Quuipu

SERIE QUUIPU RESEARCH & ARCHITECTURE

WHITEPAPER 04

Semantic Integrity

Preservare il significato nelle esperienze digitali adattive

Whitepaper fondativo · Italiano

Quuipu Edizione 2 · v1

Identità della pubblicazione

Pubblicazione
Semantic Integrity

Serie
Serie Quuipu Research & Architecture

Numero di pubblicazione
Whitepaper 04

Edizione
Quuipu Edizione 2 · v1

Lingua
Italiano

Edizione storica
Cognisphere Edizione 1

Questa pubblicazione succede a Cognisphere Edizione 1. I PDF storici restano immutabili.

Indice

01. La proprietà fondamentale

02. Canonical information

03. Semantic identity

04. Concept identity e relationship integrity

05. Semantic transformation

06. Derived representations

07. Evidence model

08. Claimability

09. Uncertainty

10. Semantic drift

11. Conflicts

12. Versioning

13. Source authority

14. Provenance graph

15. Integrity pipeline

16. Integrity states

17. Semantic fallback

18. LLM e Semantic Integrity

19. Human agency

20. High-trust domains

21. Testing Semantic Integrity

22. Metrics

23. Governance

24. Multi-tenant integrity

25. IP e proprietà definitoria

26. Semantic Integrity invariants

27. La promessa finale

A. Semantic Integrity data model

B. Semantic failure matrix

C. Claimability ladder

D. Semantic Integrity invariants

Preamble

Preservare il significato nelle esperienze digitali adattive

> Questa pubblicazione succede a Cognisphere Edizione 1. Quuipu Edizione 2 preserva la tesi storica aggiornando brand e identità di pubblicazione attivi.

Preamble

Preserving Meaning Across Adaptive Digital Experiences

FOUNDATIONAL PRINCIPLE

Il significato come invariant La forma può adattarsi. L'autorità e il significato materiale non possono cambiare silenziosamente.

Quuipu may change how information is experienced without changing what the authoritative information means.

Canonical Source ↓

Semantic Identity ↓

Evidence ↓

Transformation ↓

Claim Validation ↓

Provenance Binding ↓

Integrity State ↓

Adaptive Experience

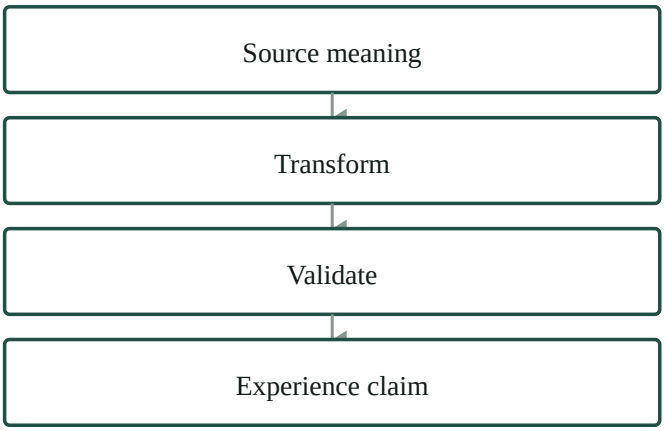


Figure 1 — Catena di Semantic Integrity.

SEMANTIC MODEL

Dal contenuto al claim Object Question Integrity requirement

Source Where does authority originate? Scope + version + authority

Concept What semantic object is this? Stable identity

Evidence What supports the statement? Traceable coverage

Claim What may the system assert? Claimability threshold

Transformation What changed in representation? Invariant preservation

Experience What does the user see? Qualification + source path

CAPITOLO 01

La proprietà fondamentale

Quuipu può cambiare il modo in cui un'informazione viene esperita senza cambiare silenziosamente ciò che l'informazione autorevole significa. Semantic Integrity è il sistema di vincoli che rende questa promessa verificabile.

Experience is variable; meaning is governed Una rappresentazione può essere semplificata, sequenziata, contestualizzata o ricomposta. Queste operazioni modificano forma, ordine e densità, ma non autorizzano il runtime a creare una nuova verità editoriale.

Integrity is not literal sameness Preservare il significato non significa ripetere le stesse parole. Significa conservare condizioni, relazioni, eccezioni, quantità, negazioni, scope e dipendenze che determinano il contenuto semantico della fonte.

A system property Semantic Integrity non è una promessa del modello generativo. È una proprietà dell'architettura: source authority, identity, transformation contracts, evidence, provenance, uncertainty, conflict handling e fallback concorrono alla stessa garanzia.

CAPITOLO 02

Canonical information

Il punto di partenza è distinguere informazione canonica e rappresentazione derivata. Senza questa separazione, l'adattamento rischia di diventare una seconda pipeline editoriale invisibile.

Canonical authority Una fonte canonica è l'autorità riconosciuta dal dominio per una determinata informazione: una pagina istituzionale, un record di prodotto, una policy, una specifica, un documento versionato o altro source system governato.

Canonical does not mean globally true Canonicality è relativa a scope e authority. Due organizzazioni possono avere fonti canoniche diverse; una fonte può essere autorevole per una policy ma non per un dato operativo.

Canonical-first La rappresentazione originale deve rimanere raggiungibile. L'utente e il runtime devono poter tornare alla fonte quando la trasformazione è insufficiente, incerta o contestata.

Canonical change Quando cambia la fonte autorevole, le rappresentazioni derivate devono poter essere invalidate, rigenerate o marcate come stale. La persistenza non deve congelare significati superati.

Layer Owns Does not imply

Canonical source Editorial/operational authority Universal truth

Derived representation Contextual form New canonical record

Provenance Derivation trace Automatic correctness

Integrity state Quality/limits of derivation Technical uptime

CAPITOLO 03

Semantic identity

Semantic identity permette di riconoscere che più rappresentazioni si riferiscono allo stesso oggetto semantico pur avendo forme differenti.

Identity anchor Un concetto necessita di un anchor: source ID, URI, semantic key o altra identità stabile nel dominio. L'anchor impedisce che una parafrasi diventi accidentalmente un nuovo concetto.

Identity across modes Original, Simple e Step-by-step condividono la stessa identità concettuale quando rappresentano la stessa fonte. La modalità è una proprietà della rappresentazione, non dell'oggetto canonico.

Identity across pages La continuità può collegare lo stesso concetto attraverso pagine diverse. Ciò consente a Explore di costruire percorsi senza fondere entità che condividono soltanto termini simili.

Identity and version Identità e versione sono distinte: la stessa entità può evolvere. Il runtime deve poter dire 'stesso concetto, versione diversa' invece di trattare ogni modifica come nuova identità.

CAPITOLO 04

Concept identity e relationship integrity

Un ecosistema adattivo non preserva soltanto singole frasi: deve preservare anche relazioni fra concetti.

Typed relationships Relazioni come requires, applies-to, supersedes, exception-to, part-of o related-to hanno forza semantica diversa. Ridurle tutte a 'correlato' distrugge informazione.

Directionality Molte relazioni sono direzionali. Se A richiede B, non segue che B richieda A. La trasformazione deve conservare direzione e cardinalità quando rilevanti.

Scope

Una relazione può valere soltanto in una versione, giurisdizione, prodotto o condizione. Lo scope deve viaggiare con la relazione.

Relationship provenance Anche i collegamenti usati da Explore devono avere origine: fonte esplicita, regola governata o derivazione qualificata. Una relazione plausibile non è automaticamente canonica.

CAPITOLO 05

Semantic transformation

Una trasformazione semantica è un'operazione controllata che produce una rappresentazione derivata da una o più fonti senza acquisirne l'autorità.

Transformation intent Ogni trasformazione deve dichiarare il proprio scopo: semplificare, decomporre, riordinare, sintetizzare, confrontare o contestualizzare. Scopi differenti richiedono controlli differenti.

Invariant payload Prima della trasformazione è utile identificare il payload che non può essere perso: numeri, negazioni, condizioni, eccezioni, termini normativi, riferimenti, prerequisiti e limiti.

Permitted change Forma, lessico, ordine, granularità e selezione possono cambiare entro il contratto. Authority, claim scope e condizioni materiali non possono cambiare senza qualificazione.

Transformation result Il risultato non è soltanto testo: include representation, source set, transformation type, integrity status, uncertainty e provenance.

Source + scope ↓

Invariant payload ↓

Transformation intent ↓

Candidate representation ↓

Claim validation ↓

Integrity state

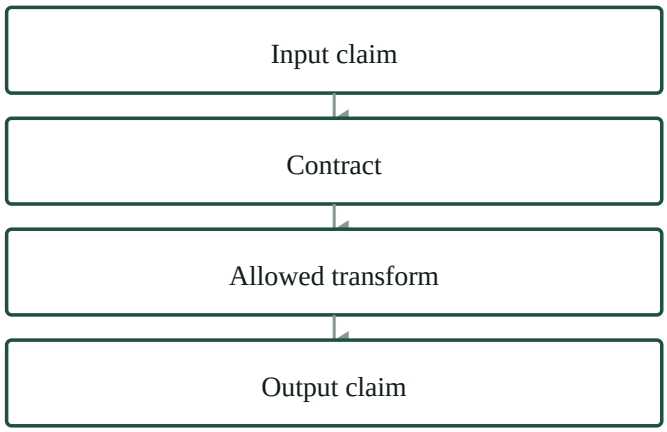


Figure 2 — Contratto di trasformazione.

CAPITOLO 06

Derived representations

Le rappresentazioni derivate sono artefatti di runtime. Il loro valore deriva dalla capacità di rendere una fonte più utilizzabile mantenendo visibile il legame con l'origine.

Original Original è il riferimento canonico o una proiezione fedele della fonte. È il controllo contro cui le altre modalità possono essere confrontate.

Simple Simple riduce complessità linguistica e densità. Non deve eliminare qualificatori che cambiano il significato né trasformare probabilità in certezze.

Step-by-step Step-by-step rende sequenziale un processo o un ragionamento. L'ordine può essere derivato soltanto se supportato dalla fonte o da una regola governata.

Composite representation Quando una risposta combina più fonti, la provenance deve consentire di distinguere quali parti dipendono da quali fonti e dove il runtime ha effettuato una sintesi.

CAPITOLO 07

Evidence model

Evidence è ciò che permette a Quuipu di sostenere una rappresentazione senza confondere plausibilità e supporto.

Evidence unit Un'evidence unit può essere un passaggio, campo strutturato, record o relazione proveniente da una fonte autorizzata. Deve mantenere source identity e localizzazione sufficiente.

Evidence coverage Non basta che una fonte sia genericamente pertinente: i claim materiali della rappresentazione devono avere copertura adeguata.

Evidence strength Una fonte primaria, un dato strutturato e una sintesi secondaria possono avere forza diversa. Il modello deve poter rappresentare gerarchie o policy di authority.

Evidence gaps Se un claim necessario non è supportato, il sistema può ometterlo, qualificarlo, chiedere chiarimento o effettuare fallback. Non deve riempire il gap con confidenza stilistica.

CAPITOLO 08

Claimability

Claimability definisce ciò che Quuipu è autorizzato a presentare come affermazione derivata sulla base delle fonti disponibili.

Claim boundary Una fonte può supportare un fatto ma non una conclusione più ampia. Il runtime deve distinguere ciò che è esplicitamente affermato, ciò che è derivabile e ciò che è soltanto plausibile.

Claim classes Una tassonomia utile distingue canonical claim, supported derivation, qualified inference e unsupported claim. Le classi possono guidare UI e policy.

Material claims Numeri, date, requisiti, obblighi, compatibilità, disponibilità e condizioni sono claim ad alta materialità e richiedono soglie più rigorose.

Refusal as integrity Rifiutare di formulare un claim non supportato è un successo di integrità, non un fallimento dell'esperienza.

Claim class Meaning Default treatment

Canonical Directly stated by authority May be presented as source content

Supported derivation Logically/structurally supported Present with provenance

Qualified inference Plausible but conditional Expose qualification

Unsupported Evidence threshold not met Do not emit as trusted claim

CAPITOLO 09

Uncertainty

L'incertezza non deve essere nascosta dalla fluidità linguistica. Quuipu deve poter rappresentare ciò che non sa, ciò che è ambiguo e ciò che dipende da condizioni non risolte.

Source uncertainty La fonte può essere incompleta, datata o contraddittoria.

Resolution uncertainty Il runtime può non sapere quale fonte, entità o interpretazione corrisponda all'intento.

Transformation uncertainty Una sintesi può essere semanticamente plausibile ma non abbastanza sicura per un contesto ad alta materialità.

Experience projection L'incertezza può produrre qualificatori, alternative, richiesta di chiarimento, ritorno a Original o refusal. Il livello di dettaglio mostrato dipende dal contesto, ma non deve essere falsificato.

CAPITOLO 10

Semantic drift

Semantic drift è la distanza progressiva tra una rappresentazione derivata e il significato attuale della fonte o del concetto.

Source drift La fonte cambia mentre cache o memoria conservano una derivazione precedente.

Model drift Un cambiamento del modello o del prompt può produrre trasformazioni diverse a parità di fonte.

Context drift Una rappresentazione valida in un contesto viene riutilizzata in uno scope differente.

Vocabulary drift Il significato operativo di un termine evolve nel dominio mentre alias e mappe semantiche rimangono invariati.

Drift controls Version binding, invalidation, regression tests, semantic fingerprints e policy review riducono il rischio. Nessun singolo controllo è sufficiente.

Drift Trigger Control

Source Canonical update Version binding + invalidation

Model Model/prompt release Golden regression suite

Context Reuse outside scope Context binding

Vocabulary Domain meaning changes Schema/ontology review

CAPITOLO 11

Conflicts

Le fonti autorevoli possono essere in conflitto. Semantic Integrity richiede di preservare il conflitto quando non esiste una regola legittima per risolverlo.

Conflict detection Il sistema deve poter distinguere differenze di versione, scope e authority da contraddizioni reali.

Authority resolution Una policy può stabilire precedenza: fonte primaria su secondaria, versione corrente su obsoleta, dato transazionale su descrizione editoriale. La precedenza deve essere governata.

Unresolved conflict Se il conflitto rimane, l'esperienza deve mostrarlo o ridurre il claim. Una sintesi che elimina il dissenso senza base è semanticamente scorretta.

Conflict provenance Le fonti in conflitto devono restare identificabili per audit e per l'utente quando rilevante.

CAPITOLO 12

Versioning

Versioning rende il significato temporalmente verificabile. Senza versione, una provenance può indicare la fonte giusta ma il suo stato sbagliato.

Source version Document version, ETag, hash, timestamp o revision ID possono fungere da anchor, a seconda del sistema.

Transformation version Anche regole, prompt, modelli e pipeline che producono la rappresentazione devono poter essere versionati nei contesti in cui la riproducibilità è importante.

Policy version Una stessa fonte può produrre output differenti quando cambiano policy di claimability o trasformazione. La policy è quindi parte della derivazione.

Temporal validity Un output può essere corretto al tempo T e non più corretto al tempo T+1. Integrity richiede di rappresentare questa temporalità.

CAPITOLO 13

Source authority

Authority stabilisce quale fonte ha il diritto di determinare il significato operativo in uno scope.

Authority is contextual Il catalogo commerce può essere autorevole per prezzo e disponibilità; la documentazione può esserlo per specifiche; una policy legale per condizioni. Il runtime deve evitare authority leakage.

Primary and secondary sources Le fonti secondarie possono aiutare a spiegare ma non devono sovrascrivere una primaria quando il claim dipende dall'autorità primaria.

Authority registry Un deployment maturo può mantenere un registry di source classes, scope, priorità e regole di conflitto. Questo è un pattern architetturale, non un requisito che ogni sito debba implementare nello stesso modo.

Authority loss Se l'autorità non può essere determinata, la resolution deve degradare. La sicurezza semantica viene prima della completezza apparente.

CAPITOLO 14

Provenance graph

La provenance più utile non è una nota a piè di pagina, ma un grafo di derivazione che collega fonti, trasformazioni, claim e output.

Nodes Source, source version, evidence unit, transformation, policy, model/capability, claim e representation possono essere nodi distinti.

Edges derived-from, supported-by, transformed-by, governed-by, supersedes e conflicts-with descrivono relazioni operative.

User view versus audit view L'utente può vedere un source link e un indicatore di derivazione; l'audit può richiedere il grafo completo. Le due viste condividono la stessa origine.

Provenance completeness Una rappresentazione può avere provenance parziale. Lo stato deve essere espresso, perché 'provenance presente' non equivale a 'provenance sufficiente'.

Node Example edge Why it matters

Source version supports → Evidence Temporal authority

Evidence supports → Claim Coverage

Policy governs → Claim Claimability

Transformation produces → Representation Derivation

Representation derived-from → Source User/audit trace

Source A conflicts-with → Source B Conflict preservation

CAPITOLO 15

Integrity pipeline

Semantic Integrity deve attraversare l'intera pipeline Quuipu, non essere applicata come controllo finale dopo la generazione.

Pre-resolution Stabilire scope, source authority, version e policy prima di scegliere le fonti.

Resolution Costruire candidate set ed evidence map distinguendo authority e uncertainty.

Transformation Applicare transformation contract e invariant payload durante la generazione.

Validation Controllare claim coverage, contradiction, material terms, provenance e policy.

Emission Emettere representation più integrity state; in caso contrario degradare, qualificare o effettuare fallback.

Authority Resolution ↓

Evidence Mapping ↓

Transformation ↓

Claim Validation ↓

Conflict / Uncertainty Check ↓

Provenance Binding ↓

Emit / Qualify / Fallback

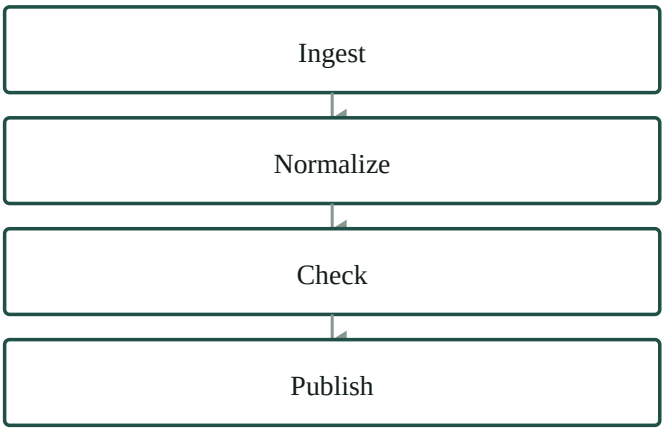


Figure 3 — Pipeline di integrità.

CAPITOLO 16

Integrity states

Un output adattivo ha bisogno di uno stato di integrità distinto dallo stato tecnico del runtime.

Verified I claim materiali sono coperti da evidenza ammissibile e non sono noti conflitti irrisolti nello scope.

Qualified L'output è utilizzabile ma contiene uncertainty, inferenze o limiti che devono essere resi visibili.

Conflicted Fonti ammissibili sostengono claim incompatibili e la policy non consente una risoluzione univoca.

Stale La derivazione è legata a una versione non più corrente o non verificabile.

Insufficient Evidence o provenance non raggiungono la soglia necessaria per emettere il claim previsto.

Rejected La trasformazione viola un invariant o una policy e non viene emessa come esperienza affidabile.

Integrity state Can display? Required behavior

Verified Yes Normal derived experience + source path

Qualified Yes Visible qualification

Conflicted Yes, bounded Expose conflict / alternatives

Stale Usually no Refresh or clearly mark

Insufficient No trusted claim Reduce scope / Original

Rejected No Fallback / refusal

CAPITOLO 17

Semantic fallback

Il fallback semantico è diverso dal fallback tecnico: il runtime può essere perfettamente operativo e tuttavia decidere di non trasformare.

Return to Original Quando la trasformazione non può preservare il significato con sufficiente affidabilità, Original è il fallback naturale.

Reduce scope Il sistema può rispondere soltanto alla parte supportata della richiesta.

Expose alternatives In presenza di ambiguità o conflitto, può mostrare interpretazioni o fonti alternative.

Ask for context Una condizione mancante può essere risolta chiedendo all'utente un'informazione esplicita anziché inferirla.

Refuse Nei claim ad alta materialità, refusal può essere l'unica risposta coerente con l'integrità.

CAPITOLO 18

LLM e Semantic Integrity

Gli LLM possono essere potenti trasformatori semantici, ma non sono l'autorità del sistema.

Model as capability Il modello riceve input bounded e produce candidate output. Source selection, policy, provenance e fallback restano responsabilità del runtime.

Grounding is necessary, not sufficient Fornire fonti al modello riduce il rischio ma non garantisce fidelity. Sono necessari controlli su claim, negazioni, quantità, eccezioni e scope.

No authority by fluency La qualità linguistica non aumenta la claimability. Un output elegante ma non supportato resta non supportato.

Model independence Semantic Integrity deve sopravvivere al cambio di modello. Se la garanzia esiste soltanto per un provider o prompt, non è una proprietà architetturale.

CAPITOLO 19

Human agency

L'integrità semantica serve la persona: non è soltanto un meccanismo di audit.

Inspect source L'utente può raggiungere la fonte canonica.

Switch representation Può confrontare Original e forme derivate.

Correct context Può correggere un intento o uno scope che il sistema ha risolto male.

See qualification Quando il sistema è incerto o il claim è derivato, la UI deve evitare di presentarlo con la stessa forza del canonico.

Exit adaptation L'utente può abbandonare il layer adattivo senza perdere accesso al contenuto.

CAPITOLO 20

High-trust domains

La soglia di integrità deve dipendere dalla materialità del dominio e del claim.

Public administration Requisiti, scadenze e procedure richiedono source authority e versioning rigorosi.

Commerce Prezzo, compatibilità e disponibilità devono derivare dai sistemi operativi corretti.

Technical documentation Versione e piattaforma sono parte del significato; una sintesi cross-version può essere pericolosa.

Education La semplificazione deve preservare il concetto e rendere distinguibili spiegazione, esempio e fonte.

Enterprise knowledge Policy interne, permessi e tenant boundaries limitano non soltanto l'accesso ma anche ciò che può essere affermato.

Domain Material claim Primary integrity risk

Public administration Eligibility / deadline Outdated or wrong authority

Commerce Price / compatibility Authority leakage

Documentation API behavior Version mismatch

Education Concept explanation Oversimplification

Enterprise Internal policy Permission/tenant leakage

CAPITOLO 21

Testing Semantic Integrity

La fidelity deve essere testabile attraverso suite che combinano controlli deterministici, dataset di riferimento e valutazione umana.

Invariant tests Numeri, negazioni, termini obbligatori, condizioni e riferimenti possono essere controllati automaticamente in molti casi.

Golden transformations Casi di riferimento curati consentono regression test tra versioni di pipeline o modello.

Adversarial cases Fonti contraddittorie, obsolete, ambigue o quasi-identiche verificano conflict handling e identity resolution.

Human review Nei domini complessi, esperti di materia devono valutare fidelity e materiality. L'automazione non elimina il bisogno di governance.

Release gates Una capability semantica non dovrebbe essere promossa soltanto sulla base di qualità linguistica: deve superare soglie di integrity, provenance e fallback.

Test family Example Detects

Invariant Negation/number preserved Material omission

Golden Expected transformation Regression

Adversarial Conflicting sources False synthesis

Version Old vs current source Staleness

Human SME Domain review Subtle semantic loss

CAPITOLO 22

Metrics

Semantic Integrity richiede metriche che descrivano qualità della derivazione, non soltanto soddisfazione o latenza.

Claim support ratio Quota dei claim materiali coperti da evidence ammissibile.

Provenance completeness Quota degli elementi derivati per cui source, version e transformation path sono sufficientemente ricostruibili.

Conflict preservation rate Capacità di non cancellare conflitti rilevanti durante la sintesi.

Stale derivation rate Frequenza con cui output serviti risultano legati a fonti superate.

Fallback precision Capacità del sistema di effettuare fallback quando necessario senza rifiutare inutilmente trasformazioni sicure.

CAPITOLO 23

Governance

Semantic Integrity richiede responsabilità organizzative oltre al codice.

Source governance Chi decide quali fonti sono autorevoli e per quale scope?

Transformation governance Quali trasformazioni sono ammesse per quali classi di contenuto?

Claim policy Quali claim richiedono evidenza primaria, doppia fonte o refusal?

Change governance Come vengono gestiti aggiornamenti di fonte, modello, prompt, policy e schema semantico?

Incident governance Una perdita di integrity deve poter essere investigata come incidente di prodotto, con provenance e remediation.

CAPITOLO 24

Multi-tenant integrity

In un'architettura multi-tenant, semantic integrity include l'isolamento del significato e dell'autorità fra organizzazioni.

Tenant-scoped authority La fonte canonica del tenant A non è automaticamente autorevole per il tenant B.

Tenant-scoped semantics Alias, tassonomie e relationship map possono essere specifiche del tenant.

No cross-tenant evidence Evidence di un tenant non deve supportare claim per un altro salvo federazione esplicitamente governata.

Shared core, isolated truth Il runtime può condividere codice e invarianti mentre source authority, policy, state e provenance restano isolati.

CAPITOLO 25

IP e proprietà definitoria

Semantic Integrity può costituire una proprietà definitoria importante di Quuipu. La sua rilevanza come asset IP dipende però da novità, specificità tecnica, implementazione e prior art, e richiede una valutazione professionale dedicata.

What may be distinctive La combinazione fra canonical authority, contextual adaptation, claimability, provenance binding, integrity states e semantic fallback può essere formalizzata come sistema tecnico coerente.

Architecture before claims Prima di parlare di brevettabilità è utile fissare invarianti, data model, pipeline, algoritmi di validation e casi di failure in documentazione tecnica versionata.

No legal conclusion Questo whitepaper non conclude che una particolare idea sia brevettabile o proteggibile. Definisce il territorio tecnico che può essere sottoposto a prior-art search e consulenza IP.

CAPITOLO 26

Semantic Integrity invariants

Gli invarianti condensano la disciplina in regole verificabili che devono restare valide attraverso modelli, host e modalità di esperienza.

Meaning before fluency La qualità stilistica non può compensare una perdita di significato.

Authority before synthesis Prima di sintetizzare occorre stabilire quali fonti hanno autorità nello scope.

Evidence before claim Un claim materiale richiede evidence sufficiente.

Provenance before trust Una rappresentazione derivata affidabile deve poter spiegare da dove proviene.

Conflict before collapse Un conflitto non risolto deve restare visibile invece di essere fuso in una falsa certezza.

Fallback before fabrication Quando l'integrità non può essere preservata, il sistema riduce scope, torna a Original o rifiuta.

CAPITOLO 27

La promessa finale

Semantic Integrity trasforma l'adattamento da semplice capacità generativa a disciplina di sistema.

One concept, many experiences Lo stesso concetto può essere letto, semplificato, sequenziato o esplorato senza perdere identità.

One source, traceable derivations Ogni esperienza derivata resta collegata alla propria origine e al processo che l'ha prodotta.

Adaptive, not arbitrary Il contesto decide quale esperienza è utile; non concede al runtime libertà di cambiare l'autorità.

The principle Quuipu may change how information is experienced without changing what the authoritative information means.

CAPITOLO A

Semantic Integrity data model

Entity Minimum fields Purpose

SourceRef id, uri, authorityScope, version Anchor canonical information

ConceptRef semanticId, sourceBindings, version Preserve identity

EvidenceRef sourceRef, locator, strength Support claims

Claim claimId, type, materiality, evidence[] Represent assertable meaning

Transformation type, version, invariantSet Describe permitted change

ProvenanceRecord sources, evidence, transformation, policy Reconstruct derivation

IntegrityAssessment state, uncertainty, conflicts, reasons Gate emission

CAPITOLO B

Semantic failure matrix

Failure Risk Integrity response

Missing authority Wrong source treated as truth Degrade / refuse

Unsupported claim Hallucinated certainty Remove / qualify / refuse

Lost negation Meaning inversion Reject transformation

Lost condition Over-broad claim Reject or restore condition

Version mismatch Stale guidance Invalidate / refresh

Unresolved conflict False consensus Expose alternatives

Broken provenance Untraceable derivation Do not trust-enhance

Cross-tenant evidence Authority/data leakage Reject + isolate

CAPITOLO C

Claimability ladder

Canonical statement ↓

Evidence-backed derivation ↓

Qualified inference ↓

Unresolved hypothesis ↓

Unsupported assertion

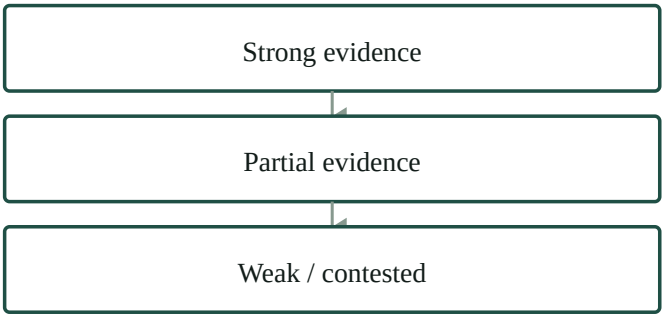


Figure 4 — La claimability diminuisce al ridursi di evidence e authority.

The runtime should become more conservative as materiality rises or evidence weakens.

CAPITOLO D

Semantic Integrity invariants

SI-01 · Canonical authority Every trusted derivation is scoped to an identifiable authority.

SI-02 · Identity preservation Representation change does not silently create a new concept.

SI-03 · Material fidelity Conditions, negations, quantities and exceptions are preserved.

SI-04 · Evidence before claim Material claims require admissible support.

SI-05 · Claimability boundary Plausibility is not permission to assert.

SI-06 · Provenance binding Trusted output remains traceable to source and transformation.

SI-07 · Uncertainty visibility Unknown, ambiguous and conditional states are not rendered as certainty.

SI-08 · Conflict preservation Unresolved authoritative conflict is not collapsed into consensus.

SI-09 · Version awareness Temporal state is part of semantic validity.

SI-10 · Semantic fallback Integrity failure returns to a safer representation rather than fabrication.

SI-11 · Model independence Integrity controls survive replacement of the generative model.

SI-12 · Tenant isolation Authority, evidence and semantic state remain tenant-scoped.

APPENDIX E

Relationship to the Quuipu series Whitepaper Primary question Relationship to Semantic Integrity

01 · The Cognitive Web Why should Quuipu exist? Integrity protects comprehension from becoming distortion.

02 · Architecture How is the runtime structured? Integrity becomes a cross-cutting architectural discipline.

03 · Quuipu Web What changes on a website? Adaptive representations remain bounded by canonical meaning.

04 · Semantic Integrity How is meaning preserved? Formalizes authority, evidence, claimability, provenance and fallback.

Semantic Integrity Preserving Meaning Across Adaptive Digital Experiences

EXPERIENCE MAY ADAPT. AUTHORITATIVE MEANING MUST NOT SILENTLY DRIFT.