World Journal of Management Science
Print ISSN: 2959-9628
Online ISSN: 2959-9636
DOI: https://doi.org/10.61784/wms3129

HOW DOES DIGITAL TWIN–BLOCKCHAIN INTEGRATION ENHANCE TRACEABILITY TRUST? A PHYSICAL–DIGITAL–TRUST TRIPLE MAPPING MODEL

LiXia Lei*, LiJuan Wang, Mang Ba
School of Business Administration, Chongqing Sanxia University of Science And Technology, Chongqing 404100, China.
**Corresponding Author: LiXia Lei*

Abstract: Agricultural traceability increasingly combines digital twins with distributed ledgers, yet the two technologies are often treated as if co-deployment were enough to create trust. This paper challenges that assumption. It treats traceability trust as the result of three linked translations: physical events into a digital representation (representational fidelity), that representation into a tamper-evident record (evidential integrity), and the record into evidence that stakeholders can inspect and understand (verification confidence). Using affordance theory, signaling theory and the trust literature, the paper explains why these translations operate sequentially, why a weak translation can produce false assurance, and why consumers, firms and regulators attach different weights to the three qualities. Nine propositions and a focused research agenda follow from the argument. The contribution is a configurational account that connects traceability design to the judgments stakeholders make about provenance.
Keywords: Traceability trust; Digital twin; Blockchain; Affordance theory; Signaling theory; Supply chain transparency

1 INTRODUCTION

Agri-food buyers rarely observe the practices behind a product. They know less than producers about growing conditions, handling and custody, and this informational disadvantage grows as products move through long and fragmented supply chains [1]. Traceability arrangements are meant to narrow the gap by preserving a product's history and making it available to parties with a legitimate interest [2-3]. Their value, however, depends on more than the presence of a record. If buyers dismiss the record as incomplete, self-serving or unintelligible, the infrastructure has not solved the underlying problem; it has merely given it a digital form.

Two technologies dominate current proposals. A digital twin maintains a data-connected representation of a physical object or process; in agri-food it can follow a batch, a cold-chain container or a processing line, and it can project how temperature, humidity or custody conditions will evolve [4-5]. A blockchain supplies a replicated ledger whose entries are difficult to alter after acceptance; in a traceability setting it can register claims, execute rules through smart contracts and leave an audit trail [6-7]. The first technology promises visibility. The second promises evidence that the visible claim has not been quietly changed.

The combination is therefore appealing: observation from the twin, durability from the ledger [8-10]. Yet a working system can still mislead. A ledger may preserve an inaccurate reading with great precision; a detailed twin may be unavailable to the consumer it is supposed to reassure; and a verified hash may mean little to someone who cannot interpret it. When an apparently rigorous system is later shown to have recorded a falsehood, the reaction can be sharper than if no claim of rigor had been made. We treat this as the false assurance paradox.

The paradox has remained difficult to explain because the relevant work sits in separate conversations. Digital-twin research has focused on model construction, synchronization and simulation, and has paid less attention to the conversion of twin outputs into trusted evidence [11-12]. Blockchain studies have emphasized immutability, consensus and smart contracts, sometimes treating on-chain data as credible by construction while leaving source validity outside the analysis [13-15]. Trust research offers a nuanced account of ability, integrity and benevolence [16-17], but has seldom examined digitally mediated provenance. The result is a missing link between technical design and the judgments that make a traceability system socially useful.

This paper develops a physical–digital–trust triple mapping model to address that link. The model starts with three translations. M1 moves from a physical event to a digital twin and produces representational fidelity. M2 moves from the twin to a ledger and produces evidential integrity. M3 moves from the ledger to a stakeholder and produces verification confidence. The three translations are ordered: a later mapping cannot repair what an earlier one has already lost. This is why the model treats their effects as configurational and multiplicative rather than as independent contributions that can substitute for one another.

Affordance theory, signaling theory and trust research perform different tasks in the argument. Affordance theory clarifies what the technologies make possible: twins support observability, ledgers support non-repudiation, and their combination supports observability that can be checked [18-20]. Signaling theory explains how those possibilities become evidence for a receiver [21-22]. Trust research explains why receivers interpret evidence in terms of

© By the Author(s) 2026, under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0).

competence, integrity and benevolence [16, 23]. The model links these traditions through the three translations rather than treating them as parallel explanations.

Four contributions follow. First, traceability trust is redefined as a configurational outcome rather than a platform attribute. Second, the paper introduces fidelity, integrity and verification confidence as mapping qualities that can connect technical design to managerial consequences. Third, it uses those qualities to explain why integrated systems can produce false assurance. Fourth, it derives nine propositions that specify what should be measured and compared in future work. The next section reviews the theoretical background; the sections that follow develop the model, state the propositions and discuss implications.

2 THEORETICAL BACKGROUND

2.1 Traceability and Trust

Traceability is conventionally defined as the ability to identify and follow a product, or its components, through specified stages of production and distribution [2-3]. It has two dimensions: tracing, which follows a product forward from origin to consumption, and tracking, which follows it backward from consumption to origin. Bosona and Gebresenbet add a logistical dimension, arguing that traceability is not only a record but a capability embedded in supply chain processes [24]. In agri-food, traceability is motivated by food safety, quality assurance, regulatory compliance, and, increasingly, sustainability claims.

Trust is a willingness to be vulnerable to another party based on the expectation that the party will act competently, honestly, and benevolently [16]. Applied to traceability, three objects of trust must be distinguished. The first is trust in the product: the belief that the item is what it claims to be. The second is trust in the system: the belief that the information infrastructure captures and preserves relevant facts. The third is trust in the actors: the belief that producers, processors, and retailers do not manipulate the record. These objects are related but not reducible to one another. A consumer may trust a brand while distrusting its blockchain, or trust the technology while distrusting the firm that operates it.

This paper defines traceability trust as a stakeholder's confidence that provenance information is complete, accurate, and verifiable. The definition deliberately combines three properties that the literature often treats separately. Completeness concerns coverage: whether all relevant stages and transformations are recorded. Accuracy concerns fidelity: whether the record corresponds to what actually happened. Verifiability concerns access and evidence: whether a stakeholder can independently check the claim. A system that is complete but inaccurate, or accurate but opaque, generates a different kind of trust problem than a system that is simply absent.

Trust in technology has been shown to shape adoption alongside perceived usefulness and ease of use [25], and trust in automation is calibrated to perceived reliability rather than to technical sophistication [26]. These findings suggest that trust is an evaluative accomplishment, not a design feature, which is why the present model locates trust in the mappings between systems and stakeholders rather than in the systems themselves.

Prior research has examined trust in food labels, certification, and supply chain partners, but less is known about trust in digitally mediated provenance. Studies of blockchain traceability often assume that immutability produces trust, yet this assumption conflates trust in the record with trust in the recorded fact. Studies of transparency similarly assume that more disclosure produces more trust, although disclosure can also generate confusion or suspicion [27-28]. The present paper takes these observations as a starting point for a more precise account of how trust is produced across the chain from physical event to stakeholder judgment.

2.2 Digital Twins: Representation, Synchronization, and Fidelity

A digital twin is a virtual representation of a physical entity, process, or system that is connected to its physical counterpart through data [4]. Kritzinger et al. distinguish three levels of integration: a digital model, which is a representation without automated data exchange; a digital shadow, in which data flow from the physical to the digital entity is automatic; and a digital twin, in which data flow in both directions and the physical entity can be influenced by the digital one [11]. This distinction matters for traceability, because only the higher levels support real-time monitoring and intervention.

Tao et al. describe the digital twin as comprising physical entities, virtual models, data, and services [5]. In agri-food, the physical entity may be a batch of produce, a cold-chain container, a processing line, or an entire supply network. The virtual model may represent product state (temperature, humidity, ripeness), process state (harvest, packing, transport), or network state (location, custody, dwell time). The data layer connects sensors, records, and transactional systems; the service layer provides monitoring, simulation, and decision support.

For the purposes of this paper, three dimensions of twin fidelity are relevant. Structural fidelity concerns whether the model represents the right entities and relationships. Data fidelity concerns whether the values in the model correspond to the physical state. Temporal fidelity concerns whether the model is updated quickly enough to represent the state that matters for a decision. A twin can be structurally rich but temporally stale, or temporally current but structurally simplistic. Each limitation constrains what the twin can warrant.

Digital twins have been applied to manufacturing, smart cities, and healthcare, and increasingly to agriculture and food supply chains [12, 29]. Their promise for traceability lies in observability: they make the state of a product or process visible in a way that paper records cannot. Their limitation lies in authority: a twin is an interpretation, produced by a

particular model, calibrated with particular data, and operated by a particular organization. Observability alone does not establish that the interpretation is correct or that the operator is trustworthy.

2.3 Blockchain: Immutability, Consensus, and the Oracle Problem

A blockchain is a distributed ledger in which transactions are grouped into blocks, cryptographically linked, and replicated across nodes [6]. Its core properties are immutability, transparency, and decentralized consensus. Smart contracts extend these properties by encoding rules that execute automatically when conditions are met. In supply chains, these properties are used to record custody transfers, certify provenance, and automate payments or penalties [13-14].

The phrase "trustless" is often used to describe blockchain systems, but it is misleading in the context of traceability. Blockchains reduce the need to trust a central record-keeper, but they do not eliminate the need to trust the inputs. This is the oracle problem: a ledger can faithfully record whatever it is told, but it cannot verify that the input corresponds to reality [15]. If a sensor is miscalibrated, a custodian misreports a transfer, or a producer enters false data, the ledger will preserve the falsehood with perfect integrity.

Reviews document applications across coffee, pork, mango, and seafood [30-32], while studies of supply chain integration emphasize that value depends on process redesign rather than on technology adoption alone [33-34].

A second limitation concerns interpretation. Immutability is valuable to auditors and regulators, but it can be counterproductive for consumers, who may find cryptographic proofs unintelligible or may misinterpret a hash as a guarantee of quality. A third limitation concerns governance. Who has permission to write to the ledger, how disputes are resolved, and how errors are corrected are organizational questions that technology cannot settle. These limitations do not diminish the value of blockchains; they locate that value precisely: blockchains provide evidential integrity, not factual truth.

2.4 The Integration Gap

Table 1 compares three configurations: digital twin only, blockchain only, and integration. A twin-only system offers rich observability but concentrated authority; its records can be altered by the operator, and stakeholders must trust that operator. A blockchain-only system offers strong integrity but weak source validation; it can preserve a claim immutably without establishing that the claim is true. An integrated system, in principle, combines the strengths of both: the twin supplies structured, real-time representations of the physical world, and the ledger anchors those representations in a tamper-evident record.

Table 1 Digital Twin, Blockchain, and Integration: Capabilities and Limitations for Traceability Trust

Configuration	What it provides	Core limitation	Trust problem
Digital twin only	Rich, real-time observability of product and process state	Concentrated authority; records can be altered by the operator	Stakeholders must trust the operator
Blockchain only	Immutable, auditable, non-repudiable records	No validation of source data; oracle problem	Immutability of unverified claims
Integration	Verifiable observability: twin states anchored on a ledger	Requires alignment of fidelity, integrity, and verifiability	Weakest-link failure; false assurance if misaligned

Yet the integration literature has largely described architectures rather than mechanisms. Studies propose layers, protocols, and data flows, but they rarely explain why the combination should produce trust, for whom, or under what conditions. The implicit model is additive: twin plus blockchain equals more trust. The argument developed below is different. It treats the combination as a chain of mappings whose weakest link determines the trust outcome, and it specifies the conditions under which integration produces assurance rather than the appearance of assurance.

2.5 Affordance and Signaling Foundations

Affordance theory explains why the same technology can produce different outcomes in different contexts. Gibson introduced the concept to describe the possibilities for action that an environment offers to an actor [18]. Hutchby extended the idea to technologies, arguing that artifacts have affordances that both enable and constrain use, but that the actualization of those affordances depends on the user and the setting [19]. Majchrzak and Markus applied the concept to information systems, distinguishing between what a technology affords and what users actually do with it [20].

Applied to traceability, digital twins afford observability: they make the state of a product or process available for inspection, simulation, and comparison. Blockchains afford non-repudiation: they make it difficult to deny or alter a recorded claim. Integration affords verifiable observability: the possibility of checking a representation against a record that cannot be quietly changed. This last affordance is not the sum of the first two; it emerges from their combination and depends on the mappings that connect them.

Signaling theory explains how affordances become credible to stakeholders. Spence showed that signals are credible when they are costly to fake, and Connelly et al. extended the logic to organizational contexts [21-22]. A traceability system emits signals—labels, certificates, hashes, dashboards—and stakeholders interpret those signals as evidence about unobservable qualities. Blockchain increases the cost of falsifying a signal once it is on-chain, but it does not

increase the cost of entering a false signal in the first place. Digital twins increase the bandwidth and granularity of signals, but they do not prevent selective representation.

Combining the two lenses yields a precise formulation of the model's logic. Fidelity increases the informational content of the signal; integrity increases its cost of falsification after entry; verification confidence increases the receiver's ability to assess it. A signal that is rich but cheap to fake, or costly to fake but poorly grounded, will not sustain trust. The triple mapping model is, in this sense, a theory of signal quality across the chain from physical event to stakeholder interpretation.

2.6 The Agri-Food Context: Perishability, Fragmentation, and Provenance

Agri-food supply chains place particular demands on the model. Products are often perishable, which raises the value of timeliness; a traceability system that reports conditions after spoilage has occurred cannot support preventive action. Production is often fragmented across smallholders, which complicates coverage and increases the heterogeneity of data quality. Geographical indications and regional brands add a collective reputation dimension: the credibility of a claim about one producer affects the reputation of an entire region.

The Three Gorges Reservoir Area illustrates these conditions. The region's mountainous terrain, dispersed plots, and long transport distances make cold-chain monitoring difficult and expensive. Specialty products such as navel oranges, late-ripening citrus, kiwifruit, plums, and tea depend on provenance claims that distinguish them from substitutes. Smallholders often lack the capital to install sensors, and intermediaries may control the data infrastructure. In this setting, the weakest link is frequently M1: the physical-to-digital mapping, where sensing is sparse and calibration is uncertain.

These contextual features do not change the logic of the model, but they change the parameters. Timeliness and coverage become more consequential, because perishability and fragmentation increase the cost of missing data. Verification confidence becomes more difficult to achieve, because the actors who most need assurance may have the least capacity to check. The model therefore predicts that interventions focused on ledger technology alone will have limited effects in this context, while interventions that improve sensing, calibration, and shared verification infrastructure will have larger effects.

2.7 Conceptual Boundaries: Trust, Trustworthiness, Transparency, and Reliance

A theory of traceability trust must distinguish trust from related constructs. Trustworthiness is a property of an entity—its ability, integrity, and benevolence—whereas trust is a stakeholder's willingness to be vulnerable based on that property [16]. A system can be trustworthy without being trusted, and it can be trusted without being trustworthy. The model is concerned with the second relationship: how system properties become grounds for a stakeholder's willingness to rely.

Confidence is narrower than trust. Confidence refers to an expectation that something will perform as anticipated; trust involves vulnerability and therefore risk. A consumer may be confident that a database will return a record without trusting that the record is true. The distinction matters because digital systems often produce confidence in their operation while leaving trust in their content unaddressed. The triple mapping model treats confidence as a component of verification, not as a substitute for trust.

Transparency is often treated as a synonym for trustworthiness, but it is better understood as a property of disclosure. Transparency can support verification, but it can also overwhelm or mislead. Verifiability is a stronger condition: it concerns whether a stakeholder can check a claim, not merely whether information is available. This distinction is central to M3 and explains why disclosure-heavy systems can fail to generate trust.

Finally, reliance is a behaviour, while trust is a psychological state that may or may not accompany it. A retailer may rely on a traceability system because it is mandated, without trusting it. Studies of automation show that reliance can be calibrated or miscalibrated relative to actual reliability [26]. The model therefore treats reliance as a downstream outcome that should be measured separately from trust, rather than as evidence of it.

3 THE TRIPLE MAPPING MODEL

3.1 Core Logic and Definitions

The model treats traceability as a chain of translations rather than a storage problem. M1 converts physical events into a digital representation. M2 converts twin states into commitments held in a distributed ledger. M3 converts ledger records into evidence that a stakeholder can access and interpret. Each translation has its own failure mode, and each failure changes what later actors can reasonably infer. Trust becomes possible when the translations preserve the properties that matter for the judgment at hand.

Mapping quality is defined here as the extent to which a translation preserves decision-relevant properties. M1 is assessed through representational fidelity: whether the twin captures the right entities and relationships, whether its values match physical conditions, and whether it is current enough to support action. M2 is assessed through evidential integrity: whether a record resists alteration and repudiation and can be audited. M3 is assessed through verification confidence: whether stakeholders can reach the record, understand what it certifies and check the claim without relying solely on its issuer.

Timeliness and coverage are scope conditions rather than additional mapping qualities. Timeliness asks whether a mapping is current enough for the decision being made; a temperature history delivered after a perishable shipment has spoiled may be accurate yet operationally irrelevant. Coverage asks whether the relevant stages, actors and transformations are included. A ledger record that begins at the packing house may be reliable while leaving the farm, where many provenance risks originate, outside the system. Both conditions limit how much trust a given level of mapping quality can support.

Figure 1 should be read from left to right as a chain of translations, not as a software architecture. The first stage is a physical event such as harvesting, handling, storage or transport. The first arrow represents sensing, modelling and synchronization, which together produce representational fidelity. The second arrow represents the conversion of twin states into a ledger commitment, producing evidential integrity. The third arrow represents access, explanation and independent checking, producing verification confidence. The band beneath the sequence marks the two scope conditions: a timely and sufficiently complete mapping can support trust, while a late or partial mapping constrains it.



Figure 1 The Physical–Digital–Trust Triple Mapping Model

Table 2 separates the three mapping qualities and suggests indicators for later measurement. The distinction is analytical rather than technological: the same platform can score well on one quality and poorly on another. Representational fidelity concerns the relation between the physical state and the twin. Evidential integrity concerns the relation between the twin state and the ledger record. Verification confidence concerns the relation between the record and a stakeholder's judgment. The indicators in the table are starting points, not validated scales; their purpose is to make the constructs observable in field research.

Table 2 Constructs, Definitions, and Illustrative Indicators

Construct	Definition	Illustrative indicators
Representational fidelity	Correspondence between the twin and the physical state it represents	Model error; sensor accuracy; synchronization lag; calibration records
Evidential integrity	Resistance of the ledger record to alteration and repudiation	Hash verification rate; consensus participation; audit trail completeness
Verification confidence	Stakeholders' ability to check and understand provenance claims	Independent verification access; disclosure clarity; third-party audit coverage
Timeliness	Speed with which physical events are reflected in the twin and ledger	Update latency; batch versus real-time anchoring; alert lag
Coverage	Share of relevant stages, actors, and transformations included	Stage coverage; actor participation rate; missing-data rate

3.2 M1: From Physical Events to Digital Twins

M1 begins with measurement. Temperature, humidity, location, weight, images and handling events are captured at selected points in the chain. Measurement is never a neutral copy of reality: sensor error, placement and sampling frequency determine what the twin can see and what it misses. The observations are then interpreted through a model, which may be thermodynamic, predictive or rule-based. That modelling choice determines which states become visible and which remain implicit.

Synchronization completes M1. A twin refreshed once a day is not the same instrument as one refreshed every minute, even when both use an identical model. Temporal fidelity should therefore be judged against the decision the twin is expected to support. A two-hour delay may be acceptable for a durable product but unacceptable for live seafood or fresh produce. The relevant question is not whether the data are recent in absolute terms, but whether they are recent enough to change or confirm a decision.

Representational fidelity has structural, data and temporal components. Structural fidelity asks whether the model contains the entities and relationships that matter, including custody transfers as well as environmental conditions. Data fidelity asks whether recorded values correspond to the physical state. Temporal fidelity asks whether the representation is current. A twin may be structurally elaborate yet fed by sparse observations, or current yet too simple to capture the relevant risk. Each combination limits what the twin can warrant.

The trust consequence of M1 is competence. When stakeholders see that a twin follows the product or process accurately, they have reason to infer that the system knows what it claims to know [16]. That inference is provisional. A stakeholder may accept the twin's accuracy while still suspecting that its operator can alter the representation or select convenient data. The second mapping addresses that residual suspicion, but it cannot restore information that M1 never captured.

3.3 M2: From Digital Twins to Distributed Ledgers

M2 turns a twin state into a ledger commitment. In most designs, a cryptographic hash of the state, or of a batch of states, is written to the ledger together with metadata; the full twin remains off-chain because of size, privacy or commercial sensitivity. The ledger therefore does not store the product's entire history. It stores a durable claim that a particular state existed and can later be checked against the off-chain record. Smart contracts may add rules, such as refusing to mark a shipment as delivered when temperature limits have been exceeded.

Evidential integrity depends on three properties. Immutability makes alteration detectable. Non-repudiation makes it difficult for a writer to deny an entry later. Auditability allows an authorized party to reconstruct the sequence of events and inspect the links between records. These properties raise the cost of manipulation after entry. They do not, by themselves, establish that the entry was correct when it was made.

The distinction between integrity and truth is central. A ledger can preserve a bad measurement, a misreported transfer or a deliberately false claim with perfect consistency [15]. This is the oracle problem in its practical form. M2 is only as strong as the twin it anchors, and the twin is only as strong as its sensing and modelling. The ledger supplies record stability; it does not supply factual accuracy.

M2 supports integrity-based trust when stakeholders believe that records cannot be quietly rewritten and that the governance of the ledger is transparent [16]. They need to know who may write, how conflicts are handled and how errors are corrected. Without those organizational answers, immutability can look like rigidity rather than accountability. The trust effect of M2 is therefore conditional on governance as well as on cryptography.

3.4 M3: From Ledgers to Stakeholder Trust

M3 is the most frequently neglected mapping in technical designs. It concerns the movement from a ledger record to a stakeholder's judgment. A proof available only to engineers does not reassure a consumer, and a dashboard that displays a hash without explaining what it certifies does not reduce uncertainty. Verification confidence depends on whether the right person can reach the right evidence in a form that supports a decision.

Three features shape M3. Access concerns who can query the record and under what conditions. Interpretability concerns whether the record is presented in terms that fit the stakeholder's decision problem: a regulator may need an audit trail, a consumer may need a plain account of origin and handling, and a buyer may need batch-level certification. Independence concerns whether the claim can be checked through a third party, a public ledger or a verifiable credential rather than accepted solely from the party that issued it.

Verification confidence should not be confused with transparency. Transparency describes how much is disclosed; verification confidence describes whether a stakeholder can check what matters. A firm can disclose a large amount of information without making any claim independently testable, and it can enable meaningful verification with relatively little disclosure. The distinction explains why information-rich interfaces do not always produce trust.

M3 supports both integrity and benevolence. Integrity is reinforced when a claim can be checked against independent evidence and when discrepancies are treated seriously. Benevolence is reinforced when the system is designed around the user's capacity to understand, question and seek redress. This is where the model connects to institutional trust: verification works better when it is embedded in rules and procedures that stakeholders regard as fair [35-36].

3.5 Multiplicative Logic and the False Assurance Paradox

The three mappings are sequentially dependent. A stakeholder cannot verify a ledger entry that was never created; a ledger cannot anchor a twin state that was never computed; and a twin cannot represent an event that was never observed. The dependence matters because failures propagate forward. High fidelity cannot compensate for a ledger that can be altered, and high integrity cannot compensate for a twin that records the wrong condition. Verification may be excellent while the evidence being verified remains misleading.

We therefore describe trust as a multiplicative configuration of the three mapping qualities, moderated by timeliness and coverage. The multiplicative language expresses a logic rather than a precise mathematical law: a near-zero value on one mapping sharply limits what the other two can achieve. Additive accounts imply that a strong ledger can offset weak sensing, or that extensive disclosure can compensate for inaccurate records. The configurational account rejects both substitutions.

The false assurance paradox follows from this logic. When integrity is high and fidelity is low, the system produces records that look authoritative but are wrong. Immutability then works against correction: the error persists, travels with the product and may acquire credibility from the very technology that preserved it. If stakeholders later discover the discrepancy, they may interpret the episode as betrayal rather than as an ordinary mistake. The durability that made the record credible also makes the eventual loss of trust severe.

Figure 2 distinguishes four configurations. The aligned case combines accurate representation with a record that cannot be quietly altered. The false-assurance case combines a reliable-looking ledger with weak fidelity. The third case offers accurate but alterable information, which may be useful internally but fragile as public evidence. The fourth case lacks a credible traceability system altogether. The figure is diagnostic: it asks managers to locate a system by its weakest mapping rather than by its most visible technology.

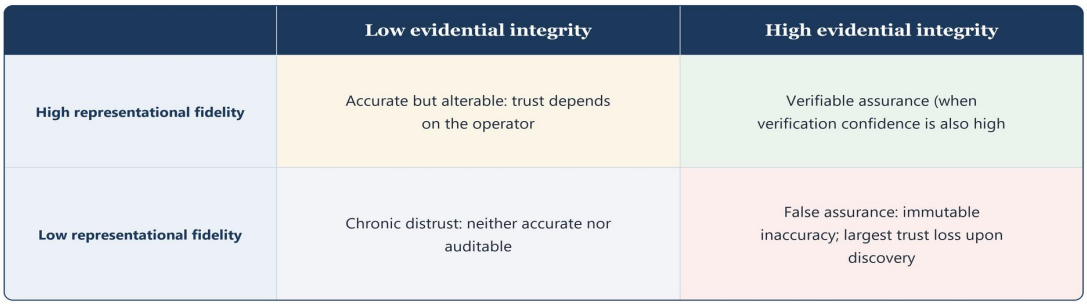


Figure 2 Alignment and Misalignment between Representational Fidelity and Evidential Integrity

3.6 Stakeholder Heterogeneity

Stakeholders do not attach equal importance to the three mappings. Consumers tend to care whether a claim is true and whether they can understand it, so verification confidence and interpretability weigh heavily. Firms care about operational reliability, which makes fidelity and timeliness more salient. Regulators care about accountability, which raises the importance of integrity, auditability and coverage. These differences are not preferences about technology; they follow from the decisions each group has to make and the consequences of getting them wrong.

Two implications follow. A single design can satisfy one group while failing another: a ledger that regulators find auditable may be opaque to shoppers, and a consumer-friendly summary may omit the detail an auditor needs. Trust is therefore better understood as a profile across stakeholder groups than as a single score. Claims that a system is "trusted" should specify by whom, for which decision and under what conditions.

3.7 Temporal Dynamics of Trust Formation

Trust formation has a temporal structure. In the initial phase, stakeholders rely on institutional cues such as brand reputation, certification and the visibility of the technology. Research on initial trust shows that people use such cues when they lack direct experience [17]. A blockchain label can therefore create confidence before any verification has occurred. That confidence is provisional and may be poorly calibrated.

In the experiential phase, stakeholders encounter the system through use. They scan a code, compare a record with the product, ask a question or hear about a recall. Verification confidence is built or weakened through these encounters. When the record agrees with experience, trust becomes better grounded; when it does not, the discrepancy is read as evidence about both the twin and the ledger. This is the phase in which the difference between fidelity and integrity becomes visible to non-specialists.

The consequential phase tests trust through failure. A recall, a dispute or a discovered error reveals whether the system can acknowledge and correct mistakes. This is where the false assurance paradox becomes observable: a system that advertised its rigor may lose more trust than a system that never made such a claim. Recovery capability—the ability to detect, disclose and remediate error—is therefore a boundary condition on long-term trust, even though it is not one of the three core mappings.

Temporal dynamics also create feedback. Trust encourages participation; participation generates data; denser data can improve fidelity and coverage, which in turn supports trust. The loop can reverse. Distrust reduces participation, sparse participation weakens coverage, and weak coverage gives stakeholders further reason to withdraw. Early design choices can therefore lock a system into a virtuous or a vicious trajectory.

3.8 Boundary Conditions and Contingencies

Institutional context conditions the model. Where regulators are credible and certification is enforced, stakeholders may rely on institutions and assign less weight to a system's own verification features. Where institutional trust is weak, the mappings carry more of the burden and failures are more damaging. Institutional trust can therefore act as a substitute for verification in some settings and as an amplifier of verification in others. The net effect is an empirical question.

Cost shapes what can be mapped. Sensing, calibration, connectivity and maintenance require resources, and smallholders may not be able to bear them. When participation costs exceed expected benefits, coverage becomes partial and assurance is uneven across products and actors. The distribution of costs therefore affects mapping quality independently of technical design. A system that is elegant in a pilot can become selective and inequitable when it is scaled.

Digital literacy and access also shape verification confidence. A system that requires users to interpret cryptographic proofs will produce confidence mainly among technical specialists. Interfaces that translate proofs into plain claims can

widen access without changing the underlying ledger. This is a reminder that M3 is a socio-technical achievement: it depends on presentation and institutional support as much as on data availability.

3.9 Illustrative Applications

Three short scenarios show how the model can be used diagnostically. They are analytical illustrations rather than empirical cases; their purpose is to show how the mappings combine in familiar agri-food settings.

Consider navel oranges from the Three Gorges Reservoir Area sold through an e-commerce platform. A twin may capture orchard conditions, harvest date and packing-house handling, but sensing at the orchard is often sparse. Packing-house records may be accurate while covering only part of the product's history. If the ledger anchors only those records, integrity is high and coverage is low. A shopper who scans the code sees an authoritative account that begins at packing, not at the farm. The model predicts that trust will be limited by the missing upstream mapping and that orchard-level sensing or cooperative data collection may do more than another ledger upgrade.

A cold-chain shipment of fresh produce illustrates a different failure. Temporal fidelity dominates: hourly temperature records may be adequate while daily averages are not. If the sensors are miscalibrated, the ledger can preserve a misleading record with high integrity—the false-assurance configuration. The practical implication is that calibration and maintenance are trust-relevant investments, not routine housekeeping. The model also predicts that trust loss after a spoilage incident will be greater when the operator has made prominent claims about blockchain certification.

A geographical-indication tea aggregated from many smallholders illustrates a coverage and verification problem. The cooperative may record processing and packaging while having limited evidence about individual growers. Consumers may have no practical way to check the cooperative's claim without technical help. In this setting M3 is as consequential as M1 and M2: a technically sound record that cannot be interpreted or independently checked will not produce trust. Shared audit arrangements or simplified verification portals may be more useful than additional ledger features.

4 PROPOSITIONS

The model yields nine propositions. They are deliberately stated at a level that permits different empirical strategies, from experiments to field surveys. Table 3 links each proposition to a mechanism and a plausible measurement approach.

4.1 Proposition 1: Fidelity Builds Competence Trust

P1. Representational fidelity is positively associated with competence-based trust. The inference is straightforward: stakeholders who observe that a twin follows physical conditions accurately have reason to believe that the system can know what it claims to know. Competence trust is not equivalent to overall trust, but it is a necessary component. Measurement should therefore capture perceived as well as technical accuracy, because the two can diverge.

4.2 Proposition 2: Integrity Builds Integrity-Based Trust

P2. Evidential integrity is positively associated with integrity-based trust. The mechanism is perceived cost of manipulation: when alteration is detectable and writers cannot easily deny their entries, stakeholders have stronger grounds for believing that what they see is what was recorded. The effect is conditional on source validity. If stakeholders know that on-chain inputs are unverified, integrity of the record will not translate into trust in the recorded fact.

4.3 Proposition 3: Verification Confidence Builds Overall Trust

P3. Verification confidence is positively associated with overall traceability trust. The mechanism is reduced dependence on the party making the claim. A stakeholder who can reach, understand and independently check evidence does not have to accept an assurance on faith. Because verification confidence combines access, interpretability and independence, it is closer to the stakeholder's experience than either fidelity or integrity. Systems should therefore be evaluated by what stakeholders can check, not only by what they record.

4.4 Proposition 4: Verification Confidence Mediates

P4. Verification confidence mediates the effects of fidelity and integrity on trust. Fidelity and integrity are largely invisible properties of an infrastructure. They become consequential when stakeholders encounter evidence they can use. An accurate twin and an immutable ledger may coexist with weak trust if neither can be checked by the relevant audience. The proposition calls for mediation designs in which mapping qualities are antecedents, verification confidence is the mediator and trust is the outcome.

4.5 Proposition 5: The Mappings Are Multiplicative

P5. The three mapping qualities combine multiplicatively rather than additively. The rationale is sequential dependence: verification needs a record, a record needs a representation, and a representation needs an observed event. Additive models imply that strength in one dimension can offset weakness in another; the configurational model predicts that compensation is severely limited. Tests should vary the three qualities jointly, for example through conjoint experiments or comparative configurational analysis.

4.6 Proposition 6: False Assurance Produces Disproportionate Trust Loss

P6. False assurance produces disproportionate trust loss. When high integrity is paired with low fidelity, initial trust may be elevated by the apparent rigor of the record. If the inaccuracy is later exposed, the loss of trust can exceed that observed in a low-technology baseline. The mechanism combines the credibility of immutability with the durability of error: the system looks authoritative, the falsehood persists, and the revelation is experienced as betrayal. Longitudinal or vignette designs are needed to observe trust before and after disclosure.

4.7 Proposition 7: Timeliness Moderates Fidelity Effects

P7. Timeliness moderates the effect of fidelity on trust, and the moderation is stronger for perishable products. Accuracy has little value when it arrives after the decision has passed. A twin that correctly represents yesterday's temperature is historically faithful but operationally useless for a shipment that must be accepted today. Studies should therefore measure product perishability and decision horizon rather than treating timeliness as a generic system attribute.

4.8 Proposition 8: Coverage Moderates Integrity Effects

P8. Coverage moderates the effect of integrity on trust. A tamper-evident record of a partial chain can create a narrow assurance that stakeholders overgeneralize. Integrity matters more when the record includes the stages and actors that are consequential for the claim. Coverage should be measured as inclusion of stages and actors, not simply as the volume of transactions.

4.9 Proposition 9: Stakeholder Type Moderates the Weights

P9. Stakeholder type moderates the weights assigned to the three mapping qualities. Consumers are expected to emphasize verification confidence, firms fidelity and timeliness, and regulators integrity and coverage. These differences follow from distinct decision problems and accountability structures. The proposition implies that trust should be measured as a profile across groups rather than as one aggregate score. Table 3 summarises the nine propositions and their suggested tests.

Table 3 Propositions, Mechanisms, and Suggested Measurement Strategies

Proposition	Core relationship	Mechanism	Suggested strategy
Proposition 1	Fidelity → competence trust	Inference from accurate representation to system capability	Twin accuracy metrics plus perceived fidelity
Proposition 2	Integrity → integrity trust	Perceived cost of manipulation	Ledger audit properties plus trust scales
Proposition 3	Verification confidence → trust	Reduced dependence on the party making the claim	Verification tasks; access and interpretability measures
Proposition 4	Verification confidence mediates	System properties become consequential through verification	Mediation model with temporal separation
Proposition 5	Multiplicative mapping effects	Sequential dependence; weakest link	Conjoint experiment; configurational analysis
Proposition 6	False assurance penalty	Immutable inaccuracy; betrayal effect	Longitudinal or vignette experiment with disclosure
Proposition 7	Timeliness moderates	Decision relevance of current state	Multi-group comparison by perishability
Proposition 8	Coverage moderates	Partial chain limits assurance	Stage coverage index; moderation analysis
Proposition 9	Stakeholder type moderates	Different decision problems and accountability	Multi-stakeholder survey; profile analysis

4.10 Alternative Explanations and Rival Hypotheses

Three rival explanations need to be taken seriously. Technology acceptance suggests that usefulness and ease of use drive trust regardless of mapping quality. Reputation suggests that brand or certification can substitute for system evidence. Dispositional trust suggests that some stakeholders are simply more trusting than others. These accounts are plausible, and the present model should be tested against them rather than assumed to supersede them.

The model locates these alternatives rather than denying them. Acceptance and disposition are likely to shape initial trust before stakeholders have verification experience. Reputation and institutional credibility are likely to substitute for

verification when checking is costly. The distinctive claim is that, once stakeholders have opportunities to verify, the three mappings explain variance that acceptance, reputation and disposition do not capture.

Testing that claim requires designs that separate mapping quality from brand and acceptance. Conjoint experiments can vary fidelity, integrity and verifiability while holding brand constant. Field studies can compare systems with similar technology but different verification arrangements. Longitudinal designs can observe what happens when a mapping fails. These approaches would let researchers distinguish the configurational account from simpler explanations.

4.11 A Research Agenda

The propositions imply four research priorities. The first is measurement: developing valid indicators for fidelity, integrity, verification confidence, timeliness and coverage. The second is experimentation: using conjoint or vignette designs to test the multiplicative logic and the false-assurance penalty. The third is field research: observing how stakeholders actually verify claims and how trust changes after failures. The fourth is comparative work across product categories and regulatory regimes, which is necessary to establish boundary conditions.

5 DISCUSSION

5.1 Theoretical Contributions

The first contribution is a configurational theory of traceability trust. Existing accounts often treat trust as a by-product of adoption or as a property of institutions. The present model treats trust as an outcome of three translations whose alignment determines what a system can warrant. This shift has a direct implication: the weakest mapping, not the most impressive feature, sets the limit on trust. It also explains why technologically advanced systems can fail to reassure the people they are designed to serve.

The second contribution is the construct of mapping quality. Fidelity, integrity and verification confidence are defined in ways that can be operationalized and compared. This addresses a gap between technical metrics and managerial outcomes: engineers can measure model error or ledger uptime, while managers need to know whether those properties become usable evidence. The construct also gives engineers, operations managers and regulators a common vocabulary for discussing traceability quality.

The third contribution is an explanation of the false assurance paradox. The paradox is not an anomaly; it follows from misalignment between fidelity and integrity. This argument speaks to debates about the limits of blockchain in supply chains, where enthusiasm for immutability has sometimes obscured source validity [37-39]. It also responds to calls for theory-driven work on blockchain in operations and supply chain management [40-41].

The fourth contribution is a stakeholder-relative account of trust. Rather than assuming one trust outcome, the model specifies how different groups weight the three mappings according to their decisions. This helps explain a familiar managerial puzzle: auditors may praise a system that consumers distrust, and both judgments can be rational. Trust is therefore better represented as a profile across stakeholders than as a scalar.

5.2 Managerial Implications

For firms, the first implication is that investment in ledger technology without investment in source fidelity is unlikely to produce trust. A blockchain can make a record permanent; it cannot make the record true. Sensor calibration, model validation and data governance belong to the traceability infrastructure, not to a separate technical background. The weakest-link logic also implies that resources should go to the weakest mapping rather than to the most visible technology.

For platform operators, verification deserves as much design attention as record keeping. Users need access to claims, explanations suited to their decisions and independent routes to checking. A screen that displays a hash without explaining what it certifies does not create verification confidence. Operators also need remediation protocols: if records are immutable, how are errors corrected, and how is the correction itself recorded? A system that cannot handle its own mistakes will struggle to sustain trust.

For supply chain managers, coverage is a strategic variable. A system that follows a product only from the packing house to the retailer may satisfy a downstream buyer while leaving the most consequential stages unobserved. Extending coverage requires collaboration with upstream partners, including smallholders, and may require different participation arrangements for different actors. Inclusion, not transaction volume, is the relevant measure.

Small and medium-sized enterprises should think in terms of sequencing rather than comprehensive platforms. The first investment should address the mapping that most directly constrains the customer's decision. For fresh produce, that is often sensing and timeliness; for a processed product with a strong regional brand, it may be verification and disclosure. Investments in consensus mechanisms that do not address the weakest mapping are unlikely to produce proportionate trust benefits. Shared sensing networks, audit services and verification portals can lower the cost of improving that link.

Firms should also treat mapping quality as a management metric. Most dashboards report uptime, transaction volume and data completeness. These are useful but incomplete. Calibration status, synchronization lag, stage coverage, verification success and independent audit findings provide a closer view of trust-relevant performance. Treating them as trust metrics rather than technical housekeeping would align operational decisions with the outcome that matters to stakeholders.

5.3 Policy Implications

For regulators, standards should address data quality and verification, not only interoperability and security. A regime that certifies ledgers but not twins can produce systems that are auditable in form and inaccurate in substance. Regulators could require evidence of calibration, model validation and independent audit before recognizing traceability claims. They could also require that verification be accessible to consumers, not only to firms.

Policy should also consider who bears the cost of verification. If checking requires expertise available only to large firms, traceability may reinforce rather than reduce information asymmetries. Shared registries, open standards and independent auditors can lower the cost of checking for small producers and consumers. The observation that distributed ledgers are not a panacea for food traceability [39] is therefore an argument for institutional design, not for abandoning the technology.

Standards could specify minimum thresholds for fidelity and coverage rather than merely prescribing data fields. A standard that defines formats but not calibration requirements leaves the most consequential quality dimension unregulated. Interoperability standards should also include verification interfaces, so that a stakeholder can check a claim across systems without depending on the firm that issued it. These are modest regulatory moves with potentially large effects on credibility.

5.4 Theoretical Positioning Relative to Adjacent Frameworks

The model complements adjacent theories rather than replacing them. Transaction cost economics explains why firms invest in monitoring when information asymmetry and opportunism are high [42]. The triple mapping model specifies what is being monitored—fidelity, integrity and verification—and why monitoring only one of them is insufficient. It therefore gives transaction cost reasoning a more concrete account of the object of governance.

Principal-agent theory explains why principals demand assurance and why agents may conceal information. The model adds that assurance depends on the chain of representations through which an agent's actions become visible. A principal may impose monitoring, but if the monitor relies on a poorly calibrated twin or a ledger of unverified inputs, monitoring can create an illusion of control. Agency problems are thus connected to the material infrastructure of verification.

Signaling theory explains how costly signals reduce information asymmetry [21-22]. The model specifies the production process behind a signal: it must be sensed, represented, anchored and made verifiable. Signaling research often treats the signal as given, without examining the infrastructure that produces it. Similarly, affordance theory explains what technologies make possible, while the model specifies the conditions under which those possibilities become trust.

Institutional theory explains how shared rules and norms create trust in markets [35-36]. Digital traceability may complement institutional trust by making verification routine, or substitute for it by supplying a technical basis for confidence when institutions are weak. Which effect dominates depends on the credibility of regulators and the accessibility of verification. The model treats that balance as an empirical question rather than a design assumption.

5.5 Limitations and Future Research

The paper is conceptual, and its propositions remain untested. The multiplicative form expresses a logic of sequential dependence rather than a specific functional form; future work should compare product, minimum and more complex configurational specifications. The model is developed with agri-food in mind, although its logic may extend to pharmaceuticals, luxury goods and carbon accounting, where physical states are represented digitally and recorded publicly.

The model says relatively little about power and cost. Traceability systems distribute visibility, accountability and expense across actors with unequal resources. Future research could draw on transaction cost economics [42] and political perspectives on supply chain governance to ask who pays for fidelity, who controls the ledger and whose verification needs are served. These questions are particularly important in agri-food chains marked by smallholder fragmentation.

Temporal dynamics also deserve more attention. Trust is built and eroded over time, and the false-assurance paradox is inherently longitudinal: it concerns what happens when stakeholders discover that a credible-looking system has been recording an error. Panel designs, field experiments and process tracing would complement cross-sectional surveys by observing trust before, during and after failure.

6 CONCLUSION

Digital twins and blockchains are often presented as complementary traceability technologies: the twin makes the physical world visible, and the ledger makes the record credible. This paper has argued that the combination produces trust only when three mappings align. Physical events must be represented faithfully in a twin; the twin must be anchored in a record that resists alteration; and the record must be accessible and interpretable to the stakeholders who rely on it. A failure in any mapping limits the trust the system can support, and high integrity combined with low fidelity can produce false assurance rather than assurance.

The model reframes traceability trust as a configurational outcome and offers constructs, propositions and measurement strategies for future research. Its practical message is to invest in the weakest mapping, design for verification rather than disclosure, and treat credibility as something earned at each link in the chain. Its theoretical message is that trust is not an attribute added to a platform; it is a relationship among what a system can show, what it can prove and what stakeholders can check.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

FUNDING

This work was supported by two research projects: (1) Mechanism and Optimization Methods of Digital Twin–Blockchain Integrated Traceability for Specialty Agricultural Products in the Three Gorges Reservoir Area (No. KJQN202601263); and (2) Model Innovation and Practical Pathways for the Digital-Intelligence-Empowered High-Quality Development of Specialty Agriculture in the Wushan Region (No. 2025sxxyjd06).

REFERENCES

[1] Akerlof G A. The market for “lemons”: Quality uncertainty and the market mechanism. Quarterly Journal of Economics, 1970, 84(3): 488-500.
[2] Moe T. Perspectives on traceability in food manufacture. Trends in Food Science & Technology, 1998, 9(5): 211-214.
[3] Olsen P, Borit M. How to define traceability. Trends in Food Science & Technology, 2013, 29(2): 142-150.
[4] Grieves M. Digital twin: Manufacturing excellence through virtual factory replication. White paper, 2014.
[5] Tao F, Zhang H, Liu A, et al. Digital twin in industry: State-of-the-art. IEEE Transactions on Industrial Informatics, 2019, 15(4): 2405-2415.
[6] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf.
[7] Iansiti M, Lakhani K R. The truth about blockchain. Harvard Business Review, 2017, 95(1): 118-127.
[8] Tian F. An agri-food supply chain traceability system for China based on RFID and blockchain technology. In: Proceedings of the 13th International Conference on Service Systems and Service Management. IEEE, 2016: 1-6.
[9] Feng H, Wang X, Duan Y, et al. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. Journal of Cleaner Production, 2020, 260: 121031.
[10] Zhao G, Liu S, Lopez C, et al. Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions. Computers in Industry, 2019, 109: 83-99.
[11] Kritzinger W, Karner M, Traar G, et al. Digital twin in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine, 2018, 51(11): 1016-1022.
[12] Jones D, Snider C, Nassehi A, et al. Characterising the digital twin: A systematic literature review. CIRP Journal of Manufacturing Science and Technology, 2020, 29: 36-52.
[13] Kshetri N. 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 2018, 39: 80-89.
[14] Saberi S, Kouhizadeh M, Sarkis J, et al. Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 2019, 57(7): 2117-2135.
[15] Caldarelli G. Understanding the blockchain oracle problem: A call for action. Information, 2020, 11(11): 509.
[16] Mayer R C, Davis J H, Schoorman F D. An integrative model of organizational trust. Academy of Management Review, 1995, 20(3): 709-734.
[17] McKnight D H, Cummings L L, Chervany N L. Initial trust formation in new organizational relationships. Academy of Management Review, 1998, 23(3): 473-490.
[18] Gibson J J. The ecological approach to visual perception. Houghton Mifflin, 1979.
[19] Hutchby I. Technologies, texts and affordances. Sociology, 2001, 35(2): 441-456.
[20] Majchrzak A, Markus M L. Technology affordances and constraints in management information systems (MIS). In: Kessler E H, ed. Encyclopedia of management theory. SAGE, 2013: 832-836.
[21] Spence M. Job market signaling. Quarterly Journal of Economics, 1973, 87(3): 355-374.
[22] Connelly B L, Certo S T, Ireland R D, et al. Signaling theory: A review and assessment. Journal of Management, 2011, 37(1): 39-67.
[23] McKnight D H, Carter M, Thatcher J B, et al. Trust in a specific technology: An investigation of its components and measures. ACM Transactions on Management Information Systems, 2011, 2(2): 12.
[24] Bosona T, Gebresenbet G. Food traceability as an integral part of logistics management in food and agricultural supply chain. Food Control, 2013, 33(1): 32-48.
[25] Gefen D, Karahanna E, Straub D W. Trust and TAM in online shopping: An integrated model. MIS Quarterly, 2003, 27(1): 51-90.
[26] Hoff K A, Bashir M. Trust in automation: Integrating empirical evidence on factors that influence trust. Human Factors, 2015, 57(3): 407-434.

[27] Egels-Zandén N, Hulthén K, Wulff G. Trade-offs in supply chain transparency: The case of Nudie Jeans Co. Journal of Cleaner Production, 2015, 107: 95-104.
[28] Montecchi M, Plangger K, West D C. Supply chain transparency: Theoretical perspectives for future research. International Journal of Logistics Management, 2021, 32(4): 1422-1443.
[29] Lu Y, Liu C, Wang K I K, et al. Digital twin-driven smart manufacturing: Connotation, reference model, applications and research issues. Robotics and Computer-Integrated Manufacturing, 2020, 61: 101837.
[30] Kamath R. Food traceability on blockchain: Walmart's pork and mango pilots with IBM. Journal of the British Blockchain Association, 2018, 1(1): 1-12.
[31] Galvez J F, Mejuto J C, Simal-Gandara J. Future challenges on the use of blockchain for food traceability analysis. TrAC Trends in Analytical Chemistry, 2018, 107: 222-232.
[32] Rejeb A, Keogh J G, Treiblmaier H. Leveraging the internet of things and blockchain technology in supply chain management. Future Internet, 2019, 11(7): 161.
[33] Azzi R, Chamoun R K, Sokhn M. The power of a blockchain-based supply chain. Computers & Industrial Engineering, 2019, 135: 582-592.
[34] Queiroz M M, Telles R, Bonilla S H. Blockchain and supply chain management integration: A systematic review of the literature. Supply Chain Management, 2020, 25(2): 241-254.
[35] Zucker L G. Production of trust: Institutional sources of economic structure, 1840–1920. Research in Organizational Behavior, 1986, 8: 53-111.
[36] Bachmann R, Inkpen A C. Understanding institutional-based trust building processes in inter-organizational relationships. Organization Studies, 2011, 32(2): 281-301.
[37] Kamilaris A, Fonts A, Prenafeta-Boldú F X. The rise of blockchain technology in agriculture and food supply chains. Trends in Food Science & Technology, 2019, 91: 640-652.
[38] Astill J, Dara R A, Campbell M, et al. Transparency in food supply chains: A review of enabling technology solutions. Trends in Food Science & Technology, 2019, 91: 240-247.
[39] Pearson S, May D, Leontidis G, et al. Are distributed ledger technologies the panacea for food traceability? Global Food Security, 2019, 20: 145-149.
[40] Treiblmaier H. The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Management, 2018, 23(6): 545-559.
[41] Wamba S F, Queiroz M M. Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. International Journal of Information Management, 2020, 52: 102064.
[42] Williamson O E. The economic institutions of capitalism. Free Press, 1985.