

The chain of trust

The foundations of a true digital traceability architecture



Long version

1. Trust begins before transport.

A common mistake: believing that traceability begins with logistics — Traceability is still frequently associated with the physical tracking of goods. In this traditional view, it begins when the resource enters the supply chain and consists primarily of recording its movements until it reaches its final destination. While this approach meets flow management needs, it leaves a crucial question unanswered: how can trust be established if the resource's very origin, the identities of the parties involved, and the conditions of its production are not themselves documented? The true chain of trust, therefore, does not begin with the initial transport. It starts upstream, with the creation of the documentation file that establishes the resource's identity, links the evidence generated throughout its lifecycle, and ensures continuity of responsibility right up to the end user.

Identity precedes movement — Every chain of trust rests on a fundamental principle: a resource can only be tracked, monitored, or leveraged once its identity has been established. This identity goes beyond the mere assignment of a technical identifier; it stems from the coherent combination of information regarding the resource, its place of origin, the authorized parties involved, the relevant permits, and the production context. Only once this identity is established can the successive events of its lifecycle be recorded, linked, and verified. Movement does not create identity; it extends it. Trust thus arises from the continuity between an initially established identity and the evidence produced at each subsequent stage.

The mine site as the primary object of trust — Before a resource can even be identified, transported, or marketed, its place of origin must itself be recognized as trustworthy. The mine site thus constitutes the first object in the documentation chain. Its identification goes beyond mere geographical location; This encompasses its legal status, operating permits, authorized operators, competent authorities, and all information establishing the legitimacy of the activities conducted there. It is based on this documentary identity of the site that the identity of the resources derived from it can be linked. Trust, therefore, does not begin with the first extracted batch, but with the prior qualification of the environment in which that extraction is authorized and monitored.

Identifying cooperatives before the ore — The trust associated with a resource also depends on the prior identification of the organizations involved in its extraction. In the artisanal mining sector, cooperatives constitute the primary operational level of this governance. Their registration involves more than just creating an administrative record; it establishes their documentary identity, verifies their authorizations, identifies the sites where they operate, and links their activities to the competent authorities. Each extracted resource can thus be traced back to an identified organization even before it is formed into a batch. The chain of trust therefore begins not with the ore itself, but with the actors whose legitimacy and responsibilities have been established beforehand.

GoldConnect as an origin registry — A chain of trust requires a registry capable of establishing, from the very beginning, the documentary identity of mining sites, authorized cooperatives, and the initial documentary objects associated with them. This function goes far beyond that of a mere administrative database. It ensures the preservation of foundational information, its integrity, its updating, and its linkage to the events that will subsequently mark the resource's lifecycle. In this architecture, GoldConnect serves as the origin registry. It acts as the documentary anchor point

from which each resource can be linked to its production environment, authorized stakeholders, and the initial evidence underpinning its traceability. The chain of trust thus originates in a structured registry that guarantees documentary continuity from the moment of the first record.

The first NFT: creation of the documentary record — Once the mining site and cooperative have been identified, the chain of trust can advance to the next stage with the creation of the first NFT. This NFT is neither a title of ownership nor a simple digital identifier; it marks the creation of the resource's documentary record. It establishes a unique link between the origin data, authorized stakeholders, production context, and the initial evidence associated with extraction. From that moment on, every subsequent operation—inspection, transport, processing, certification, or transfer—enriches this record without breaking its continuity. The first NFT therefore represents more than just a physical object; it serves as the permanent repository of its documentary identity and the starting point of the chain of trust.

2. Producing evidence rather than tracking objects

Why tracking ore is not enough — Tracking the movement of ore reveals its route but is insufficient to establish its reliability. A supply chain can accurately record transport stages without demonstrating that the resource originated from an authorized site, was extracted by certified operators, or complied with applicable procedures. A true chain of trust goes beyond tracking physical flows; it involves generating, preserving, and linking the evidence accompanying every stage of the resource's lifecycle. Trust is built not on movements, but on the continuity of evidence establishing the origin, the legitimacy of operations, and the accountability of the actors involved throughout the chain.

The digital record becomes the primary asset — In a modern traceability architecture, a resource's value no longer rests solely on its physical characteristics. It also depends on the quality, continuity, and verifiability of the digital record accompanying it throughout its lifecycle. This record compiles the resource's documentary identity, the successive events concerning it, the inspections performed, the transformations undertaken, and the responsibilities assumed by each stakeholder. As this evidence accumulates and remains verifiable, the record becomes the primary basis for trust. While the resource retains its inherent economic value, its credibility with public authorities, financial partners, and markets now hinges on the robustness of its documented history.

Every event generates evidence — A chain of trust advances not merely by recording a resource's movements, but by accumulating evidence linked to each event marking its lifecycle. Extraction, inspection, weighing, transport, transformation, certification, and changes in responsibility all constitute documentary events that enrich the resource's digital record. Each of them adds a piece of dated information, attributed to a specific actor and linked to the initial documentary identity. Trust thus stems less from the existence of a single document than from the coherence of a series of successive proofs, the continuity of which allows the resource's complete history to be reconstructed and each stage to be verified.

Blockchain as an integrity ledger — Generating evidence is not enough to establish a chain of trust; one must also guarantee its integrity over time. Blockchain addresses this requirement. Within a digital governance architecture, its function is neither to create the documented events nor to replace the operational systems that produce them. Instead, it serves as an integrity ledger, enabling the timestamping of essential information, the preservation of its coherence, and the detection of any subsequent modifications. Each piece of evidence thus maintains its link to the preceding and succeeding items within a continuous documentary chain. Trust, therefore, stems not merely from using blockchain, but from its ability to preserve the authenticity, continuity, and verifiability of the evidence comprising the resource's digital record.

VLink: linking evidence rather than copying documents — In a proof-based governance architecture, the goal is not to multiply copies of the same document, but to ensure continuity between evidence produced by different stakeholders. Each certificate, authorization, inspection report, or analysis result remains the responsibility of its legitimate issuer. VLink links these elements to the resource's digital record via verifiable connections, thereby preserving their origin, integrity, and traceability. This approach prevents the proliferation of divergent versions, reduces the risk of document tampering, and allows each piece of evidence to be viewed within the context of its issuance. The chain of trust relies not on document duplication, but

on the coherent organization of relationships between them, ensuring documentary continuity without any break in accountability.

Documentary continuity — Isolated evidence is never sufficient to establish lasting trust. It is documentary continuity that gives the whole its probative value. Each documented event must be linkable to the resource's initial identity, as well as to the evidence preceding and following it, without any breaks or ambiguity. This continuity makes it possible to reconstruct the resource's entire documentary lifecycle—from origin to final use—while identifying the responsibilities successively assumed by each stakeholder. The chain of trust stems not from a mere accumulation of documents, but from their coherent integration within a single, verifiable, and continuously enriched digital file. It is this continuity that transforms a series of information items into a genuine governance architecture.

3. Key players in building trust

A proof is as good as its author — The value of a proof lies not only in its content, but also in the identity of the person who produced it. Weighing does not have the same significance depending on whether it is carried out by an unidentified operator or by a competent authority; a certification only produces effect if its issuer has the necessary legitimacy to establish it. In an architecture of governance by proof, each documentary event is therefore inseparably linked to its author, whose identity, authorizations and responsibilities are themselves documented and verifiable. Trust is not based only on the existence of proof, but on the ability to establish who produced it, in what legal framework and with what level of responsibility. Thus, the credibility of the digital file comes as much from the quality of the evidence as from the trust placed in those who issue it.

WorldKYC as an identity infrastructure — The reliability of a chain of trust depends on the ability to positively identify the actors who produce, validate or use documentary evidence. This requirement goes beyond traditional identity verification procedures; it involves sustainably linking each natural person, legal entity or public authority to their authorizations, their responsibilities and the actions they carry out within the system. In this architecture, WorldKYC fulfills the function of identity infrastructure. It makes it possible to establish a verified digital identity, associate it with the corresponding intervention rights and guarantee that each proof can be attributed to an authenticated actor. Trust is thus not only based on the validity of documents, but also on the certainty of the identity of those who produce, approve or control them.

Institutional authorizations — The identification of an actor is not enough to guarantee the legitimacy of its interventions. An architecture of governance by evidence must also establish the authorizations which define the rights, responsibilities and limits of action of each person. Each documentary operation – recording an extraction, validating a control, certifying an analysis, authorizing transport or approving a transformation – can only be carried out by an actor with the corresponding skills and authorizations. Authorizations thus become a constituent element of the chain of trust. They make it possible to verify not only who produced evidence, but also whether this actor was actually authorized to do so at the time of his intervention. The credibility of the digital file therefore rests as much on the validity of the authorizations as on the authenticity of the evidence itself.

Successive responsibilities — A governance architecture through evidence does not aim to dilute responsibilities between the different stakeholders, but on the contrary to precisely identify them at each stage of the resource life cycle. Each actor takes responsibility for the operations it carries out and the evidence it produces, while subsequent actors rely on these elements to accomplish their own missions. The documentary chain thus establishes a continuity of responsibilities, in which each intervention is dated, attributed and placed in its context. This organization makes it possible to accurately reconstruct the resource's journey, identify the origin of a possible anomaly and determine the corresponding responsibilities. Trust thus results from a succession of clearly established responsibilities, and not from an indiscriminately shared responsibility.

Continuous compliance — In a "governance-by-evidence" architecture, compliance is no longer the result of a check performed at a specific point in time; instead, it is built throughout the resource's lifecycle. Each new piece of evidence, control, validation,

and change in responsibility adds to the digital record, enabling continuous assessment of adherence to applicable requirements. Compliance thus shifts from a reactive approach based on ad-hoc audits to a continuous process of updating and verification. This approach enhances the ability of authorities, economic operators, and institutional partners to maintain a reliable, documented, and verifiable view of the resource's status at any time. Trust is no longer based on preparing for an inspection, but on the persistent availability of evidence that makes such an inspection possible at any moment.

TrustSignal: the trust orchestrator — A governance-by-evidence architecture cannot simply collect, store, and link information. It must also be capable of consistently and continuously assessing whether the evidence produced meets the requirements set by competent authorities and applicable rules. Within this architecture, TrustSignal acts as the trust orchestrator. Using verified identities, authorizations, documented events, and recorded evidence, it applies governance rules to assess the compliance of operations, detect potential inconsistencies, and flag situations requiring verification or intervention. Trust is thus no longer based on a one-off interpretation of information, but on a continuous, transparent, and reproducible assessment of available evidence. TrustSignal transforms a documentary chain into a genuine governance chain, where every decision can be justified by a coherent set of verifiable evidence.

From compliance to continuous vigilance — Trust is not built solely during the identification of actors or the verification of transaction compliance; it must also be maintained throughout their execution. In this context, a platform such as FraudTrack complements identity and governance mechanisms by helping to detect anomalous behaviors, vulnerabilities, and signals that could indicate a fraud attempt. Its goal is not to replace the competent authorities, but to strengthen their capacity for analysis, prevention, and intervention, ensuring that the chain of trust remains a chain of constant vigilance.

4. Logistics is becoming a legal chain.

Each transfer becomes a transfer of responsibility — In a governance-by-proof architecture, the movement of a resource is not merely a logistical event. Each handover between two actors also entails the transfer of documented responsibility. The carrier, laboratory, regulatory authority, refinery, or certifying body does not simply assume physical custody of the resource; they successively become accountable for the operations they perform and the evidence they generate. Consequently, every change of custodian is accompanied by a new documentary event linking the resource to its new responsible party, within the scope of their recognized authorizations. The supply chain thus transforms into a legal chain, where each transfer establishes a continuity of responsibility, ensuring that the resource's origin, compliance, and custody remain demonstrable at every stage of its journey.

The Air Waybill as proof — In a governance-by-proof architecture, logistics documents take on new significance. The air waybill—traditionally used to organize and certify the air transport of goods—also becomes documentary evidence of the continuity of the chain of trust. It is no longer limited to recording a physical movement; it establishes the transfer date, the identities of the parties involved, the nature of the transported resource, and the responsibilities assumed during that phase of the journey. Linked to the resource's digital record, it forms part of an unbroken sequence of evidence connecting each custodian to the next. The logistics document thus ceases to be a mere administrative record and becomes a constituent element in demonstrating origin, documentary continuity, and accountability throughout the chain.

Eliminating blind spots — The robustness of a chain of trust is measured by its ability to eliminate areas of uncertainty that may arise during a resource's lifecycle. Any break in the documentary trail, any unrecorded transfer, or any intervention by an unidentified actor creates a blind spot that can undermine the credibility of the entire system. Conversely, a governance architecture based on evidence aims to ensure information continuity across every stage by systematically documenting changes in responsibility, operations performed, and the associated evidence. The goal is not to eliminate all risk, but to ensure that no significant step remains without an identified actor, justification, or verifiable record. Trust thus emerges from the progressive reduction of "grey areas" in favor of complete, verifiable documentary continuity.

Reconstructing an audit years later — The value of a chain of trust is also measured by its ability to reconstruct a resource's full history years after the events took place. Thanks to documentary continuity, it becomes possible to reconstruct the sequence of events marking the resource's lifecycle, identify the actors involved, verify their authorizations, review the evidence they produced, and place each operation in its proper context. Auditing no longer relies on hunting down scattered documents or depending on organizational memory; instead, it draws on a digital record built up during operations and preserved intact. This capacity for reconstruction enhances legal certainty, facilitates retrospective checks, and makes it possible to demonstrate—objectively and verifiably—the conditions under which the resource was produced, transformed, and transferred.

5. Seamless transformation

The ore changes, the identity remains — The lifecycle of a natural resource is marked by a series of transformations that gradually alter its physical form. The ore becomes concentrate, then a small ingot, a refined ingot, or a marketable product. However, these material changes do not disrupt the continuity of the chain of trust. Each transformation generates a new documentary event that establishes a link between the resource's previous and subsequent states, while preserving its documentary identity. Thus, even as the material changes in nature throughout industrial operations, its history remains continuous, verifiable, and linked to the same digital record. Governance based on proof ensures that the transformation of the resource never entails a break in its documentary identity.

Parent-child relationships — Documentary continuity involves more than just recording the successive transformations of a resource; it also establishes lineage relationships between its various forms. Each new state—concentrate, small ingot, refined ingot, or finished product—remains linked to its preceding state through an explicit documentary relationship. These "parent-child" relationships make it possible to reconstruct the resource's complete genealogy, from extraction to final use. They ensure that every transformation retains a record of its origin while creating a new documentary identity suited to its new state. The chain of trust, therefore, does not merely track objects; it preserves the continuity of the links connecting the successive states of a single resource.

Refining adds proof — Refining is a pivotal stage in the lifecycle of a mineral resource, yet it does not break the chain of trust. On the contrary, it adds a new category of evidence to the resource's digital record. Purity analyses, quality checks, refining certificates, and the identification of the resulting new products complement the data recorded since the extraction stage. Each piece of information remains linked to prior documentary records through clearly established lines of descent. Refinement does not replace evidence of origin; rather, it extends it by attesting to transformations carried out according to identified and verifiable procedures. Trust is thus built through the progressive enrichment of the documentary record, with each stage reinforcing the demonstration of the resource's origin, quality, and continuity.

The Product Passport — Upon completion of the various stages of its lifecycle, the resource is accompanied by a Product Passport that compiles key information regarding its documentary identity in a structured format. This passport is neither a mere certificate nor a standalone document; it provides organized access to the body of evidence underpinning the chain of trust. It allows for the review of the resource's origin, the parties involved, successive transformations, checks performed, certifications obtained, and responsibilities assumed at each stage. The Product Passport does not create new evidence; instead, it makes the evidence already contained in the digital record accessible, understandable, and verifiable. It thus serves as the interface of trust between the resource and the various authorities, business partners, and users called upon to assess its provenance, compliance, and history.

Trust becomes visible — A governance architecture based on evidence fundamentally transforms how trust is assessed. It no longer relies on declarations, isolated certifications, or the reputation of the parties involved; instead, it becomes objectively verifiable through a coherent set of proofs organized across the resource's entire lifecycle. Every identity, authorization, transformation, transfer of responsibility, and control contributes to making the documentary continuity accompanying the resource

visible. The Product Passport provides an accessible representation of this history without replacing the underlying evidence. Trust thus ceases to be a mere perception or promise; it becomes a demonstrable attribute of the governance system itself, enabling public authorities, business partners, and financial institutions to base their decisions on objectively verifiable data.

6. The chain of trust as a reference framework

The ten requirements for a credible architecture — A genuine chain of trust cannot be reduced to a single technology, ledger, or digital platform. It arises from the coherent integration of several complementary functions that underpin its credibility. A robust architecture must, in particular, be capable of establishing the documentary identity of resources, verifying the identity of actors, managing their authorizations, generating evidence for every significant event, guaranteeing the integrity of that evidence, maintaining continuity, documenting transfers of responsibility, preserving the lineage between the resource's various states, consistently applying governance rules, and making the entire system intelligible through a shared framework such as a Product Passport. Only when these requirements are met does trust become a demonstrable property of the system, rather than the result of a mere declaration of conformity.

Why a single break weakens the whole — A chain of trust derives its credibility from the continuity of the evidence that constitutes it. If a significant step can no longer be documented, an actor can no longer be identified, an authorization can no longer be verified, or a transfer of responsibility remains unjustified, the entire chain of evidence is compromised. Such a break does not necessarily invalidate all preceding or subsequent evidence, but it introduces an area of uncertainty that affects the ability to establish complete documentary continuity. The robustness of a governance architecture therefore depends not only on the quality of its individual components but also on their seamless interconnection. A chain of trust is truly credible only if each link remains connected to the preceding and succeeding ones, without creating any discontinuity in the resource's documentary history.

From technical evidence to institutional trust — Digital technologies now make it possible to generate, store, and link evidence with a high level of reliability. However, their true value lies not in their technical performance, but in their ability to meet the requirements of institutions responsible for monitoring, certifying, financing, or regulating economic activities. Evidence only fully achieves its significance when it can be understood, verified, and recognized by all the authorities and partners required to base their decisions on its content. The chain of trust thus establishes a common language among operators, government agencies, oversight bodies, and financial institutions. Governance based on evidence therefore does more than just transform traceability technologies; it creates the conditions for institutional trust grounded in evidence that is objective, transparent, and verifiable over the long term.