Genesis One experiment protocol

Version 4.2 · 4 November 2026 · proposed work; no execution results.

Working title: Portable conditional-payment intent and outcome across digital euro prefunding and SME investment settlement.

This is a research specification for the proposed synthetic two-series SME case, not a working prototype. The applicant has identified five expected contributors and their roles in the application; no allocation of hours, supplier endorsement, regulated partner, ECB connection or tested payment capability is asserted here. The participant role and permitted APIs must be confirmed after selection. The financial-instrument, custody, bank and accounting parts remain explicit local models unless separately evidenced.

1 Question contribution and limits

Can a payer authorise a narrowly defined conditional payment and receive the same truthful status and permitted next action across different application implementations when the payment passes from digital euro prefunding into bank money and a separately modelled investment settlement?

The proposed contribution is a portable, versioned description of **intent, authority, money form, observed outcome and next permitted action**. Two independently authored consumers must interpret it consistently without guessing missing facts. The milestone itself is a known payment pattern, not the novelty claim. The research can fail: inconsistent interpretations, missing external references, a need to re-enter material fields, or a false completed state would refute the proposed interoperability benefit.

The format does not move money, transfer a PSP authorisation, create a legal right, guarantee a milestone or make separate ledgers atomic. Genesis preserves a coherent business history while payment providers, banks, the applicable securities system, custody records and accounting retain their respective authority.

The payer benefit is concrete: knowing whether funds left, where they are, what right exists, whether cancellation is still possible, and what to do after an interruption without making a second payment. Accounting traceability is a supporting consequence, not the main AI research topic.

2 Synthetic business fixture

- One Czech SME; one warehouse device costing EUR 20,000; EUR 18,000 initially available to the project.
- One fictitious euro-area individual investor; two distinct bond series, A and B, each one fully paid EUR 1,000 unit at par, with independent terms, subscription, payment and issue references. The illustrative terms are 24 months from each issue and a 4% annual coupon. Coupon payments, maturity, taxation and valuation are outside the primary experiment.
- After A closes, available project funds are EUR 19,000. A EUR 10,000 supplier advance leaves EUR 9,000.

- Delivery produces a EUR 20,000 invoice; offsetting the advance leaves EUR 10,000 payable. B supplies EUR 1,000; paying the balance leaves project cash of zero. The equipment is recorded as ready for use when the relevant conditions hold, independently of B and supplier payment.
- B requires a separate investment decision and a payment instruction authorised before the milestone. The design validity is 24 hours, with no long-term reservation. Amount, payee, collection-account profile, condition version and provider binding are fixed. The model makes the conditional order revocable until the declared cutoff; changing payment consent does not generally cancel a contract.
- The milestone requires the matching device serial and order, a signed acceptance/test record by the designated synthetic technical role, a matching advance/invoice check, and no open dispute. These are authored fixture facts, not AI conclusions or real-world proof.
- The investor pays a modelled authorised collection/distribution arrangement through a PSP. Digital euro receipt and waterfall are separate observations. Bank funds then enter a separately modelled DSS DvP arrangement. The issuer is not assumed to maintain a digital euro balance or to be the initial payment recipient.

3 Boundaries and reference account model

Every account uses a synthetic reference, not a real IBAN or person. The account manifest states holder, servicing institution, currency, money form, legal/client-money model, permitted operations and source authority. These are design choices for simulation, not approved provider arrangements.

Object	Model owner / authority	Permitted interpretation
Payer DE account	Simulated PSP / assigned ECB test interface	Payer funds and PSP-authorised payment state only.
Collection DE account	Synthetic collection-provider profile	Receipt by the collection arrangement; no automatic issuer cash or security ownership.
Linked bank client-money account	Model bank and collection agent	Waterfall credit and per-client allocation; no claim about actual safeguarding law.
DvP settlement cash account	Model settlement bank and DSD arrangement	Cash conditional on securities delivery under the specified model.
Issuer EUR account	Model bank	Issuer cash only on the authoritative successful closing outcome.
Nominee securities account	Model DSD/custodian	Top-tier position under legal_model_id.
Investor custody allocation	Model custodian client ledger	A separately evidenced client entitlement, not inferred from a wallet label.

Object	Model owner / authority	Permitted interpretation
Issuer GL	Model accounting policy and authorised posting process	Recognition, value and period; never inferred solely from a chain event.

The initial profile assumes no fees or FX. An amount mismatch is an exception, not silently reduced investment principal. Future fees require their own consent, posting and reconciliation model.

The normal securities closing requires DvP. Unilateral irreversible cash or securities delivery is a settlement break, not an accepted intermediate step. Independent message arrival times alone do not prove such a break. Legal notary/issue, delivery and subsequent maintenance must be distinguished. Receipts in this experiment model those outputs; they do not validate a live DvP mechanism.

4 Four matched comparison profiles

Each of the 28 scenarios below is planned once in each profile: **28 × 4 = 112 planned scenario runs per frozen release**. A run includes successful A setup, the supplier advance/delivery context appropriate to the scenario, B under test, and reconciliation. A's setup is not counted as an additional run. Each run starts from clean synthetic state.

Profile	Payment path and initiation	Presentation	What the comparison isolates
P1 Bank/manual	Model bank route; payer starts the eligible B payment after the milestone	Structured facts and actions	Conventional manual initiation baseline.
P2 Bank/conditional	Same model bank route; B is authorised in advance and automatically released when eligible	Identical structured facts and actions	P2 versus P1 isolates pre-authorisation/orchestration.
P3 DE/conditional	Model DE route, or assigned ECB interface where supported; waterfall followed by the same local investment model	Identical structured facts and actions	P3 versus P2 isolates rail/interface implications, not automation.
P4 DE/conditional + assistant	Exactly the same financial instructions as P3	Assistant explains verified facts and permitted actions	P4 versus P3 isolates explanation output and interaction burden.

For P1, the same investment condition and eligibility window still apply; a scripted premature or revoked payment attempt must be rejected by the application. There is no claim that the bank provider itself implements our business condition. P2 is a deliberately equally capable conditional bank comparator, so digital euro is not credited for an advantage created merely by unequal application design.

The manual action is supplied by a deterministic test script, not a recruited user. Counts are interface-action counts, not evidence of human preference or time saved. Provider delays and error schedules are matched in local models. Local versus live-test-environment latency is reported separately and cannot establish that one monetary rail is intrinsically faster.

5 State and command contract

State has separate axes: subscription, mandate, milestone, payment, waterfall, dvp, custody, accounting and return. No single Boolean represents completion.

- payment: NOT_SENT / SUBMITTED / PENDING / AUTH_REQUIRED / CONFIRMED / REJECTED / UNKNOWN. CONFIRMED carries the exact provider-defined finality meaning; absent such evidence it must remain pending/unknown.
- dvp: NOT_READY / PREPARED / PENDING / COMMITTED / ABORTED / UNKNOWN / SETTLEMENT_BREAK.
- custody: UNALLOCATED / PENDING / ALLOCATED / BREAK.
- accounting: NOT_DUE / POSTING_PENDING / POSTED / RECONCILIATION_BREAK / RECONCILED.
- A return has its own instruction/reference and status. It never changes a historical payment into “never happened”. A payment refund before issue, redemption after issue and legal unwind are separate operations.

At dispatch, a deterministic guard re-checks amount, currency, collection payee/account profile, provider, condition version, object/serial match, active authority, absence of an open dispute, expiry, revocation and unused instruction identity. Trigger and revocation are serialised against the same mandate version. The application cutoff is recorded as DISPATCH_COMMITTED; it is not bank settlement or payment finality. The sender checks the deadline and the applicable condition, dispute, role and provider-authorisation guards again before transmitting a previously committed but unsent instruction. A detected block is recorded without claiming that the provider received or cancelled a payment.

After dispatch, provider binding and payment instruction ID are immutable. A timeout or failed callback never authorises a new payment through another provider. Retry of the original instruction is allowed only where the actual provider contract guarantees the required idempotence; otherwise query the original reference. Provider-specific authentication requirements override the desired zero-extra-click path. In this fixture, send_by is a deadline for a new authorised submission, not a promise that final settlement will occur before that time. A pending authentication challenge may continue only if the provider deadline and the mandate deadline are both met. An expired mandate does not reverse a payment already accepted by the provider. An unclear acceptance boundary requires an original-status query, not an assumed cancellation or renewed payment.

The assistant has no payment credential or independent command capability. It explains a checked fact bundle. Material instruction fields are validated after generation and cannot be modified by the explanation. A changed amount/payee/condition requires a new explicit authorisation. The assistant must not infer investment quality from milestone success or claim that a hash proves physical delivery.

6 Fixed 112-run matrix

Case IDs become G1-<case>-<profile>-R1. Each row runs in P1–P4. Ordering is frozen before execution. Correct handling of an expected failure is a **logic pass**, not a completed payment.

Case	Injected condition at B	Expected invariant / authoritative end state
C01	Valid milestone, authority and funds	One B payment, one successful model DvP, one allocation and posting; completed position. P1 requires a post-milestone action, P2–P4 do not unless the provider separately requires it.
C02	Milestone never arrives before expiry	No B dispatch, no B instrument; A remains valid.
C03	Milestone evidence is signed by a role not authorised to attest this condition	Milestone rejected; no B dispatch.
C04	New condition/evidence version supersedes authorised version before dispatch	Old mandate cannot silently authorise the changed condition; hold for explicit renewed consent.
C05	Valid revocation wins ordering before dispatch commit	No provider submission; order and mandate cancellation recorded separately according to the fixture contract.
C06	Dispatch wins, cancellation request arrives later; provider reports payment final	Preserve payment; show cancellation could not stop it. Complete lawful model closing or follow the declared contract, never claim a successful cancellation.
C07	Mandate expires before trigger	No B submission.
C08	Mandate valid at commit but expires before actual transmission	Unsent instruction is not sent after expiry; no false payment result.
C09	Duplicate milestone triggers	Exactly one instruction identity and at most one provider payment effect.
C10	Duplicate successful payment callback	Exactly one economic effect, no duplicate DvP, allocation or journal.
C11	Older pending callback arrives after confirmed result	Valid later knowledge is not overwritten by stale status. Conflicting final evidence is quarantined, not resolved by arrival order.
C12	Submit timeout; query of original reference later proves success	One payment effect; no second instruction; recover the original result and continue.
C13	Submit timeout; original status remains unavailable	UNKNOWN, no retry with a new ID/provider, no completed B position. Owner and next permitted action shown.
C14	Provider definitively rejects payment	No issuer financing or B issue; disclosed rejection and permitted re-authorisation path only.
C15	Funds insufficient at trigger	No automatic credit or reduced amount; B not completed; A unaffected.

Case	Injected condition at B	Expected invariant / authoritative end state
C16	Provider requires extra authentication, then scripted approval completes before both the provider deadline and mandate send-by deadline	Visible AUTH_REQUIRED; only after valid provider approval can payment continue. Extra action counted.
C17	DE receipt confirmed, waterfall credit unknown	In P3/P4 client funds open, no issuer cash claim. In P1/P2 inject analogous collection-to-settlement transfer uncertainty, not a fictitious waterfall.
C18	Bank credit is EUR 999 instead of the authorised EUR 1,000	Reconciliation break; no normal DvP/issue based on incomplete or mismatched funds.
C19	Funds prefunded, DvP aborts before either leg is final	No B instrument; funds remain in the defined client regime or separate return process. No issuer revenue.
C20	Model reports irreversible issuer cash while securities delivery definitively failed	SETTLEMENT_BREAK; do not report successful DvP. Stop onward use; model the specific unsettled-subscription/return obligation under the fixture contract.
C21	DvP finality status remains unavailable from its original authorities	Query original cash and securities authorities; do not issue again, refund automatically or claim completion.
C22	DvP completes; custody allocation confirmation is delayed, then arrives	Issuer debt and nominee position persist; payer is not shown an allocated client position prematurely; one eventual allocation.
C23	DvP and allocation complete; ERP export rejects, then corrected export accepted	Rights and money preserved; one posting after versioned repair; no duplicate financing.
C24	Sender crashes after external receipt but before local acknowledgement	Recovery looks up original instruction; one payment effect, no provider failover; preserve original external references.
C25	Manifest reuses A's payment receipt as funding evidence for B	Validation/quarantine; zero unauthorised effects. No inference from plausible UI labels.
C26	The attester was authorised when signing but that role is revoked before B dispatch commit	The fixture requires the attesting role to remain active at dispatch. No B dispatch; a replacement attestation under current authority is required. The historical receipt remains recorded. This is a chosen fixture policy, not a general claim that revocation invalidates earlier acts.
C27	A valid milestone attestation is followed by an open dispute before B dispatch commit	The dispute guard prevents B dispatch; evidence is preserved and the user sees a hold and a human resolution route. The agent cannot dismiss the dispute.

Case	Injected condition at B	Expected invariant / authoritative end state
C28	Extra authentication remains incomplete when the mandate send-by deadline expires; the scripted response arrives later	No accepted payment exists at expiry in this fixture. Do not transmit the late approval or create a B payment. A new mandate is required for a later attempt. If the provider had already accepted the payment, preserve its authoritative status instead; that is not this case.

This is a directed coverage set, not statistical proof of production reliability. It does not cover every possible interleaving or legal failure. Mandatory schema/guard checks also cover altered amount, changed payee, wrong currency, wrong device serial, invalid signatures, unknown schema versions and contradictory final receipts. They are separately recorded validation tests and are not counted as additional payment-journey runs in the 112-case matrix. Future stress, insolvency, multi-investor, secondary-market, maturity and coupon journeys must be separately scoped and counted.

7 Oracle and reproducibility

Before implementation, freeze a fixture bundle containing: schema versions; four profile definitions; 28 cases; synthetic role/account table; legal-model assumptions; expected state vectors at named checkpoints; allowed commands; journal expectations; message schedules; and immutable expected amounts/identifiers. Store its hash and the reviewers' actual approvals once given. Approvals are not claimed in this draft.

Expected outcomes must be authored from this protocol independently of the production state reducer. A test that calls the same reducer to create both actual and expected results is not an independent oracle. The authority fixture emits planned external receipts; the application under test ingests them; a second consumer reconstructs state from exported manifests using a separately authored implementation. Differences are retained, not normalised away.

Each run records source/version, environment, seed or fixed schedule, monotonic time, simulated business clock, every input/output, rejected input, command attempt, external effect, state checkpoint, user-visible message, allowed action, posting, reconciliation difference and verdict. No assertion may rely only on a screenshot. The UI record must reference the facts from which it was rendered.

For P4, freeze model identifier, settings, prompt/template version and the exact synthetic fact bundle. Record each response. A repeat sample is a new documented execution; it must not replace a failed response. The automated assertions check critical amount/payee/status/action facts; expert review checks unsupported assurance, misleading omissions and investment advice. This evaluates outputs, not real-user understanding.

8 Interoperability acceptance

The detailed candidate fields are in the accompanying Candidate event manifest appendix. These acceptance requirements are part of every applicable run:

1. Both consumers read the versioned package without a Genesis database connection or manually re-entered material facts. Private keys and payment credentials are never exported.

2. Both produce the identical authoritative state vector and permitted-action set at each checkpoint. Display wording may differ; material meaning may not.
3. Amounts use integer minor units with currency/exponent; references are namespaced by authority. One provider's accepted must not silently map to another's settled.
4. Every definitive claim identifies its authority, raw external reference and assurance class: LOCAL_MODEL, ECB_TEST_ENV or another explicitly evidenced environment. A missing receipt is not success.
5. Reordered or duplicate messages preserve the declared results; contradictory final evidence opens a discrepancy. Unknown enum/schema versions and missing mandatory fields fail closed into a visible unsupported state.
6. A legal event, message, payment instruction, bank transfer, DvP operation, custody allocation and journal are distinct IDs linked by relationships. A single receipt cannot cover A and B without an explicit allocation model, which this protocol does not permit.
7. A second adapter may map a preselected provider profile or replay evidence as a shadow reader. It must not resubmit an in-flight or unknown payment. Portability of data does not transfer PSP authorisation.
8. Reconciliation can explain the exact amount and owner of each open balance at the common cut-off. Client prefunding, issuer cash and provider revenue are not simultaneously counted as the same owned asset.

Acceptance requires zero unexplained semantic differences in the applicable frozen matrix. It does not certify interoperability with real banks, custodians or ERP products that were not connected.

9 Metrics and pass criteria

Measure	Definition and required reporting
Unauthorised instructions	Number of externally submitted instructions violating a current guard. Required: 0; report attempted and blocked instructions separately.
Duplicate financial effects	Count of more than one provider payment effect, issue/allocation or posting for one permitted economic operation. Required: 0. Duplicate messages themselves are expected.
State/action correctness	Checkpoints matching the independent oracle / applicable checkpoints, with numerator and denominator. Required: 100% for the frozen matrix; report every failed checkpoint.
False completion	UI claims payment, DvP or custody completion without its required authority. Required: 0.
Interoperability	Equal state vectors/action sets across the two consumers / applicable checkpoints. Required: 100%, plus 0 manually repaired material fields.
Traceability	Completed B cases with every required reference and clean reconciliation / completed B cases. Required: 100%; incomplete cases counted separately, not removed from the overall run report.

Measure	Definition and required reporting
Payment completion	Actual completed payment cases / submitted cases, by profile and scenario. No universal success-rate target; induced failures are retained.
Actions after milestone	Scripted payer actions by profile, separating intended initiation, PSP authentication and exception handling. No claim about real-user time or satisfaction.
Time	Measured condition→dispatch, dispatch→provider observation, prefunding→model closing and recovery times. Report environment and sample count; never invent ECB latency. Quantiles only when the actual sample supports meaningful interpretation.
Manual repairs	Number and type of re-entered material fields, operator reconciliations and corrected exports. Compare identical matched cases, not a deliberately degraded bank control.
Assistant fidelity	Unsupported material claims and instruction changes: 0. State all evaluated responses and failed cases; no inferred compliance or investment-safety score.

Completion requires a report distinguishing PASS, FAIL, EXPECTED_OPEN, UNSUPPORTED and NOT_RUN. EXPECTED_OPEN may pass handling assertions while remaining financially incomplete. Unsupported cases are not relabelled as backend success.

10 Accounting and reconciliation checks

Under the declared conditional legal model, successful DvP A/B gives issuer Dr bank / Cr respective bond liability, EUR 1,000 each. Partner prefunding is not issuer cash. A unilateral abnormal cash receipt may create a distinct unsettled-subscription/return obligation under the chosen terms; it is not an alternative normal closing. Earlier enforceable contractual rights would require different recognition and a new legal/accounting model version.

Supplier entries follow the case: Dr advance / Cr bank 10,000; Dr equipment acquisition / Cr payable 20,000; Dr payable / Cr advance 10,000; Dr payable / Cr bank 10,000. Ready-for-use transfer is independent of funding. Journal IDs preserve economic-event references and distinguish posting time from event time.

Reconcile DE receipt to waterfall/client ledger; client funds to settlement cash; DvP cash to delivered nominal; nominee balance to custody allocation; instrument principal to the relevant issuer liability subledger; and posting to its accepted journal reference. Separate principal from carrying value, accrued coupon and future costs. Unresolved timing, posting and unexplained breaks have distinct categories and named functional owners; actual people are assigned only once confirmed.

11 Delivery stages and capability questions

Stage A — design freeze: finalise this protocol, account/legal models, consent text, candidate manifest and independent expectations; confirm actual delivery roles, availability and IP boundaries.

Stage B — local build: implement a narrow instruction/state service, synthetic authority fixtures, structured UI, optional constrained assistant, two consumers and an accounting

export reader. Execute the 112-run matrix locally. A standalone HTML presentation is not this implementation.

Stage C — assigned ECB interface: map only available operations; retain a capability record with method, semantics, authorisation, query/idempotence/cancellation and environments. Execute the supported P3/P4 subset against that interface. There are at most 56 DE-profile entries in the core matrix; unsupported ones remain explicitly marked. Financial-instrument, custody and bank outcomes remain local unless separately connected. Report local and connected counts independently.

Stage D — findings: deliver the reproducible synthetic evidence pack, failed/unsupported cases, schema differences, limits and lessons under the agreed contractual and communication terms. Any publication follows the applicable consent process; public release is not assumed. Keep a change log if ECB specifications require a revised protocol. Never overwrite the frozen initial matrix or count a changed case as an unchanged successful repeat.

Questions requiring confirmation include: permitted recipient/account profile for investment collection; non-reserved conditional initiation; provider authorisation lifetime and extra authentication; reliable original-status query; idempotency scope and retention; cancellation cutoff; meaning of each finality status; waterfall evidence/reference exposure; permitted metadata; rate limits; and permitted local-model/AI use.

No evidence supplied in this draft confirms the answers. If the relevant function is unavailable, the experiment can still report a useful interface gap; it cannot claim the originally proposed backend behaviour was demonstrated.

12 Source and evidence status

The scope reflects ECB's 2026 call: the initial test environment concerns simulated PSP-to-backend interaction, with specifications after selection. The known baseline is ECB's 2025 outcome report, including milestone-based financing. This proposal is a differentiated research hypothesis, not a claim that the general pattern is new.

Current internal evidence supports architectural work, selected identity/audit components and a Genesis testnet. It does not demonstrate this payment protocol, a working PSP connector, live DvP, custody integration or completed 112-run suite. The applicant retains a separate internal source register for existing architecture and component evidence; those records are distinct from results of this proposed experiment. No personal data, real investor information or existing XIX/T19 test imports are included in the proposed dataset. There is no user-testing study in this protocol.

Candidate event manifest field and authority contract

Version 4.2 · 4 November 2026 · proposed interoperable record, not an implemented or accepted industry standard.

This is the field-contract appendix to the Genesis One experiment protocol. The package contains a versioned business manifest, immutable evidence observations and explicitly related operations. It is not a payment authorisation token, a negotiable instrument, a legal title, a public disclosure package or a universal source of external finality.

1 Identity rules

An **event ID** identifies one immutable message/observation. An **economic event ID** identifies one real/modelled economic operation; several observations can concern that operation. A **command ID** identifies one requested action. A **provider operation ID** identifies the external effect. None may be substituted for another.

The same project_id joins the whole project. A and B have separate instrument_id, series_id, subscription_id and payment identities. Payment funding, waterfall, settlement transfer, DvP, supplier advance, invoice, invoice offset and final supplier payment have different economic-event identities. A bank debit and credit that are evidence of the same transfer may share one economic event through typed references; creating a new ID does not create another economic transfer.

Namespaces combine authority and local identifier. No ordering or meaning is inferred from UUIDs. Corrections append an event with supersedes_event_id or corrects_event_id; they do not mutate a signed historical receipt. causation_id means triggered by, not legally guaranteed by.

2 Package-level fields

Field group	Candidate fields	Constraint / authority
Version and scope	schema_id, schema_version, package_id, created_at_utc, environment, dataset_id, case_id, profile_id, release_id	Unsupported mandatory schema version yields visible UNSUPPORTED, not guessed parsing. Environment stated for every external leg as well as package.
Business identities	project_id, issuer_party_ref, investor_role_ref, series_id, instrument_id, subscription_id, legal_model_id, terms_version, terms_digest	Synthetic refs only. Terms digest links exact fixture; it does not prove legality or investor understanding.
Subscription	investment_consent_id, consent_version, consent_authority_ref, consent_time, order_state, withdrawal_rule_id, withdrawal_cutoff_event_ref	Investment consent is distinct from PSP payment authorisation.

Field group	Candidate fields	Constraint / authority
Payment mandate	mandate_id, mandate_version, payer_ref, collection_payee_ref, payee_account_profile_ref, commercial_beneficiary_ref, amount_minor, currency, minor_unit_exponent, purpose_ref, condition_id, condition_version, valid_from, send_by, provider_authentication_deadline, provider_binding_ref, authorisation_receipt_ref	EUR 1,000 = integer 100000, exponent 2. No floats. Amount, payee, provider or condition changes require a new mandate. A syntactic identifier is not proof of authority.
Revocation and cutoff	revocation_event_ref, revocation_effective_at, dispatch_commit_ref, dispatch_committed_at, provider_cancel_ref, cancel_outcome	Authoritative serialisation order, not client clock, decides pre-dispatch race. Sending deadline and applicable guards are checked again at actual transmit. An expired mandate cannot erase an already accepted provider payment; the acceptance boundary is separately mapped.
Milestone	condition_id, condition_version, expected_object_ref, evidence_refs, asserting_party_ref, asserting_role, role_version, evaluated_at, policy_version, role_validity_at_dispatch, evaluation_result, dispute_state, supersedes_condition_ref	Original synthetic evidence has defined provenance. AI interpretation is never authoritative acceptance.
Accounts	account_profile_id, holder_ref, servicer_ref, account_ref, currency, money_form, client_money_model_id, legal_capacity, permitted_operations, effective_version	Distinguish DE, commercial-bank money and securities/client positions. Use placeholders, not real account details. Actual provider capability remains an external requirement.
Operation graph	operations[], each with economic_event_id, operation_kind, parent_project_ref, subscription_ref, command_refs, provider_refs, funding_allocation_refs, relationship_type	Explicit one-to-one cash use for A/B. No implicit shared funding or netting in this model.
Outcomes	state_axes, state_as_of, source_evidence_refs, unresolved_discrepancy_refs, permitted_action_codes, action_reason_refs, knowledge_version	Derived state remains traceable to its authority. A permitted action is not independently a legal opinion.
Presentation	fact_bundle_version, display_amounts, money_location_ref, rights_state_ref, cancellation_state_ref, next_action_ref, assistant_output_ref	Payer application must distinguish funds collected from instrument/client position established. Human-readable labels cannot override structured facts.
Integrity and access	content_digest, digest_algorithm, signature_ref, signer_authority_ref, access_scope, retention_profile, anchor_ref	Optional anchor proves the defined integrity claim only. Hashes and identifiers can be linkable; the synthetic experiment includes no personal information.

3 Immutable observation envelope

Each external or model receipt has: event_id, economic_event_id, source_authority_ref, source_system_ref, source_environment, provider_operation_id, raw_status_code, raw_status_reference, mapping_version, normalised_observation, event_time, received_time, sequence_or_version_if_defined, finality_domain, finality_meaning_ref, evidence_digest, authenticity_check_result, related_command_id, correlation_refs, and supersedes_or_corrects_ref where applicable.

Receipt types include DE_PAYMENT_OBSERVATION, WATERFALL_BANK_CREDIT, CLIENT_LEDGER_ALLOCATION, DVP_OUTCOME, SECURITY_ISSUE_RECORD, SECURITY_DELIVERY_RECORD, CUSTODY_ALLOCATION, JOURNAL_ACCEPTANCE, RETURN_PAYMENT_OBSERVATION and DISCREPANCY_RESOLUTION. Source-specific terms such as accepted, booked and settled require a documented mapping. An asserted finality field without the referenced authority is invalid evidence.

Unknown/missing status is not failure. Two contradictory final receipts produce a discrepancy requiring source resolution. A later arrival cannot overwrite a higher-authority valid result just because its timestamp is later. Authority precedence is defined by domain, not by a single universal source ranking.

4 Financial and legal closing fields

settlement_instruction_id, dvp_operation_id, cash_leg_operation_ref, securities_leg_operation_ref, cash_finality_receipt_ref, securities_finality_receipt_ref, dvp_scheme_model_ref, legal_effective_event_ref, notary_record_ref, issue_date, nominal_minor, nominee_position_ref, custody_allocation_ref, client_entitlement_model_ref, closing_outcome.

Normal COMMITTED requires the specified DvP and legal-model evidence. The issuer's recognition date follows the real/modelled legal effect, not arrival of the UI callback. A client allocation may be pending after the nominee position exists. No completion rule can infer the client's exact legal entitlement solely from a token address.

5 Posting and reconciliation fields

accounting_entity_ref, accounting_policy_version, journal_id, journal_version, economic_event_id, recognition_date, posting_date, period, currency, entries[] with account_role, debit_minor, credit_minor, source_document_ref; prepared_by_role_ref, reviewed_by_role_ref, export_id, acceptance_receipt_ref, reverses_journal_ref, correction_reason_ref.

Reconciliation record: reconciliation_id, scope, cutoff_time, source_a_ref, source_b_ref, expected_amount_minor, observed_amount_minor, difference_minor, difference_category, age_since, responsible_role_ref, next_action, resolution_event_ref, review_status. Principal and carrying value use separate measures; accrued coupon and fees cannot be hidden in a principal mismatch.

Balanced debits/credits are necessary but not sufficient. The journal must refer to the correct legal event and entity. An export rejected by ERP remains an open posting problem while money and rights continue to exist.

6 Candidate interoperability validations

- Reject changes of amount, currency, payee account, provider or condition against the active mandate version.
- Deduplicate immutable observations by authority/event identity; detect reuse of a provider effect for another unauthorised economic operation.
- Require every money-form transition to name source and destination account profiles and linked evidence.
- Preserve external receipt provenance and environment; do not promote LOCAL_MODEL to ECB_TEST_ENV through a later blockchain anchor.
- Require exactly one permitted command lineage per instruction; a new transport message is not automatically a new payment instruction.
- Reject unknown mandatory schema/status semantics visibly. Preserve unsupported raw evidence for investigation without executing financial commands.
- Export a self-contained minimal fact package to the shadow consumer; exclude credentials and non-required original documents.
- Compare state vectors, action codes and accounting links at common checkpoints, not textual equality of natural-language explanations.

7 Example references intentionally incomplete

Project SYN:PROJECT:WAREHOUSE-01 contains subscription SYN:SUB:A and SYN:SUB:B. B authorises EUR 100000 minor units to SYN:COLLECTOR:01, using SYN:ACCOUNT:COLLECT-DE-01, condition SYN:M1:v1, and provider SYN:PSP:01. A separately referenced waterfall changes the money form to commercial-bank EUR; it does not change the authorised commercial purpose or establish a bond. DvP and allocation then have their own references. These names illustrate relationships only and are not a complete executable fixture or valid instruction.

8 Design choices still to freeze before implementation

Choose the actual serialisation/signature/canonicalisation scheme, identifier generation, digest algorithm, access/retention profile and provider-specific mapping once the agreed environment is known. Record the semantics of validity across clock skew and provider acceptance. Define the final legal/client-money model with the accountable roles. None of these open implementation choices can be silently filled by an LLM during payment execution.