/issuer interfaces require separate agreements and test methods.

Prove the proposed service

Synthetic pilot

Synthetic input: 100 kg eligible yarn, 5 kg documented process loss and 95 kg output. Try allocating 110 kg of eligible claim, then mix a second batch. The system must flag over-allocation and prevent an identity-preserved claim on an unsegregated mixture.

Acceptance tests

Catch wrong units, altered report digests, missing transformation links and expired claim authority. Reviewer can state insufficient evidence. No source is fabricated, and a valid hash alone never clears the claim.

Measures

Source-link completeness; unexplained material balance; claim corrections; reviewer minutes; extraction errors. Compare like-for-like claims only.

Proposed payer and economics

Proposed payer: manufacturer/brand under a lot-based traceability or scoped assurance service. Laboratory, scheme and independent review charges are separate and disclosed. A subscription does not purchase proof of origin.

Release gate

Assign actual accountable people, permitted evidence sources, cost ceiling, test results, exception handling and rollback. No model may determine rights, certify claims or release money. Keep the affected feature disabled until failures are resolved and required operating/legal approvals are recorded.

Producer payment and value-share accountability

COTO design extension, not a PPT extract or activated feature. Synthetic pilots only. No Everledger partnership, integration or certification is claimed. Blockchain preserves a record of an assertion; it cannot make an inaccurate source true.

Intended outcome

Make agreed producer remuneration, lawful deductions and evidence of payment inspectable by authorized people, without publicly exposing individual wages or treating customer payment as a condition for earned pay.

Accountable roles

Actual employer/contracting payor owes remuneration; the producer or authorized representative can query records; finance prepares evidence; an independent labour/accounting reviewer checks discrepancies. COTO is not the wage payor unless a valid actual contract says so.

Required evidence

Understandable work order; payor; lawful employment/contract status; work quantity/time and agreed rates; required local payment currency; lawful conversion rule if relevant; permitted deductions; due date; restricted receipt evidence; safe correction/grievance route.

Six accountable steps

1. Agree an understandable work order / Payor + producer/group

Record the actual work, rate, input ownership, quality criteria, due date and permitted deductions. An authorized coordinator cannot waive individual mandatory rights. International trade amounts remain USD; wage payments follow the currency and rules required locally.

2. Record work and independent queries / Producer + work supervisor

Confirm completed work and provide an accessible statement. Preserve a channel outside the immediate supervisor to dispute quantities or deductions. No smartphone, publicity release or public biometric record is required to receive earned pay.

3. Prepare the remuneration statement / Finance preparer

Calculate gross entitlement, each lawful agreed deduction and net amount using exact arithmetic. Separate advances, credits, employer contributions and any COTO/service fee. Do not silently deduct platform charges from wages.

4. Flag mismatches for review / Rules/AI + independent reviewer

Detect arithmetic gaps, duplicate references, inconsistent rates, unusual repeated deductions and missing receipt evidence. AI may extract fields or prioritize missing paperwork only. It cannot determine a person's legal wage entitlement, employment status or eligibility.

5. Confirm payment through a lawful route / Actual payor + beneficiary + reviewer

Record separately payment instructed, credited and available, according to the real banking/payment arrangement. A supervisor's attestation is not proof the producer received money. Permit a safe producer challenge; handle cash evidence only with a lawful, proportionate procedure.

6. Share aggregates with scope / Authorized reviewer + data owner

Release only appropriately protected period/batch-level totals and methodology to authorized buyers or programme overseers. Small cohorts may be identifiable; suppress or aggregate further. Show wage evidence status and unresolved differences without claiming exploitation-free production.

Separate evidence, AI and blockchain

Blockchain role

Keep personal/payroll records off-chain, including individual complaint links. If needed, anchor only an approved aggregate statement digest and reviewer authority after a re-identification assessment. No worker wallet, wage token, public salary ledger or automatic deduction is created.

AI role

Assist extraction and anomaly triage under a fixed documented purpose; baseline rules handle arithmetic and duplicate checks. Log evidence, model/version and human disposition. No biometric age inference, employment decision, punitive scoring or autonomous denial of pay is allowed.

Exceptions and safeguards

Missing beneficiary confirmation remains unresolved; a lawful due wage must not be relabelled paid. Suspected coercion/retaliation goes to a competent independent safeguarding route. Customer non-payment does not automatically defer earned remuneration. Corrections retain the original statement and reason.

Current / manual route

Trial a private remuneration register under appropriate labour/privacy advice and controlled evidence exchange. Existing carpet order balances do not represent individual payroll or prove worker payment.

Additional work required

A separately permissioned producer-work/remuneration ledger, accessible statements, restricted evidence, aggregate disclosure, independent challenge and lawful retention. Local specialist review is needed before real worker data is processed.

Prove the proposed service

Synthetic pilot

Use fictional work orders with one duplicate payment reference, one unexplained deduction and one payment marked sent but not credited. Confirm the producer can dispute it and buyers cannot view individual salaries or identities.

Acceptance tests

Block cross-person/payor data access, detect the duplicate and unexplained difference, preserve a challenge and prevent a supervisor from representing an unsupported receipt as final payment.

Measures

Undisputed amounts paid by lawful due date; unresolved statement differences; safe query accessibility; duplicate/short-payment detection; privacy exposure (target zero in scripted tests).

Proposed payer and economics

Proposed payer: contracting manufacturer or responsible-sourcing programme under a scoped assurance order, never an undisclosed worker access fee. Review cost and remediation funding are distinct from wage principal.

Release gate

Assign actual accountable people, permitted evidence sources, cost ceiling, test results, exception handling and rollback. No model may determine rights, certify claims or release money. Keep the affected feature disabled until failures are resolved and required operating/legal approvals are recorded.

Certificate validity and claim assurance

COTO design extension, not a PPT extract or activated feature. Synthetic pilots only. No Everledger partnership, integration or certification is claimed. Blockchain preserves a record of an assertion; it cannot make an inaccurate source true.

Intended outcome

Make clear who issued a certificate, what it covers and whether it remains valid for the particular rug, site or batch, rather than displaying an unsupported logo.

Accountable roles

The certificate issuer controls its attestation/revocation; the supplier submits evidence; a conflict-aware reviewer validates identity/scope; the claim publisher is accountable for the public wording.

Required evidence

Issuer identity and verification channel; certificate reference/version; subject/site/products/batches; standard and scope; issue/expiry; status/revocation source and last check; document digest; reviewer authority; public claim wording.

Six accountable steps

1. Declare the precise claim / Supplier/brand

Identify the standard, issuing body and exact site/product/batch scope. A general company certificate must not be represented as certification of every carpet. Identify self-declared assertions separately.

2. Validate issuer and source / Reviewer + actual issuer

Use an independently verified issuer channel or registry where available, not only the uploaded PDF. Confirm its authority, reference and scope, and record the response/time. An issuer is not assumed to partner with COTO.

3. Extract and compare / AI operator + reviewer

OCR relevant fields from the permitted document, then match identifiers, dates and scope against source records. Flag inconsistent typography or metadata only as suspicion; a model cannot conclusively label a document forged.

4. Attest the reviewed status / Issuer/authorized reviewer

Set supplier-declared, document-checked, issuer-confirmed, expired, revoked, disputed or unknown with scope and last-check time. Only the issuer can make its own original certification; a reviewer attests the checks actually performed.

5. Monitor expiry and revocation / Status service + reviewer

Apply expiry reminders and verified issuer updates, keep a stale-source state and remove the current-valid badge when support lapses. Corrections do not erase the historical fact that a certificate was previously presented.

6. Expose a bounded assurance view / Claim publisher

Publish only the approved claim, evidence/status source, scope, date and limitations. Restrict confidential reports and personal data. A verifier page must not show a broader assurance level than the underlying issuer evidence.

Separate evidence, AI and blockchain

Blockchain role

Anchor document/version digests and authorized attestations with scope, status and revocation links after ledger activation. Issuer keys and authority need onboarding, rotation and revocation controls. A timestamped PDF hash alone is only evidence of the presented file, not issuer authenticity.

AI role

Extract and reconcile, detect missing fields and route uncertain matches. Measure exact critical-field accuracy and false accusations on varied scans/languages. Approval remains human/issuer based; deterministic expiry rules do not require a language model.

Exceptions and safeguards

Issuer unreachable: display not revalidated/stale, not confirmed. Name mismatch: resolve documented legal-name changes. Revoked certificate or compromised signing key: retract affected current claims and queue dependent passports. A paid review may not guarantee a positive status.

Current / manual route

Record certificate references and review notes in controlled registers/evidence descriptions. The current business approval and lot fingerprint do not establish certification status.

Additional work required

Issuer directory, claim-scope model, attestation/revocation events, independent verification evidence, expiration jobs and filtered public views. Issuer integrations require their actual consent/terms and operational testing.

Prove the proposed service

Synthetic pilot

Use fictional certificates including an expired one, a real-looking altered reference, a revoked one and a company-level certificate wrongly applied to a rug. Each must receive the appropriate limited status.

Acceptance tests

Do not clear the altered reference from its hash; propagate revocation; mark stale checks; prevent a supplier from granting itself issuer-confirmed status; block a badge outside certificate scope.

Measures

Current claims with verified scope/source; expiry/revocation propagation delay; false confirmation rate; unresolved issuer queries; review effort per claim.

Proposed payer and economics

Proposed payer: subscribing brand/manufacturer or scoped document-review customer. Fee buys documented checking, not certification or a favourable result. Independent issuer charges remain separate.

Release gate

Assign actual accountable people, permitted evidence sources, cost ceiling, test results, exception handling and rollback. No model may determine rights, certify claims or release money. Keep the affected feature disabled until failures are resolved and required operating/legal approvals are recorded.

Physical rug authentication and copied-tag detection

COTO design extension, not a PPT extract or activated feature. Synthetic pilots only. No Everledger partnership, integration or certification is claimed. Blockchain preserves a record of an assertion; it cannot make an inaccurate source true.

Intended outcome

Combine physical inspection, controlled product photography and tag history to investigate substitution or copied identifiers, without treating a QR code or image score as conclusive authenticity.

Accountable roles

Manufacturer registers the reference rug; a trained examiner reviews suspected mismatches; tag administrators control replacement; the brand/rights holder approves any authenticity statement.

Required evidence

Item/batch/design ID; authorized reference photos at defined angles/scale/lighting; distinctive construction/pattern features; sample/capture method; tag serial; issuance/custody history; examiner findings; known variations and test dataset.

Six accountable steps

1. Capture a trustworthy reference / Manufacturer + examiner

Photograph the actual item using a repeatable protocol and link it to the batch, design and tag attachment evidence. Check the reference source; a false initial registration would otherwise acquire a convincing digital history.

2. Issue and bind the identifier / Tag administrator + custodian

Create a random first-party ID and controlled label; document attachment and checking. Record reissues and revocation. Tags, NFC and RFID can be copied or moved, so the binding procedure is part of the evidence.

3. Collect a comparison safely / Retailer/customer + examiner

Request minimum product images or a physical examination through a controlled route. Avoid collecting customer location or personal information unnecessarily. Record image quality and whether the capture is adequate for comparison.

4. Compare in shadow mode / Computer-vision tool + examiner

A model may rank similarity against the right reference and flag possible mismatch or duplicate-tag use. Record model/version, capture conditions and uncertainty. Poor images, repairs and handmade variation must not become automatic fraud accusations.

5. Decide with physical/contextual evidence / Trained examiner + accountable brand

Review texture/construction, history, tag mapping and any available inspection. Record consistent, inconclusive or mismatch requiring investigation. An adverse finding needs a fair correction/appeal route and must not be based solely on machine vision.

6. Correct or reissue the record / Authorized administrator

Link a confirmed replacement/reissue to the original history; suspend an unsupported public claim when needed. Preserve the evidence and reason. A scan cannot transfer title, debit a buyer or permanently erase another claimant's record.

Separate evidence, AI and blockchain

Blockchain role

A future ledger can anchor the registered-reference digest, controlled tag lifecycle and authorized examiner attestation. Raw image files and customer details remain private. A persistent identity is a claim to be checked against the object, not an unforgeable physical guarantee.

AI role

Use bounded similarity/anomaly assistance only after representative tests covering genuine variation, wear, repairs, copied labels and poor lighting. Report false match/non-match rates and an inconclusive option. No facial/person identification is needed.

Exceptions and safeguards

No valid reference, inadequate image or substantial repair: request more evidence or in-person inspection. Duplicate tag: retain both reports and investigate. Disputed authenticity: prevent broad public accusation and permit qualified review.

Current / manual route

Trial controlled photographs and a manual tag/examination register with fictional items. The current pilot has no trained authentication model, examiner network or public authenticity service.

Additional work required

Reference-image storage, capture validation, tag-reissue records, examination/appeal workflow and a permissioned result view. Add computer vision only after a representative labelled evaluation and appropriate rights/data arrangements.

Prove the proposed service

Synthetic pilot

Use genuine test-item variations, a moved/copied tag and poor-quality photographs. Blind reviewers to the model output for a baseline, then compare assisted decisions and confidence.

Acceptance tests

A copied tag must not prove authenticity; a poor photo must allow inconclusive; a genuine handmade variation must not automatically trigger fraud; unauthorized users cannot change the reference or examiner result.

Measures

False match/non-match and inconclusive rates; examiner time; physical mismatch detection; erroneous adverse claims; controlled reissue completeness.

Proposed payer and economics

Proposed payer: brand/retailer under an examination or identity-maintenance service. Physical inspection cost is disclosed. Do not sell a guarantee of counterfeit elimination.

Release gate

Assign actual accountable people, permitted evidence sources, cost ceiling, test results, exception handling and rollback. No model may determine rights, certify claims or release money. Keep the affected feature disabled until failures are resolved and required operating/legal approvals are recorded.

Environmental footprint and sustainability claim evidence

COTO design extension, not a PPT extract or activated feature. Synthetic pilots only. No Everledger partnership, integration or certification is claimed. Blockchain preserves a record of an assertion; it cannot make an inaccurate source true.

Intended outcome

Show the evidence, boundaries and uncertainty behind an environmental statement so buyers can distinguish a measured result, a modelled estimate and a marketing claim.

Accountable roles

The manufacturer supplies source data; a qualified analyst selects the method and calculation; an independent reviewer checks relied-on claims; the publisher is accountable for the wording.

Required evidence

Defined product/functional unit and life-cycle boundary; material amounts; energy/fuel/water/waste records; allocation rules; supplier factors with dates/geography/method; transport assumptions; uncertainty/data quality; calculation version and review scope.

Six accountable steps

1. Define one comparable question / Claim owner + qualified analyst

Specify the unit, product life/use scenario and included stages. Carbon, water use and chemical compliance need their own appropriate methods; do not collapse them into an unsupported universal eco-score. Define comparison rules before comparing suppliers.

2. Collect and classify source data / Site/supplier + analyst

Record measured bills/meters, material records and declared estimates separately, including periods and units. Missing information remains missing or uses a justified labelled estimate; it is not zero impact.

3. Assist extraction and detect gaps / AI operator + analyst

Extract figures from permitted bills/reports and check unit/period consistency. Flag improbable values or missing coverage. A language model must not invent an emission factor, meter reading or supplier certificate.

4. Calculate reproducibly / Qualified analyst

Use a versioned method/factor library and exact units; record each allocation and assumption. For carbon, use an appropriate product life-cycle accounting approach with documented scope/data quality. Compare alternatives only on consistent boundaries and declared uncertainty.

5. Review the claim and wording / Independent reviewer + publisher

Check material drivers, double counting, data quality, calculation and review scope. State measured versus modelled, period, boundary and uncertainty. No carbon-neutral, zero-impact or certified label follows merely from paying a subscription or anchoring a number.

6. Maintain and disclose selectively / Claim publisher

Publish the approved summary and method/reference dates, while restricting commercially sensitive bills and personal data. New factors or corrected inputs create a new calculation/claim version and a documented reason for changed results.

Separate evidence, AI and blockchain

Blockchain role

Anchor an approved calculation-package digest, method/factor version and scoped reviewer attestation after ledger activation. A later reader can check that the referenced package changed; the ledger does not validate a measurement or confer environmental certification.

AI role

Assist document extraction and anomaly triage, with all critical values traceable to source pages. Use deterministic calculations as the numerical authority. Require a qualified person to approve substitutions, assumptions and comparative claims.

Exceptions and safeguards

Missing major data, incompatible boundaries or obsolete factors: publish insufficient/not comparable rather than a green ranking. Recycled-content and renewable-energy claims need evidence for their own allocation rules; do not count the same attribute twice.

Current / manual route

Run a reviewed private source/calculation register. Existing lot descriptions may reference approved evidence but do not constitute an LCA/footprint engine or verified environmental claim.

Additional work required

Versioned source inventory, method/factor library, calculation lineage, uncertainty/coverage fields, claim approval and controlled disclosures. Obtain specialist review and any scheme permissions before making certified/comparative statements.

Prove the proposed service

Synthetic pilot

Use fictional site bills and material records. Change kg to tonnes incorrectly, remove a large input, mix two boundaries and update one factor. A reviewer must detect the errors and the published claim must retain its version and limitations.

Acceptance tests

Reject an unsupported factor, missing-data-as-zero and incomparable ranking; preserve earlier calculations; separate water/carbon metrics; require reviewer approval before claim publication.

Measures

Primary-data coverage; traceable critical inputs; sensitivity/uncertainty; corrected calculation errors; comparable scope coverage; reviewer effort. No untested reduction percentage is advertised.

Proposed payer and economics

Proposed payer: manufacturer/brand under a scoped analysis and evidence-maintenance order. Analyst and independent assurance fees are separate. No trade in carbon credits or offsets is created.

Release gate

Assign actual accountable people, permitted evidence sources, cost ceiling, test results, exception handling and rollback. No model may determine rights, certify claims or release money. Keep the affected feature disabled until failures are resolved and required operating/legal approvals are recorded.

Invoice, packing and trade-document reconciliation

COTO design extension, not a PPT extract or activated feature. Synthetic pilots only. No Everledger partnership, integration or certification is claimed. Blockchain preserves a record of an assertion; it cannot make an inaccurate source true.

Intended outcome

Detect inconsistencies between the agreed carpet trade and its documents before they become avoidable payment, customs or delivery disputes.

Accountable roles

Seller prepares documents; buyer/importer and its qualified customs/logistics adviser confirm their role-specific requirements; finance checks USD obligations; a named coordinator resolves mismatches.

Required evidence

Accepted order/design version; USD invoice; packing list; quantities/units; shipping/custody references; origin and certificate references; permitted classification declarations; agreed Incoterm/place; document versions; issuer and approval references.

Six accountable steps

1. Freeze the comparison baseline / Seller + buyer

Use the exact accepted order, parties, quantities, USD prices, destination, Incoterm/place and document conditions. A different commercial assumption cannot be smuggled in through a later invoice.

2. Register document versions / Document preparer

Keep each authorized invoice/packing/shipping file and issuer reference in restricted storage. Assign a document ID and digest; mark drafts, superseded and issued versions. Avoid sensitive bank details in public comparisons.

3. Extract and normalize fields / AI operator + rules

OCR and match party names, item/lot IDs, counts, weights/units, dates and monetary fields. Use exact decimal/cents for USD and documented unit conversions. Preserve source snippets and confidence for each extracted critical field.

4. Run deterministic comparisons / Finance/logistics reviewer

Check arithmetic, invoice totals/milestones, duplicated references and packing counts against approved terms. AI may prioritize conflicting documents but cannot determine legal classification, origin entitlement, customs clearance or payment authorization.

5. Resolve with the correct issuer / Responsible party + counterparty

Obtain an authorized corrected document or a separately approved order variation, with reason and reference to the superseded version. A coordinator cannot edit another issuer's certificate or silently change an accepted quantity.

6. Release the checked package / Authorized finance/importer reviewer

Record which checks passed and which remain open. Only the legally responsible party/customs professional submits filings or approves actual payment. Document matching is a review service, not a clearance, banking or sanctions certification.

Separate evidence, AI and blockchain

Blockchain role

After activation, anchor the issued-package digest, approval scope and supersession events, using opaque references. Keep documents, bank information and counterparties' confidential terms off-chain. An anchored fraudulent invoice remains fraudulent.

AI role

OCR/entity linking and mismatch triage with critical-field human checking. Measure false clearance and extraction error on scans, currencies and layouts. Prompt/document instructions are untrusted data; they cannot authorize changed beneficiaries or new system actions.

Exceptions and safeguards

Unknown charge, non-USD price, changed beneficiary, duplicate invoice or unit mismatch: hold the affected package for review. Independent callback verifies beneficiary changes. A customs authority/query is handled by the actual importer/adviser, not an AI approval.

Current / manual route

Compare issued documents manually with existing order/invoice/balance records and evidence digests. No document upload/OCR/customs connector or payment instruction service is active.

Additional work required

Controlled document versions/vault, extraction schemas, source-field links, deterministic rule engine, resolution/approval workflow and export. Any customs/provider interface needs a separately authorized integration and role-specific review.

Prove the proposed service

Synthetic pilot

Seed fictional document packs with 20-versus-19 count, an altered beneficiary, duplicate invoice and a different currency. Compare manual and assisted checking; include a valid unusual layout to measure false alarms.

Acceptance tests

Do not clear a critical mismatch from a model score; preserve issuer corrections; detect the duplicate; block unapproved beneficiary changes; ensure no filing, email or payment is sent automatically.

Measures

Critical-field accuracy; mismatch detection and false-clearance rate; review time; reissued document rate; disputes caused by unnoticed document differences.

Proposed payer and economics

Proposed payer: exporter/importer through a per-package review or subscribed workflow, with specialist advice separately scoped. No percentage on client funds or promise of customs acceptance is implied.

Release gate

Assign actual accountable people, permitted evidence sources, cost ceiling, test results, exception handling and rollback. No model may determine rights, certify claims or release money. Keep the affected feature disabled until failures are resolved and required operating/legal approvals are recorded.

Custody, seal and transit-condition evidence

COTO design extension, not a PPT extract or activated feature. Synthetic pilots only. No Everledger partnership, integration or certification is claimed. Blockchain preserves a record of an assertion; it cannot make an inaccurate source true.

Intended outcome

Identify what was handed over, in what condition and under whose responsibility, so transit damage and quantity differences can be investigated on evidence rather than conflicting messages.

Accountable roles

Each actual custodian attests its handover; sender/receiver confirm independently; a qualified surveyor assesses damage; the contractual parties/carrier/insurer decide obligations under their actual agreements.

Required evidence

Item/lot and package IDs; count/condition photographs; seal IDs; custodian/site references; dispatch/receipt times; agreed environmental limits; any sensor identity/calibration/clock; route/transport documents; inspection and exception records.

Six accountable steps

1. Agree the evidence protocol / Trading parties + carrier/custodian

Specify packaging, count, condition, seal handling, inspection and relevant environmental limits. Risk, ownership and carrier liability follow the sale/specialist contracts, not automatically the next scan.

2. Capture dispatch condition / Sender + authorized checker

Record package/lot mapping, count, visible condition, seal and time using controlled evidence. A seal number is not proof a package was never opened. Store only necessary location/site information; no public driver tracking.

3. Collect the transport record / Custodian + approved data source

Record handovers and source timestamps. If sensors are justified, verify device identity, calibration, clock, tamper status and outages. Begin with manual inspections where sufficient; sensors are not assumed to exist.

4. Flag anomalies / Rules/AI + logistics reviewer

Compare readings/condition reports with the agreed limits and known context. A model may prioritize suspected humidity/shock or photo changes, but an alert is not proof of causation, negligence or an insurance claim.

5. Countersign receipt and differences / Receiver + sender/custodian

Record actual count, seal and visible condition independently. Differences open a case linked to specific packages and contract terms. Preserve the one-sided dispatch record without inventing the receiver's acceptance.

6. Resolve and publish the scoped history / Surveyor + actual parties

Link inspection, survey and agreed outcome; preserve source gaps and corrections. Show approved custody status without disclosing confidential routes or personal contacts. Carrier/insurer decisions remain with authorized parties.

Separate evidence, AI and blockchain

Blockchain role

Anchor authorized dispatch/receipt/condition-event digests and linked exceptions after approval. Device data remains in a controlled evidence store with source metadata. A blockchain record prevents silent version substitution, not sensor malfunction or false reporting.

AI role

Assist comparative image/condition triage and sequence anomaly detection, with a deterministic threshold/manual baseline. Test sensor gaps, clock errors and ordinary appearance variation. Never automatically assign liability or release an insurance payout.

Exceptions and safeguards

Broken seal, missing sensor intervals, changed clock or count difference: label the affected leg incomplete/disputed. Quarantine affected goods where appropriate and preserve evidence. An outage is not an all-clear condition history.

Current / manual route

Use existing dispatch/received/disputed events plus manual package/seal registers. The current pilot has no IoT feeds, carrier integration, surveyor service or insurance-settlement engine.

Additional work required

Package/custodian model, independent handover confirmation, condition evidence, device/source validation, exception cases and authorized claims exports. Complete real transport/insurance contracts and integrations separately.

Prove the proposed service

Synthetic pilot

Use fictional packages with one broken seal, a missing sensor interval, a clock shift and a receiver count mismatch. Preserve all observations without inferring who caused the damage.

Acceptance tests

Reject a fabricated receiver confirmation, duplicate handover and unsupported sensor identity; detect missing intervals; keep custody and title separate; prevent a model alert from issuing a liability or payout decision.

Measures

Countersigned handovers; package differences; missing-condition coverage; time to assemble a dispute file; false damage alerts and claim corrections.

Proposed payer and economics

Proposed payer: exporter/importer or logistics customer under a scoped record/exception service. Devices, carrier services and independent surveys are separately priced; insurance is not provided by COTO.

Release gate

Assign actual accountable people, permitted evidence sources, cost ceiling, test results, exception handling and rollback. No model may determine rights, certify claims or release money. Keep the affected feature disabled until failures are resolved and required operating/legal approvals are recorded.

Design rights, licences and royalty accountability

COTO design extension, not a PPT extract or activated feature. Synthetic pilots only. No Everledger partnership, integration or certification is claimed. Blockchain preserves a record of an assertion; it cannot make an inaccurate source true.

Intended outcome

Link the actual permission to use a carpet design to each released version and agreed royalty calculation, protecting designers and artisan/community rights without claiming a token creates ownership.

Accountable roles

The actual rights holder grants a defined licence; manufacturer records permitted production/sales; a rights/accounting reviewer checks scope and royalty statements; disputed ownership requires competent legal resolution.

Required evidence

Design/reference digest and version; creator/rights-holder evidence; community/third-party permissions where applicable; licence territory/use/term/exclusivity; production units; royalty base/rate/exclusions; approval and payment references; restrictions on AI use.

Six accountable steps

1. Establish the rights chain / Rights holder + reviewer

Collect documented authorship/assignment/licence evidence and identify traditional, community or third-party elements. A timestamp alone does not prove creation or ownership. Do not ask a coordinator to grant rights it does not hold.

2. Agree a specific licence / Actual rights holder + licensee

Define the design/version, permitted products, territories, term, exclusivity, attribution, AI-input/training permissions and remuneration. Separate an image/publicity release from design rights and from wage obligations.

3. Bind approved production / Designer + production planner

Link the approved file and physical sample to its licence and work order. Record quantity and dates; stop new use if permission expires or is disputed, while addressing legally permitted existing goods and work already done under the real contract.

4. Assist scope checking / AI tool + rights reviewer

Compare submitted designs to authorized references and flag possible unlicensed reuse or out-of-scope variants. Similarity is not plagiarism proof; allow handmade variation, lawful independent creation and an inconclusive result.

5. Prepare transparent royalty statements / Licensee finance + reviewer

Use the exact contractual base and rate with declared units, returns and exclusions. Keep production, sales and payment states distinct; record the rights holder's queries. A contract may not use units produced and units sold interchangeably.

6. Confirm corrections and payment evidence / Rights holder + finance reviewer

Reconcile the statement to evidence and record agreed adjustments. Payment uses the actual lawful route outside COTO. Do not auto-transfer royalties, seize a design or publish a fraud accusation from a model score.

Separate evidence, AI and blockchain

Blockchain role

A future ledger may anchor permission/version digests, scoped approval and royalty-statement attestations with correction/revocation links. Contracts, confidential rates and personal information remain restricted. No NFT or registry entry conveys IP rights by itself.

AI role

Similarity and document-extraction assistance with source links and human legal/creative review. Do not upload licensed/confidential designs to an external model without the actual permitted data route. No universal originality/ownership score is offered.

Exceptions and safeguards

Unclear ownership, community permission gap, expired licence, copied source or disputed royalty base: hold the relevant claim/use for review and retain evidence. Do not withhold lawful wages to fund a rights dispute.

Current / manual route

Use Draft Licence 09 after completion/legal review, a private licence/version register and the existing approved lot/order evidence references. No automated royalty or IP adjudication service exists.

Additional work required

Structured licences/permissions, production/sale linkage, expiry/scope rules, restricted statements, queries/corrections and optional model evaluation. Enforce access and no-training permissions separately from copyright questions.

Prove the proposed service

Synthetic pilot

Use fictional licences with 100 permitted units and a sales-based royalty, then submit an expired variant, unauthorized territory and returned units. Confirm the statement follows the agreed base, not an invented rule.

Acceptance tests

A timestamp cannot clear ownership; a similarity hit cannot condemn copying; expired/out-of-scope use is flagged; duplicate statements cannot create duplicate payment claims; confidential rates stay private.

Measures

Production linked to a valid scoped licence; royalty reconciliation differences; unresolved permissions; false similarity accusations; rights-holder query resolution.

Proposed payer and economics

Proposed payer: licensee/brand under a transparent rights-administration service. The creator's contractual royalty is separate from COTO's fee. No unapproved deduction, compulsory assignment or automatic royalty collection is created.

Release gate

Assign actual accountable people, permitted evidence sources, cost ceiling, test results, exception handling and rollback. No model may determine rights, certify claims or release money. Keep the affected feature disabled until failures are resolved and required operating/legal approvals are recorded.

Repair, resale and recycling provenance

COTO design extension, not a PPT extract or activated feature. Synthetic pilots only. No Everledger partnership, integration or certification is claimed. Blockchain preserves a record of an assertion; it cannot make an inaccurate source true.

Intended outcome

Extend a rug passport beyond first sale with credible condition, repair and material recovery records.

Accountable roles

Current custodian authorizes inspection; qualified repairer records work; seller confirms lawful disclosure; material reviewer checks recovery claims.

Required evidence

Original item reference; authority and possession evidence; condition photos; repair materials; resale description; recovery weights and losses; consent and retention rules.

Six accountable steps

1. Identify the existing rug / Custodian + reviewer

Match physical references and existing identity. A scan does not prove legal title. Investigate missing tags without automatically rejecting an owner.

2. Inspect condition / Qualified examiner

Record wear, contamination and construction limits. Separate observed condition from assumptions; do not promise as-new quality without evidence.

3. Authorize and record repair / Owner + repairer

Agree work, cost and permitted materials. Link before/after evidence and replaced components to the original passport.

4. Disclose resale facts / Actual seller

Publish authorized condition and repair history without previous owner identities. Describe uncertainties and applicable terms.

5. Reconcile recovery / Recycler + material reviewer

Record input weights, recovered outputs, losses and downgraded uses. Allocate recycled attributes once; avoid counting the same content in two products.

6. Correct identity and close / Identity steward

Revoke replaced tags and preserve links. A retired rug cannot remain a second active item when its materials become a new batch.

Separate evidence, AI and blockchain

Blockchain role

Future anchors link approved repair, tag replacement and recovery attestations. Private ownership/contact records stay off-chain; no token automatically transfers title.

AI role

Optional image sorting and repair suggestions, checked by an examiner. No automated safety clearance, resale valuation guarantee or invented recycled content.

Exceptions and safeguards

Uncertain identity, unsafe contamination or disputed title triggers restricted review; incomplete recovery records cannot support a recycled-content claim.

Current / manual route

Use manual passport/repair/material registers linked to existing lot/order references. There is no active resale marketplace or recycling connector.

Additional work required

Lifecycle event types, tag revocation, condition reviews, permissioned resale views and mass reconciliation with double-count prevention.

Prove the proposed service

Synthetic pilot

Synthetic repaired rug, lost-tag replacement, returned goods and a downcycled batch. Reconcile losses and show why repaired is not automatically as new.

Acceptance tests

Block two active identities; preserve original history after repair; reject excess recovered mass; hide previous owners; flag an unsupported as-new claim.

Measures

Identity match exceptions; repair evidence coverage; recovery reconciliation differences; duplicate attributes prevented; authorized disclosure completeness.

Proposed payer and economics

Proposed payer: reseller, repair network or brand through a scoped service. Separate actual repair/logistics costs and avoid guaranteed resale returns.

Release gate

Assign actual accountable people, permitted evidence sources, cost ceiling, test results, exception handling and rollback. No model may determine rights, certify claims or release money. Keep the affected feature disabled until failures are resolved and required operating/legal approvals are recorded.

Grievance, corrective action and independent closure

COTO design extension, not a PPT extract or activated feature. Synthetic pilots only. No Everledger partnership, integration or certification is claimed. Blockchain preserves a record of an assertion; it cannot make an inaccurate source true.

Intended outcome

Give affected people a safe route to raise concerns and check whether corrective action actually reached them.

Accountable roles

A staffed safeguarding lead owns restricted intake; an independent reviewer assesses findings; responsible business implements remedy; affected person can respond and appeal.

Required evidence

Minimal confidential report; safe contact preferences; permission to share; evidence references; allegation versus finding; protective actions; corrective plan; recipient feedback and appeal.

Six accountable steps

1. Provide safe access / Safeguarding lead

Offer assisted local-language intake, safe contact options and clear confidentiality limits. Ordinary feedback email is not a secure vulnerable-person grievance service.

2. Protect and triage / Trained reviewer

Assess immediate protection needs and route urgent concerns to competent services. Collect proportionate evidence; avoid exposing a complainant to a supervisor or alleged wrongdoer.

3. Review fairly / Independent reviewer

Separate allegations from supported findings; hear relevant parties safely. Translation or summary must preserve uncertainty and be checked by a person.

4. Agree corrective action / Responsible business + reviewer

Define action, owner, due date, resources and evidence of completion. Preserve legal rights and protection against retaliation; do not use a model to determine wage entitlements.

5. Check the affected outcome / Independent reviewer + affected person

Seek safe recipient feedback and corroborating evidence. An alleged wrongdoer cannot unilaterally close its own case.

6. Close, appeal or reopen / Authorized independent lead

Record reasons, outstanding concerns and appeal route. Publish only carefully privacy-assessed aggregate trends; no identifying case narrative or linkable complaint digest.

Separate evidence, AI and blockchain

Blockchain role

No personal complaint record or linkable individual digest belongs on a public chain. Only a separately approved, scoped aggregate assurance may be anchored after re-identification assessment; anchoring does not prove remediation.

AI role

Optional translation, redaction and routing assistance under trained human review. No credibility score, labour-violation verdict, worker eligibility decision or automatic closure.

Exceptions and safeguards

Retaliation concern, unsafe contact, mistranslation or reviewer conflict requires protective handling and independent reassignment. Missing response is not acceptance or proof of remedy.

Current / manual route

Existing feedback/contact is an ordinary business route. Safeguarded intake, trained staff and independent review must be established before inviting sensitive reports.

Additional work required

Restricted case store, safe contact controls, access logging, escalation, independent closure, appeal/reopening and privacy-safe aggregation; resource qualified people first.

Prove the proposed service

Synthetic pilot

Fictional withheld pay, retaliation allegation, mistranslation, self-closure attempt and reopened appeal. Use no real vulnerable-person data.

Acceptance tests

Prevent alleged wrongdoer self-closure; block unauthorized access; preserve original language; require recipient-outcome review; stop identifying public exports.

Measures

Safe acknowledgement and outcome times; independent review coverage; recipient-confirmed remedies; reopening and retaliation concerns; privacy incidents.

Proposed payer and economics

Proposed payer: participating businesses under a safeguarded service scope. Access must not depend on a worker paying a fee; financing cannot buy a favourable finding.

Release gate

Assign actual accountable people, permitted evidence sources, cost ceiling, test results, exception handling and rollback. No model may determine rights, certify claims or release money. Keep the affected feature disabled until failures are resolved and required operating/legal approvals are recorded.

An evidence-backed claim model

One claim, one defined scope

Record claim ID, item/batch/site, issuer, period, method, source evidence, reviewer, review date, expiry and correction/revocation links. Preserve unknowns. Different claims on one rug may have different assurance states.

Honest assurance labels

Use supplier-declared, document-checked, source/issuer-confirmed or independently assessed only with the supporting scope and method. Expired, disputed and unknown remain visible. These are not a universal ranking or a blanket verified badge.

Physical and digital binding

A controlled tag/reference record connects the physical item to evidence. A QR scan retrieves information but does not establish title, authenticity or labour conditions. Independent inspection and source checks address the gap between a record and reality.

Permissioned transparency

Show buyers relevant status, dates and gaps; restrict contracts, producer identities, wages and banking data. Store evidence off-chain with controlled retention. Even a hash can be identifying when linked to a person.

Architecture and human responsibility

Capture, check, attest, share, correct

Capture source records; validate structure and units; authenticate issuers where possible; assign human review; issue scoped attestations; share authorized views; append corrections without silently rewriting history.

Separate status dimensions

Maintain evidence review, physical custody, legal title, commercial acceptance, payment and anchoring separately. An anchored invoice is not a paid invoice. A receipt record is not a bank guarantee.

AI as a controlled assistant

Evaluate OCR, matching, translation and anomaly detection against representative manual-labelled samples. Log model/version, source, uncertainty and reviewer outcome. Treat uploaded instructions as untrusted data. No autonomous rights, money or safeguarding decisions.

Current boundary

The pilot has protected trade/audit records and selected workflows. Public blockchain writes, payments, crypto, AI services and the rich evidence services described here remain inactive. A permissioned ledger or selective public anchoring is an architecture decision to validate, not an existing Everledger implementation.

A practical rollout and revenue logic

First: evidence readiness

Pilot certificates, trade-document reconciliation and material lineage using fictional records and reviewed registers. Test revoked documents, quantity mismatches, duplicate events and cross-business access before using real data.

Next: people and physical goods

Resource independent producer-pay and grievance review, privacy controls and safe language support. Validate physical authentication with examiners and genuine variations before making brand-protection claims.

Then: measured environmental and lifecycle claims

Add footprint, logistics and circularity only where source data and qualified review justify them. Missing data remains missing. Evaluate staff burden and false-positive harm alongside speed.

Proposed revenue, not current results

Business subscriptions can support permissions and trade coordination; scoped onboarding, evidence review, integration and passport services may be charged transparently in USD. Separate client funds and trade value from revenue. Disclose independent review/hardware costs; do not sell favourable verification or deduct hidden worker fees.

References and pilot approval

Everledger inspiration

Everledger describes digital asset identities, permissioned provenance and evidence-backed transparency. COTO adapts these principles into original carpet-specific proposals; no affiliation or equivalent capability is asserted.

Method references

GHG Protocol informs bounded product-footprint accounting; NIST AI RMF informs model governance and evaluation. ILO indicators support trained risk detection/referral rather than automated proof of labour violations.

Pilot approval record

Record accountable owner, actual entity, evidence rights, staffed reviewer, data/security assessment, approved costs, legal/provider requirements, test outcomes, unresolved exceptions and rollback. Synthetic success is not commercial traction.

Official sources

<https://everledger.io/our-platform/> | <https://everledger.io/technology/> | <https://ghgprotocol.org/standards> | <https://airc.nist.gov/airmf-resources/airmf/5-sec-core/> | <https://www.ilo.org/publications/ilo-indicators-forced-labour-1>