Intelligent Blockchain for Collusion and Fraud Governance in Supply Chain Finance: Mechanisms, Stakeholder Interactions, and Research Directions

Yang Lu[1, *]

[1] Faculty of Business, Information & Human Sciences, Kuala Lumpur University of Science and Technology, Kajang, Malaysia 43000

* Email: yanglu@klust.edu.cn (Corresponding Author)

Received 10 June 2024 · Revised 25 July 2024 · Accepted 8 September 2024 · Published 30 December 2024

Abstract

Supply chain finance can convert trade receivables into liquidity, yet the financing decision often depends on information controlled by parties whose incentives are not aligned with those of lenders. The risk is especially difficult to manage when buyers, suppliers, platform participants, or intermediaries coordinate to create consistent but misleading transaction evidence. This critical narrative review examines how blockchain, artificial intelligence, smart contracts, and selected sources of external data may contribute to the governance of collusion and fraud in supply chain finance. It synthesizes research on financing instruments, digital platforms, strategic behavior, fraud analytics, and legal and regulatory arrangements. A five-layer framework links the formation of risk to technical intervention, behavioral incentives, stakeholder coordination, and measurable outcomes. The analysis distinguishes ledger integrity from the truthfulness of underlying transactions, and distinguishes risk identification from a legal finding of fraud. Existing studies offer mechanisms and illustrative applications, but many results depend on model assumptions, prototype environments, or observational indicators that do not directly measure collusion. Effective governance therefore requires independently verifiable data, credible identity and authority checks, accountable node governance, human review, and proportionate remedies alongside technical controls. Research priorities include transaction-level evaluation, strategically adaptive fraud models, accessible and contestable credit decisions, cross-platform verification, and assessment of how risks and costs are distributed among participants. The review provides a basis for designing governance arrangements that improve financing access while preserving verifiable accountability.

Keywords: supply chain finance; collusion; fraud governance; blockchain; artificial intelligence; smart contracts; financial regulation; accounts receivable

Intelligent Blockchain for Collusion and Fraud Governance in Supply Chain Finance: Mechanisms, Stakeholder Interactions, and Research Directions

1. Introduction

Supply chain finance (SCF) connects financing decisions to transactions among buyers, suppliers, financial institutions, and other service providers. In receivables-based arrangements a supplier may obtain funds before the buyer's payment becomes due, while the financier evaluates the underlying obligation and the relevant parties. This relationship can reduce working-capital pressure, but benefits depend on the form of financing, its cost, and the rights and responsibilities of the participants (Kouvelis, 2023; Kouvelis & Xu, 2021; Zhou et al., 2022). A lender may rely on the buyer's acceptance of an invoice, transport records, or payment history when the supplier has limited financial statements. The same reliance creates opportunities for misrepresentation if the information used to establish the claim is incomplete or controlled by interested parties.

Fraud in this setting is not restricted to a borrower submitting an altered invoice. Several participants can coordinate a trade narrative that is internally consistent but economically false. They may produce mutually confirming contracts, delivery notes, acceptance records, and repayment promises, or arrange transactions that are genuine in form but designed to create misleading collateral. Coordination can also involve a platform employee, warehouse operator, broker, or other intermediary. A financing system must therefore ask not only whether each document appears valid, but also whether the participants supplying mutually supportive evidence are independent and whether the underlying transaction occurred. Ordinary late payment, commercial default, suspicious anomalies, and proven collusion should remain separate analytical categories.

Blockchain has been proposed as a shared and tamper-evident record of transactions across organizations. The associated literature discusses visibility, automation, and reduction of administrative frictions, while recognizing operational, legal, and organizational barriers (Hastig & Sodhi, 2020; Sodhi & Tang, 2019; Sodhi et al., 2022). Artificial intelligence (AI), particularly machine learning and graph analysis, adds tools for examining large volumes of transactions and identifying unusual relationships. Smart contracts can execute specified digital actions after defined conditions are satisfied; sensor or third-party data can supply additional observations. Combining these capabilities creates possibilities for verification and monitoring, but each capability introduces assumptions about identity, data quality, authorization, and accountability.

This review uses the term *intelligent blockchain* as a working description for a governance arrangement that combines a distributed ledger and programmable rules with AI-supported analysis and, where relevant, independent external data. The term does not imply that every SCF platform uses all of these components or that the components automatically validate one another. A record may resist unauthorized alteration after submission yet faithfully preserve a false invoice. A well-performing fraud classifier may still miss a coordinated group or mistakenly flag legitimate suppliers. A programmable transfer may be technically executed while its legal consequences remain disputed. For these reasons, governance must encompass the organizations and rules surrounding the technology as well as the technology itself.

The need for a focused synthesis follows from a literature that approaches the problem from several directions. Reviews of supply-chain transparency and blockchain traceability examine organizational requirements and implementation limits (Hastig & Sodhi, 2020; Sodhi & Tang, 2019; Sodhi et al., 2022). Other studies analyze blockchain-enabled financing arrangements and the economic effects of sharing information (Chod et al., 2020; Dong et al., 2023; X. Wang & Xu, 2023). Fraud-detection, audit, and supplier-governance research adds evidence about connected firms, corroboration, and oversight (C. Li et al., 2023; L. Chen & Lee, 2017; Trotman & Wright, 2012). The present review integrates these strands around coordinated misrepresentation, stakeholder incentives, and accountable intervention. This positioning builds on existing research and does not claim that earlier work ignored fraud, governance, or financial frictions.

ISSN: 3068-3661 | © 2024 INATGI (Institute of Advanced Technology and Green Innovation)

The review addresses four questions. How do collusion and related fraud arise in SCF? Through which mechanisms might technical and institutional interventions affect them? How do incentives and responsibilities differ across participants? Finally, what do available forms of evidence establish, and where do meaningful uncertainties remain? To answer these questions, the article proposes a five-layer framework linking risk formation, technical intervention, behavioral incentives, governance coordination, and outcomes. It compares analytical models, empirical fraud research, and documented platform-oriented studies, then develops a research agenda grounded in observable measures and credible counterfactuals.

2. Review Approach and Analytical Boundaries

This article is a critical narrative review. In October 2026, targeted searches were used to identify academic publications on supply chain finance, factoring and receivables, collusion and fraud, blockchain and smart contracts, AI and financial analytics, and governance. Publisher records, available abstracts and selected full texts were examined, and DOI and bibliographic metadata were checked against the Crossref registry. The 86 cited publications were selected from journals appearing in the 2026 Financial Times research journal list and were published no later than 2024. This journal-level criterion is a transparent selection rule; it is not a substitute for evaluating the relevance, methods, or evidentiary quality of each study.

The selection was organized by relevance to the review questions rather than by a pre-specified database export. The corpus combines work on financing instruments and participant incentives; blockchain-enabled supply networks; accounting fraud, audit, and interfirm misconduct; and credit prediction, information sharing, and algorithmic fairness. Studies from adjacent settings, such as social-security fraud or product counterfeiting, are included only where their methods or governance mechanisms inform the review; their results are not presented as direct evidence of receivables-financing collusion. The published journal articles used here include analytical, experimental, empirical, review, and conceptual work.

The search was not an exhaustive systematic review of Scopus, Web of Science, or every relevant legal database. It did not produce a complete screened-record count, a PRISMA flow diagram, independent duplicate screening, or a formal study-level risk-of-bias assessment. Some publisher pages provide abstracts and bibliographic information without unrestricted full text. Consequently, the analysis identifies mechanisms and plausible research directions without presenting its coverage as comprehensive or assigning pooled effect sizes. Before journal submission, the search can be expanded and documented further, and individual source claims can be checked against the full texts available to the authors.

Four evidence categories guide the synthesis. Analytical studies show how conclusions depend on assumptions about payoffs and behavior. Design and prototype studies illustrate feasibility in a specified environment. Observational, interview, and experimental studies report associations or behavior in identified settings. Review and conceptual articles synthesize or interpret previous work. These categories answer different questions: a proof of concept does not establish field effectiveness, a credit rating does not establish fraud, and documented misconduct in another industry does not by itself establish collusive factoring.

2.1 A theoretical foundation for the synthesis

Information-asymmetry theory explains why a financier may struggle to distinguish reliable receivables from doubtful ones before funding. If the financier cannot verify differences, it may price all applications conservatively or refuse transactions, with adverse consequences for legitimate suppliers. Akerlof's analysis of quality uncertainty provides the general logic, although receivables differ from the product market in his original model (Akerlof, 1970). A platform can reduce some uncertainty by making relevant information available, but its effect depends on whether the shared information actually differentiates claims of different quality. An increase in the quantity of submitted records is therefore an insufficient measure of information quality.

Agency theory adds a second question: whether a participant acts in the interest of the party that relies on its report. Jensen and Meckling (1976) describe agency costs associated with divergent interests and monitoring, while Fama (1980) examines monitoring and incentive issues within firms. In SCF, a buyer's confirmation, a platform's verification service, and a bank's approval decision can each create a separate agency relationship. If an agent can alter a report or conceal an error without bearing the resulting loss, a signed digital record does not fully align incentives. Independent assurance, liability rules, and the ability to challenge a record affect the value of the technical signal.

A third lens is deterrence under uncertainty. Becker's economic analysis of enforcement provides a foundation for examining the expected costs of prohibited conduct (Becker, 1968). It does not imply that every firm is perfectly rational or that financial fraud can be reduced to one formula. The useful contribution for this review is a disciplined way to ask how detection, enforcement, financial penalties, and future market consequences interact. The next section applies this logic as an illustrative comparison, while recognizing that detection probabilities and the distribution of sanctions require empirical measurement. These three lenses—information, incentives, and enforcement—support the five-layer framework without assuming that technology alone resolves the underlying governance problem.

3. How Collusion and Fraud Arise in Supply Chain Finance

3.1 Financing instruments and their information requirements

SCF is a family of arrangements rather than a single loan product. In factoring, a receivable is transferred or sold to a factor under a particular contract, potentially with or without recourse. Reverse factoring typically begins with a buyer-supported program in which approved supplier invoices can be financed using the buyer's credit profile. In a secured loan against receivables, a lender instead advances funds against a receivable as collateral. The legal treatment, ownership of the claim, loss allocation, and notification requirements can differ across instruments and jurisdictions (Kouvelis, 2023; Kouvelis & Xu, 2021). Using one term for all three obscures who bears the risk if a receivable is disputed or never existed.

All of these arrangements require information about an underlying commercial obligation. A financier may need to verify the identities and authority of the parties, existence and value of the receivable, acceptance of goods or services, payment status, prior assignments or pledges, and any right of set-off or return. A purchase order is not equivalent to proof of delivery; an invoice is not necessarily a debt accepted by a buyer; and a digital confirmation is meaningful only if the person or system issuing it is authorized. In multi-tier arrangements, a claim may be subdivided or transferred several times. Each additional transfer can improve liquidity, but it also creates questions about provenance, competing claims, and the completeness of the records available to a particular financier (Dong et al., 2023; Hastig & Sodhi, 2020).

Financing access may improve when a credible buyer confirms an obligation. Yet dependence on the buyer can leave smaller suppliers with little bargaining power over payment terms, program participation, and data access. Research on reverse factoring and buyer intermediation shows that financing arrangements and contract terms affect how costs and benefits are distributed; an improvement cannot be assumed from participation alone (Kouvelis & Xu, 2021; Tunca & Zhu, 2018). A review of fraud governance must therefore consider whether a control reduces misconduct without shifting excessive expense, delay, or exclusion onto legitimate smaller firms.

The financing literature supplies several distinctions needed for risk analysis. Petersen and Rajan (1997) and Klapper et al. (2012) study the economic roles and contractual forms of trade credit; Biais and Gollier (1997) relate trade credit to credit rationing, and Cuñat (2007) examines suppliers' roles as collectors and insurers. These mechanisms can supplement bank credit without guaranteeing that a trade obligation is genuine.

Models of working capital, bank borrowing, and credit allocation further show that financing terms interact with operational decisions (Chod, 2017; Devalkar & Krishnan, 2019; Kouvelis & Zhao, 2018; Yang & Birge, 2018). Credit insurance and guarantees introduce additional risk-sharing and monitoring arrangements (W. Wang & Cai, 2024; Yang et al., 2021; Zhou et al., 2020). Research on financing through buyers compares early payment, contractual payment terms, and retailer-supported credit under different assumptions (X. Huang, 2022; Zha et al., 2024; Zhou et al., 2022). These studies explain alternatives and incentives; they are not direct measurements of collusion.

The financing environment also changes across the supply network and over time. Studies examine purchase-order financing, buyer competition, trade-credit borrowing costs, and payables cash management (Kouvelis & Zhao, 2012; Murfin & Njoroge, 2015; Ning, 2022; Reindorp et al., 2018; Yan et al., 2024). Empirical research relates supplier competition, trade credit, financial crises, production networks, and supply-chain stability (Chod, Lyandres, & Yang, 2019; Ersahin et al., 2024; Gofman & Wu, 2022; Lee et al., 2018; Love et al., 2007). These findings underline why an evaluation should compare similar firms, financing instruments, and economic conditions instead of treating all financed receivables as interchangeable. Work on supplier diversification under buyer risk and responsible production financing provides additional perspectives on supplier constraints and operational choices (Chod, Trichakis, & Tsoukalas, 2019; X. Chen et al., 2023).

3.2 From individual misrepresentation to coordinated fraud

Individual fraud may involve an applicant altering an invoice, inflating its value, hiding prior payment, or submitting the same claim to multiple financiers. Collusion adds coordinated behavior by two or more participants who align messages or actions in order to mislead another party. The precise legal definition depends on the jurisdiction; here the term describes coordinated deception as a research scenario, not a conclusion about an individual transaction. The participants need not have equal bargaining power or equal information. A dominant buyer, for example, may induce a dependent supplier to follow a proposed reporting arrangement, while a broker or insider supplies access to the financier.

Several configurations are possible. A supplier and buyer may confirm a fictitious receivable; an intermediary may forge a buyer's authorization without the buyer's knowledge; a warehouse operator may produce inaccurate inventory evidence for a borrower; or platform insiders may delay an update that would reveal repayment or a previous assignment. A ring can divide activity across entities to keep each individual transaction below a threshold. These configurations differ in their information sources and legal consequences, and they should not be treated as evidence that all SMEs or all core firms are likely to collude.

Colluding parties often create consistency across documents because conventional due diligence treats matching documents as corroboration. If the same person or connected organization controls the invoice, delivery confirmation, and warehouse declaration, three matching records may represent one underlying assertion rather than three independent observations. Likewise, an apparently separate node may be operated by an affiliate of another participant. A risk assessment should examine beneficial ownership, administrative control, data provenance, and how each piece of evidence was generated. External verification, where legitimate and available, can improve the evidentiary basis but is not automatically independent merely because it arrives through a separate application interface.

The possibility of coordination against a lender is not new to financing theory. Biais and Gollier (1997) study trade credit under asymmetric information and consider incentive constraints that can prevent collusion between parties. Their model predates blockchain and does not evaluate a digital platform. It nevertheless provides an important theoretical starting point for asking which controls and contractual terms make collusive behavior less attractive in modern receivables financing.

3.3 The lifecycle of a misleading receivable

A simplified fraud lifecycle begins with the creation or manipulation of a trade narrative. Relevant documents are then submitted for confirmation, a receivable is registered or assigned, financing is requested, and proceeds are transferred. Subsequent stages may involve delayed updates, staged repayments, renewed financing, or contested collection. Controls can be placed at each point: identity and authority checks before account creation; consistency checks at issuance; checks for competing interests before funding; monitoring of payment and ownership changes; and investigation and recovery processes after a serious alert. These controls serve different purposes and may be operated by different organizations.

The same lifecycle also shows why a static record is insufficient. A valid claim can later be reduced by returns or set-off; a previously unassigned receivable can be transferred elsewhere; and a buyer's authorization can be revoked. A reliable system must preserve a history of changes while ensuring that current status is available to authorized parties. It also needs clear rules for correcting errors, challenging entries, and handling participants that leave the network. Without these arrangements, a ledger may improve visibility of outdated or incomplete data rather than the underlying quality of the financing decision. The receivables-financing risks and possible controls are summarized in Table 1. The receivable lifecycle and associated governance responses are illustrated in Figure 1.

Table 1. Common Receivables-Financing Risks and Possible Controls

Risk pattern	Typical evidence problem	Possible control	Remaining limitation
Fictitious receivable	Invoice and buyer confirmation arise from coordinated statements	Verify identity, authority and independent trade evidence	Independent evidence may be unavailable or incomplete
Duplicate financing	One claim is assigned or financed more than once	Reconcile claim identifiers and status across relevant registries	A transaction outside connected systems may remain unseen
Inflated or disputed value	Recorded amount exceeds the underlying valid claim	Compare contract, delivery, acceptance, adjustments and payments	Differences may reflect legitimate returns or disputes
Insider or node manipulation	A privileged actor submits or delays a status update	Separate duties; log credentials and review changes	Compromised credentials can make harmful actions look authorized
Misleading relationships	Related entities appear to be independent corroborators	Review ownership, control and data provenance	Ownership and affiliation data can be missing or outdated

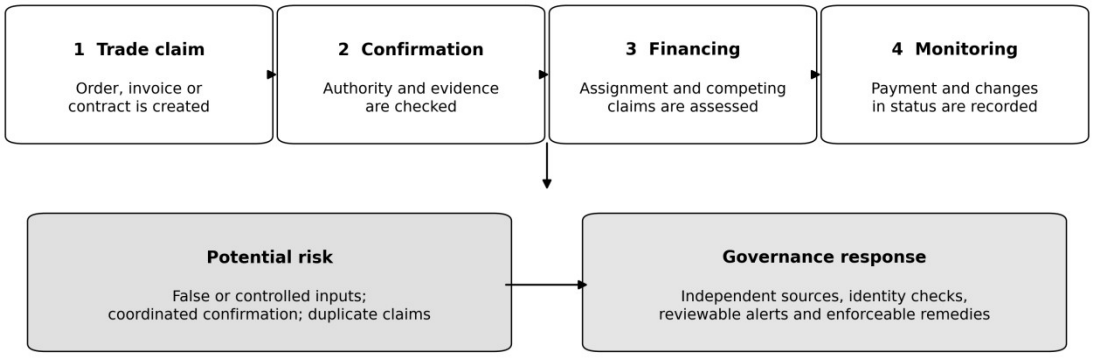


Figure 1. A Stylized Receivable Lifecycle, Points of Vulnerability, and Governance Responses

3.4 Why information consistency is necessary but insufficient

Traditional screening can fail when it treats a buyer's confirmation as conclusive without considering whether the confirming official had authority or incentives to mislead. It can also fail when financiers cannot observe off-platform financing, when several companies share a hidden owner, or when source systems are compromised. Blockchain may help preserve signed confirmations and show their subsequent changes, but it does not inherently establish the authenticity of the goods, the financial capacity of the debtor, or the absence of an undisclosed transaction elsewhere (Babich & Hilary, 2020; Franke et al., 2024; Hastig & Sodhi, 2020; Rui & Lai, 2015; X. Wang & Xu, 2023).

Empirical accounting research offers a related illustration of why multiple linked records can matter. C. Li et al. (2023) compare information reported by suppliers with accounting information of economically linked customers when studying revenue fraud. The study concerns accounting fraud in financial statements, not a court finding of receivables-financing collusion or evidence that a blockchain platform would have detected it. Its relevance here lies in the research design: a financing institution can ask whether apparently corroborating claims are consistent with independently obtained information from the relevant economic relationship.

3.5 A conditional incentive comparison

A compact incentive comparison clarifies how the mechanisms reviewed below may interact. Let B be the incremental expected benefit from coordinated misrepresentation relative to compliance, after ordinary financing and operating costs. Let C be the incremental cost of fabricating, coordinating, or circumventing controls. Let p be the probability that the conduct is detected and an applicable financial consequence is imposed during the relevant period, and let F be the incremental financial loss conditional on that event. Let q be the probability of a separate loss of future business, and L its discounted value; to prevent double counting, that loss is excluded from F. For risk-neutral actors and a clearly specified time horizon, the difference in expected payoff is:

$$\Delta U = B - C - pF - qL. \quad (1)$$

Under these assumptions, compliance is preferred to the specified collusive option when ΔU is negative; equality represents indifference. This expression is a conceptual accounting identity for the comparison, not an estimated equation or a complete model of collusion. It omits heterogeneous gains within a group, retaliation, imperfect knowledge, and the possibility that penalties or future access are negotiated. A powerful

buyer and a dependent supplier may face different values of B, C, p, F, q, and L, so a negative total gain for a proposed alliance does not establish that every participant will independently refuse it.

Each technology affects the expression only under identifiable conditions. Independent verification might increase C or p; a reliable and contestable credit history might affect q or L; and credit terms can change the relative benefit B. These are hypotheses, not automatic properties of a ledger. If several supposedly independent data feeds are controlled by the same actor, C and p may change little. A higher formal sanction F may also have limited effect when the conditional probability of enforcement p is low. Conversely, an aggressive alert threshold can raise the cost of errors for honest firms without necessarily raising the probability of identifying a coordinated group.

Equation (1) also prevents a common interpretation error: a model's assumed increase in p after adopting a platform is not an empirical estimate of that increase. In practice, p includes both detection and follow-through; it can be decomposed into the probability of an actionable detection and the conditional probability that a valid consequence is imposed. Each component varies with investigative capacity, access to source records, and legal process. The appropriate test is whether the implemented combination of controls changes these measurable components relative to a credible alternative, rather than whether a simulation produces a desirable equilibrium.

4. Technological Mechanisms for Fraud Governance

4.1 Shared records and provenance

A permissioned blockchain can provide participating organizations with a synchronized history of authorized events. A receivable might be associated with a unique identifier, the issuer's digital signature, time-stamped status changes, a record of assignments, and links to supporting materials. If the participants agree on authoritative identifiers and communicate updates promptly, this history can reduce the difficulty of reconstructing who submitted or changed a record (Dong et al., 2023; Hastig & Sodhi, 2020; Sodhi & Tang, 2019). It can also help a financier see whether a claim has already been transferred within the participating network. The benefit depends on the actual coverage and integrity of the network: a duplicate financed outside the network remains invisible unless an external registry or reconciliation process makes it observable.

Tamper evidence should be distinguished from absolute immutability. The practical security of a permissioned system depends on node permissions, consensus arrangements, key management, software updates, and the number and independence of validating organizations. An administrator with excessive privileges, a compromised signing key, or a coalition of nodes may invalidate a simplistic assumption that every entry is beyond challenge. Auditors should be able to trace the origin and authorization of an entry, compare a hash or signature with the underlying evidence, and review changes in node governance. The technical fact that a record exists is different from the business and legal question of whether the receivable is genuine or enforceable (Babich & Hilary, 2020; Franke et al., 2024; Hastig & Sodhi, 2020; Rui & Lai, 2015).

Provenance is most useful when the underlying events are specified precisely. For example, “invoice uploaded,” “buyer representative signed acceptance,” “carrier recorded delivery,” and “bank approved financing” are different events with different evidentiary value. A system should not label all of them simply as “trade verified.” The original data may be held off chain while the ledger stores references, hashes, or proofs, reducing unnecessary disclosure and allowing controlled access. This architecture still requires durable storage, reliable retrieval rights, and procedures for correction or deletion where applicable. Cryptographic commitments can help reveal whether a retrieved file differs from the committed version, but cannot reveal whether that version was truthful when created.

Blockchain's economic value depends on the arrangement being analyzed. Chod et al. (2020) model verifiable transaction information as a financing signal, whereas Cui et al. (2024) study the trade-off between transparency and the competitive cost of sharing data. Dong et al. (2023) examine deep-tier finance, and Iyengar et al. (2024) analyze adoption when a manufacturer has market power. These models identify conditional mechanisms rather than prove that every deployment reduces fraud.

Traceability research examines the business requirements and design of traceability-driven blockchains (Cui et al., 2023; Hastig & Sodhi, 2020). Work on RFID adoption and counterfeiting illustrates how technology adoption and verification incentives may matter in other supply chains (Pun et al., 2021; Shen et al., 2022; Whang, 2010), but those findings should not be transferred automatically to receivables finance. Research on emerging technologies also describes the gap that can arise between expected and realized benefits (Sodhi et al., 2022).

4.2 AI-supported identification of suspicious relationships

AI can assist investigators by combining signals that are difficult to assess manually across large numbers of firms and transactions. A model might examine repeated invoices, unusual invoice-to-shipment timing, unexpected changes in counterparties, rapid financing and repayment cycles, shared contact details, or patterns of circular payments. Graph-based methods represent entities as nodes and relationships as edges, allowing models to search for connected groups, shared controllers, or suspicious transaction paths (C. Li et al., 2023; Van Vlasselaer et al., 2017). These methods are useful for generating leads, especially when a coordinated group distributes its activity across many accounts. They do not, by themselves, prove a fraudulent agreement or explain the commercial purpose of a transaction.

The transfer of analytics into SCF requires care. Network-based fraud work in social-security administration illustrates how relationships among companies can help identify potentially suspicious entities (Van Vlasselaer et al., 2017), while credit-rating research uses supplier–customer links to predict credit risk (Wu et al., 2022). These are different settings and outcomes. Neither study establishes that a model trained on its data will detect coordinated receivables fraud. SCF transactions may be infrequent, values large, verification slow, and labels dependent on legal or internal investigations; a network connection can represent ordinary commercial activity as well as a risk signal.

Data leakage is a major practical concern. If a model uses a court outcome, a later repayment status, or an investigation note that was unavailable when the original loan decision was made, a retrospective test can substantially overstate real-world performance. Training and evaluation should respect the timing of information, with entity-level and temporal separation where appropriate. Test sets should include later periods, new firms, and different regions or sectors. Because suspicious cases may be selectively investigated, labels can be incomplete or biased toward behaviors that existing rules are already good at detecting. Continuous monitoring, investigator feedback, and independent testing are needed to assess whether models remain useful as participants change behavior.

An AI score should support a decision process rather than become an unchallengeable verdict. Lending studies show why accuracy and interpretability both matter when automated analysis affects financing decisions (Berg et al., 2020; Fu et al., 2022). Risk teams should know the data sources available at scoring time, the model version, the threshold and its rationale, and the actions expected after an alert. Firms should have a proportionate way to correct factual errors and seek review. Explanations can be incomplete or unstable, so a plausible feature attribution is not a substitute for evidence that a model is fair, calibrated, and appropriate for the transaction being assessed.

4.3 Multi-source verification, sensors, and oracles

The most important technical boundary is the link between digital records and the underlying commercial event. An oracle is a mechanism for bringing external information into a blockchain application. An oracle

can relay data from tax, logistics, bank, warehouse, or other systems, but its reliability depends on the source, the transmission process, and the incentives of the party providing the data (Babich & Hilary, 2020; Franke et al., 2024). Multiple feeds do not necessarily create independence: several feeds may reproduce the same supplier-provided statement or depend on a common data vendor. Identifying common control and common failure modes matters as much as counting the number of feeds.

Sensors can contribute observations about location, temperature, weight, or entry to a warehouse. However, a sensor reading does not automatically demonstrate ownership, authenticity, or delivery of a particular item. A device can be attached to the wrong container, lose connectivity, be substituted, or be calibrated improperly. Modeling work on supplier product adulteration illustrates why inspection and incentives remain relevant to physical-product integrity (Rui & Lai, 2015). In receivables finance, a defensible design should link each observation to a specific transaction, record the responsible operator and time, and provide for calibration, inspection, and incident reporting. These measures increase assurance but do not eliminate the need for commercial and legal verification.

Cross-checking should follow a hierarchy of independence. A signed buyer acceptance may be corroborated against a carrier's independently held shipment record and a bank's payment record where access is authorized. Tax or customs records may supply additional evidence, subject to availability, timeliness, and legal restrictions. Disagreements should be retained as reviewable events rather than overwritten to create a superficially clean record. A reasonable audit trail identifies which records were checked, what was unavailable, and which uncertainty remained when financing was approved. Where independent sources are unavailable, decisions should reflect that limitation rather than treat the absence of contradictory data as proof of authenticity.

A data-sharing arrangement must balance verification with the possibility that information recipients use sensitive data against the provider. Research on supply-chain disclosure and information protection examines transparency, confidentiality, and leakage under different contractual settings (Guan et al., 2020; L. Li & Zhang, 2008; T. Li et al., 2014; Y. Chen & Özer, 2019). Studies of supplier auditing and audit-information sharing in other supply networks likewise show why the source and verification of an assertion should be explicit (J. Chen et al., 2020; Ha et al., 2023). These findings inform the design of data governance; their original outcomes are not direct observations of factoring fraud.

4.4 Smart contracts and controllable automation

Smart contracts can encode actions such as recording an assignment, issuing an alert when a payment date passes, calculating a contractual fee, or initiating a transfer after specified confirmations. The potential benefit is consistent application of agreed rules and a traceable record of their execution (Babich & Hilary, 2020; Cong & He, 2019; Cong et al., 2023). For example, a financing program can require two authorized confirmations before changing the registered holder of a claim. The rule becomes useful only when the identities, authority, input data, and exception procedures have been established outside the code as well as within it.

Automatic execution has limits. A delivery can be disputed, goods can be returned, a court can order a payment to be suspended, or the original code can contain an error. Contractual arrangements should specify when a transfer can be paused, who may initiate review, how the pause is logged, and how an affected party can contest the decision. Security testing, access control, software-change procedures, and emergency recovery are necessary because code may behave exactly as written while producing an outcome that conflicts with the parties' intended agreement (Babich & Hilary, 2020). Legal recognition of an electronic record, a digital signature, and an automatically executed transaction also varies by jurisdiction and by the surrounding contractual facts.

Cong et al. (2023) examine the economic implications of a layer-2 solution for scaling blockchain-based smart contracts. The empirical setting concerns blockchain activity and scaling, not a controlled demonstration that a specific contract eliminated receivables fraud. This distinction matters for practice: evidence about technical adoption and transaction costs can clarify dependencies, while a claim about fraud prevention requires observations and a design that directly measure the risk of interest.

4.5 Reputation, incentives, and the cost of circumvention

A shared record can help a financier observe performance over time, potentially rewarding reliable firms through faster review or more favorable financing. It can also make an adverse history visible to authorized participants. The deterrent effect depends on whether firms expect future consequences, whether records can be attributed to the correct entity, and whether a firm can evade consequences by creating a new legal entity or moving to another platform. A persistent score may also penalize a legitimate business for a disputed delivery or an error it did not cause. Reputation systems therefore require correction, review, retention, and appeal mechanisms, alongside limits on inappropriate sharing.

Technology may increase the cost of sustaining deception when independent checks make consistent fabrication more difficult, records are reviewed, and a detected violation has credible consequences. Conversely, costs can remain low when the same parties control all inputs, regulators cannot access relevant records, or penalties are unlikely to be enforced. The effect is thus conditional: the relevant comparison is the expected benefit of misrepresentation against the expected cost of verification failure, detection, sanction, exclusion, and subsequent correction. The technology affects some of these elements, but institutional enforcement and market access affect others.

Differentiated financing is another possible channel. Where legally permissible and supported by robust evidence, a financier may adjust rates, advance ratios, collateral requirements, or review intensity according to assessed risk. These decisions can encourage truthful reporting, but differential terms also create risks of biased exclusion or feedback loops. A supplier rejected by a model may have fewer opportunities to build a credit history, making future access harder. Performance and fairness should therefore be assessed by firm size, sector, geography, and data availability where such comparisons are lawful and statistically meaningful (Berg et al., 2020; Fu et al., 2022). Table 2 summarizes the technological mechanisms, their conditions, and residual risks. The five-layer governance framework is illustrated in Figure 2.

Table 2. Technological Mechanisms, Conditions, and Residual Risks

Mechanism	Potential contribution	Condition for useful operation	Residual risk
Shared ledger	History of authorized status changes	Participating nodes, reliable identity and timely updates	Recording does not establish truth; incomplete network coverage
AI and graph analytics	Prioritize anomalies and related entities for review	Relevant data, appropriate labels and temporal validation	False alerts, missed cases, biased data and adaptation
Oracles and external data	Bring external observations into a workflow	Independent sources, secure transmission and authority	Shared upstream sources, compromised providers or stale feeds
Smart contracts	Consistent execution of specified rules	Tested code, authorized inputs and exception procedures	Coding errors, disputed obligations and legal uncertainty

Mechanism	Potential contribution	Condition for useful operation	Residual risk
Reputation and financing terms	Link verified behavior to future decisions	Reliable attribution, proportionality and review rights	Exclusion, erroneous records and evasion across platforms

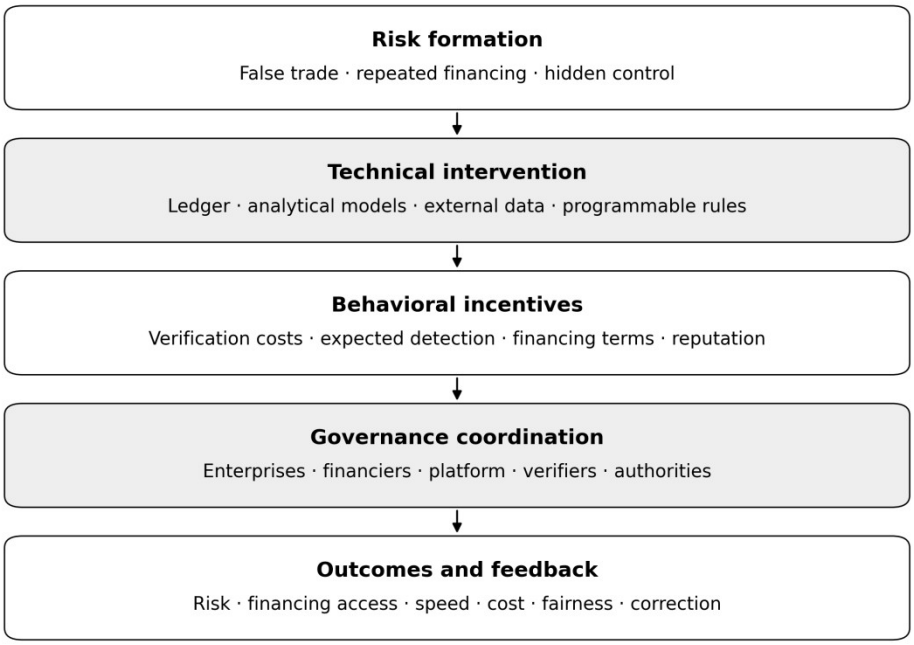


Figure 2. A Five-Layer Framework for Collusion and Fraud Governance in Supply Chain Finance

4.6 An integrated verification workflow

The following workflow translates the four technical channels into a sequence of decisions. First, an institution verifies the legal identity and authority of the parties and assigns a persistent claim identifier. It records the source and time of the initial invoice and the basis for the buyer's confirmation. This step should explicitly identify the authority level of the person or system submitting each record. If an authorization cannot be verified, the workflow records that uncertainty instead of converting a missing answer into a positive confirmation.

Second, the financier checks the status of the receivable against available assignment, payment, and financing records. Where several institutions participate, reconciliation should distinguish an exact match from a possible match that requires manual review. A shared identifier reduces ambiguity only within the domains that use it consistently. Where possible, an independent delivery or acceptance source can be linked to the claim, and the system should record whether that source is controlled by the buyer, supplier, platform, or an unrelated party. An apparently consistent invoice, delivery note, and acceptance that all originate from the same administrative account should receive less corroborative weight than genuinely independent observations.

Third, an analytics layer may rank exceptions for human investigation. Wu et al. (2022) use supplier–customer links in machine-learning models of credit ratings, whereas C. Li et al. (2023) examine linked-firm

information in predicting accounting fraud. These outcomes and data differ from verified collusive factoring fraud. The studies illustrate how relationships can be used in financial risk analysis, but neither by itself validates prospective performance against adjudicated collusion cases on an operational platform. A deployable workflow should record information available at scoring time, the model version, the reason for review, and the investigator's final disposition.

Finally, a decision must have an accountable owner. A bank may approve subject to additional evidence, request correction, postpone a transaction, or escalate a serious allegation under its applicable procedures. A smart contract can implement an authorized status change or a temporary hold where the contract and law permit it. An independent reviewer should be able to reconstruct what was known, what remained uncertain, and who made each decision. This sequence reduces the risk that an automated score or a platform's status label is treated as conclusive proof.

5. Stakeholder Interactions and Governance Coordination

5.1 Decomposing the enterprise alliance

Some analytical models aggregate a buyer and supplier into a single enterprise alliance to study their joint external strategy. This abstraction can clarify how a coordinated action affects a lender, but it suppresses the negotiation that precedes the agreement and the distribution of benefits afterward. In practice, a large buyer and a small supplier can have different access to finance, different control over data, and different outside options. They may also face different legal consequences or incentives to disclose misconduct. A supplier might agree under commercial pressure, whereas a buyer might exploit its authority to confirm or delay an invoice. These possibilities cannot be inferred from a model that treats the alliance as a single decision maker.

A richer representation separates at least the buyer, supplier, financier, platform, and relevant verification actors. It allows one participant to refuse, report, or withdraw from an arrangement and permits an insider or third-party provider to participate in the deception. Such detail does not automatically make a model more accurate; it increases the number of assumptions and the data needed to identify parameters. The purpose is to identify which assumptions change the result. Bargaining power, the credibility of whistleblowing channels, and the ability to switch lenders are especially relevant to whether a formal anti-fraud policy is effective in practice.

Governance and bargaining research provides further context. Interorganizational trust can influence the form and performance of governance arrangements (Gulati & Nickerson, 2008), while evidence on supply-chain structure shows that visibility depends on the network being observed (Gualandris et al., 2021). Contract design under asymmetric information can affect participation (Corbett et al., 2004), while research on bidding in peer-to-peer lending illustrates related information problems in a distinct financing setting (Gao et al., 2023). Related research on supplier oversight, reporting incentives, and behavioral responses to partner misconduct informs how an institution might design escalation channels (Dennis & Johnstone, 2018; L. Chen & Lee, 2017; Patterson et al., 2019; Stikeleather, 2016).

5.2 Financial institutions and platform operators

Banks and factors decide which information they require, which risks they are prepared to finance, and how much independent review is economically justified. A platform can lower duplication of administrative work when participants share standardized data, but the financier remains responsible for understanding the data's origin and limitations. If platform participation becomes a substitute for all other due diligence, a new common point of failure can emerge. A lender should assess service-provider security, control rights, incident response, and the availability of records for disputes and audits rather than equating platform membership with verified creditworthiness (Hastig & Sodhi, 2020; Lumineau et al., 2021).

Platform operators choose onboarding rules, node permissions, data-access policies, fees, and procedures for changing software. These choices shape who benefits from information sharing and who bears the cost of errors. A buyer-controlled platform, an independent consortium, and a public registry may face different conflicts of interest. The platform's own operational incentives deserve examination: income from transaction volume or rapid approvals may conflict with incentives to investigate suspicious participants. Governance can include independent assurance, separation of administrative duties, controlled regulator access, and documented responsibility for correcting errors. The appropriate arrangement will differ by legal structure and market context.

Participation also depends on how platforms attract and retain different users. A model of reward-based crowdfunding studies platform design under risks of misappropriation and performance opacity (Belavina et al., 2020), while research on participants who assume multiple roles on blockchain platforms (T. Li & Zhang, 2024) examines another aspect of platform development. Neither study establishes a fraud-reduction effect in SCF; together they highlight the need to account for participant behavior and platform incentives when assessing a proposed governance intervention.

5.3 Government and regulatory coordination

Public authorities can influence SCF through licensing, information-sharing standards, supervision, enforcement, and policies supporting smaller firms. Their actions interact with the capacity and incentives of private actors. Strong verification and credible enforcement may complement a shared ledger by making an inaccurate entry more likely to be challenged and by increasing the expected consequences of misconduct. Conversely, poor access to records or a lack of authority to act can make an otherwise sophisticated platform ineffective as a governance instrument.

Regulatory intensity should not be treated as a single switch. It can vary across onboarding inspections, transaction monitoring, independent audits, data access, sanctions, and remedies. A risk-based approach may reduce routine duplication in well-controlled transactions while increasing targeted investigation of high-risk cases. Whether this improves outcomes depends on evidence about independent data coverage, false alerts, incident response, and supervisory resources. It is not safe to infer that a mature technology automatically justifies weaker supervision; a high volume of transactions or a long operating history does not by itself prove that collusion is being detected.

Supervision depends on whether participants have incentives and authority to act. L. Chen and Lee (2017) model certification, process audits, and contingency payments under supplier responsibility risk; Stikeleather (2016) examines incentives for reporting internal misconduct. These studies concern different governance settings and should not be read as tests of a particular financial regulation. They illustrate why access to an alert must be paired with authority, incentives, and a credible process for investigation.

5.4 What game-theoretic models can and cannot establish

Game-theoretic models clarify how the financing terms of one party depend on the decisions of others. Dong et al. (2023) model blockchain-enabled financing across three supply-chain tiers, while W. Wang and Cai (2024) analyze bank lending and loan insurance under risk regulations. The models compare specified strategic settings rather than report observed changes in collusion. Other research examines how credit ratings, supplier financing, and bargaining power affect operational choices (Kouvelis & Zhao, 2018; Yan et al., 2024; Zhou et al., 2020).

The resulting equilibria are conditional on the strategy set, payoff functions, parameter values, and behavioral dynamics chosen by the modelers. A simulation with higher detection probability after blockchain adoption does not independently establish that a real platform achieves that increase. Similarly, a result under binary strict and loose supervision cannot directly identify the optimal mix of inspections, audits, sanctions, and

appeals. These models are most valuable when treated as generators of testable propositions, followed by sensitivity analysis, empirical calibration, and comparison with alternative institutional arrangements.

One useful proposition is that additional on-chain documentation is more likely to deter coordinated misrepresentation when at least some evidence comes from sources outside the control of the suspected participants. Another is that the effect of an alert depends on whether investigators can act on it and whether participants expect credible consequences. A third is that cost sharing can improve participation, but subsidies may be ineffective if they do not resolve weak data quality or unequal bargaining power. These propositions express possible mechanisms to investigate; they are not conclusions established for all sectors or jurisdictions. The illustrative governance priorities are shown in Figure 3.

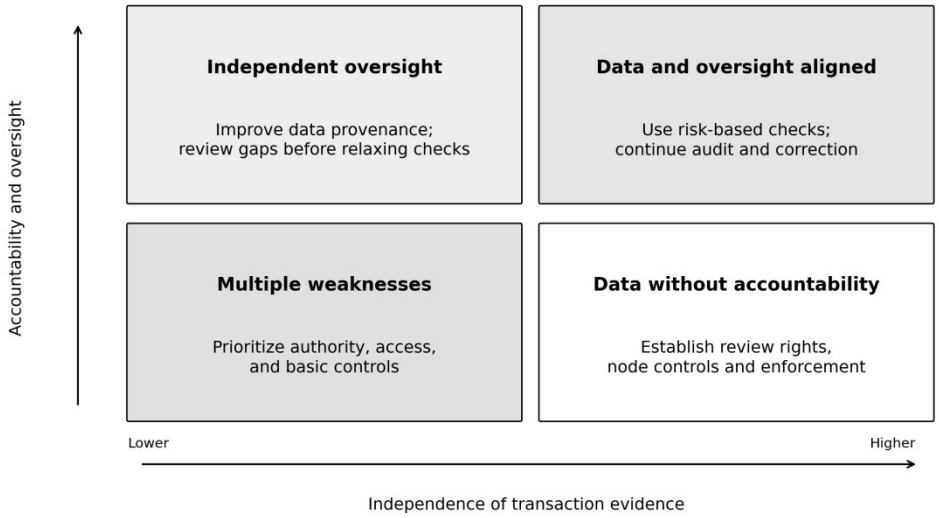


Figure 3. Illustrative Governance Priorities across Data Independence and Oversight

Note: The quadrants are conceptual and are not empirical thresholds.

5.5 Governance arrangements and distribution of responsibility

A platform is a governance arrangement as well as a technical system. Node operators decide how new participants enter, which data are accepted, whether software changes require approval, and who can access disputed records. Lumineau et al. (2021) discuss blockchain as a form of interorganizational governance, while Franke et al. (2024) model conditions under which blockchain networks can provide information. These studies illuminate governance choices and information limits; their conclusions should be interpreted within the settings studied.

The identity of the platform operator matters. A buyer-led system may obtain participation rapidly from suppliers already dependent on the buyer, but the same concentration of control can make it harder for a supplier to contest a buyer's record. A bank-led system may have stronger access to payment information but limited visibility into goods or another bank's financing. A multi-party consortium can distribute decision rights, yet a nominally diverse node list may still be controlled by related firms. Governance disclosures should therefore describe actual control over membership, keys, rule changes, data corrections, and emergency suspension—not merely the number of registered nodes.

Trust also depends on how records are corrected when the interests of participants conflict. One useful arrangement separates the party that submits a disputed assertion, the party that investigates it, and the authority that can approve a correction. An immutable audit trail can retain the original entry and the later correction without forcing all participants to rely on an erroneous current status. The affected firm needs a channel to present evidence, a documented response time, and a proportionate remedy where financing was wrongly delayed. The most suitable arrangement is an empirical and legal question; imposing the same governance structure on every jurisdiction could generate unnecessary cost or conflict with applicable obligations.

Research outside SCF also highlights the gap between records and underlying conduct. Rui and Lai (2015) model deferred payment and inspection under supplier product-adulteration risk. Their analysis illustrates how verification and contract incentives can affect behavior in physical-product supply chains; it is not evidence of receivables-financing fraud. The broader implication is that researchers should examine incentives and actual verification rather than assume that a transparency system changes all underlying conduct.

Several adjacent studies illuminate governance boundaries. Research on supplier transparency under outside scrutiny and on the market consequences of the Rana Plaza disaster addresses sustainability and sourcing rather than financing fraud (Jacobs & Singhal, 2017; S. Chen et al., 2019). Work on product adulteration and organizational misconduct examines incentives and conditions that may shape wrongdoing (Bianchi & Mohliver, 2016; Rui & Lai, 2015). These are contextual analogies, not estimates of SCF fraud rates.

Detection studies also address different stages of an investigation. Accounting research examines omission strategies, the role of internal-audit reporting, and the triangulation of evidence (Hamilton & Smith, 2021; Norman et al., 2010; Trotman & Wright, 2012). Related work considers auditor tenure and the information content of credit ratings for fraud prediction (A. Huang et al., 2023; Patterson et al., 2019). These findings suggest practical questions about review design, but they do not establish that a particular on-chain score is a legal finding of collusion.

6. Evidence, Cases, and Evaluation

6.1 What different research designs show

The literature contains valuable but heterogeneous evidence. Analytical research on supply-chain financing describes how financing, operating decisions, and blockchain adoption can interact under specified cost and risk conditions (Dong et al., 2023). Game-theoretic studies compare possible strategic outcomes under assumed incentives and technology effects (Dong et al., 2023; W. Wang & Cai, 2024). Such work identifies causal pathways that might matter, but the parameters are not necessarily measured in the field. An equilibrium can change if a detection probability, adoption cost, or sanction is changed; establishing those values requires separate data.

Firm-level and supply-network empirical research offers a different perspective. Wuttke et al. (2019) analyze adoption of SCF programs, Wu et al. (2022) examine whether supplier–customer information improves credit-rating prediction, and Cong et al. (2023) study a scaling solution for blockchain-based smart contracts. These outcomes concern adoption, prediction, and technical activity; they are not direct measures of verified collusive factoring fraud. Firms that adopt a technology or enter a program can differ from other firms in digital capacity, internal controls, and access to finance; credible causal interpretation depends on the research design and its assumptions.

Qualitative case research can reveal operational details hidden in numerical indicators. Sternberg et al. (2023) examine technology management and agency in multi-tier outsourced logistics, while X. Wang and Xu (2023) model the role of smart contracts in trade finance. The studies address different settings and use

different methods: one examines organizational relationships, and the other develops an analytical model. Neither establishes an average reduction in collusive financing fraud across platforms, but both can inform hypotheses about implementation and incentives.

Analytical and design-oriented studies add another evidence category. Chod et al. (2020) develop a financing theory and describe a blockchain protocol for verifiable supply-chain transactions. Franke et al. (2024) model the potential and limits of blockchain networks for information provision. These contributions inform technical and governance mechanisms; neither result should be interpreted as a field estimate of collusion prevented in receivables factoring. Fraud prediction research (C. Li et al., 2023; Van Vlasselaer et al., 2017) likewise requires careful attention to the outcome being predicted and the context in which the model is evaluated. Table 3 maps representative studies to the questions they can address.

Table 3. Representative Research and the Scope of Its Evidence

Study	Design or evidence	Contribution to this review	Interpretive boundary
Kouvelis and Xu (2021)	Analytical model	Contrasts factoring and reverse factoring	Model results depend on specified assumptions
Dong et al. (2023)	Multi-tier analytical model	Examines blockchain-enabled financing choices	Model conditions are not observed fraud outcomes
Wuttke et al. (2019)	Empirical adoption study	Examines supplier adoption of SCF	Adoption is not verified collusive fraud
X. Wang and Xu (2023)	Analytical model	Examines smart contracts and trade finance	Model outcomes depend on specified assumptions
Cong et al. (2023)	Empirical blockchain study	Examines smart-contract scaling	Scaling is not a fraud measure
C. Li et al. (2023)	Linked-firm fraud prediction	Uses customer data to study accounting fraud	Accounting fraud is not proof of factoring collusion
Wu et al. (2022)	Machine-learning credit prediction	Uses supply-chain links to predict ratings	Credit ratings are not fraud labels
Franke et al. (2024)	Analytical information model	Examines information provision	Not an empirical receivables-finance test

6.2 Comparing analytical and empirical examples

The first example is the empirical accounting-fraud study by C. Li et al. (2023), which combines information from economically linked suppliers and customers. It illustrates how inconsistencies between different parties' records can add information to a fraud-prediction model. The study focuses on accounting fraud and does not establish that a detected case involved collusive factoring or blockchain use. Its practical value for this review is the emphasis on external corroboration and the limits of an entity-only view.

The second example is the empirical study by Cong et al. (2023), which examines a layer-2 approach to scaling smart contracts. It illustrates how a technology intervention can be assessed using evidence on blockchain activity. Its setting and outcomes differ from receivables finance, so its results should not be repurposed as an estimated reduction in SCF fraud.

The third example is the analytical model of smart contracts in trade finance by X. Wang and Xu (2023). The authors examine how contractual commitment can affect firms, financing decisions, and bank risk under

specified assumptions. The model helps identify possible mechanisms, but it does not estimate a platform fraud-detection rate or establish the authenticity of any transaction. Table 4 summarizes what can and cannot be inferred from these examples.

Table 4. Illustrative Studies and What They Establish

Study	Focus	Useful insight	What it does not establish
C. Li et al. (2023)	Accounting fraud and linked-firm data	Customer information can contribute to prediction	Does not establish blockchain use or factoring collusion
Cong et al. (2023)	Smart-contract scaling	Examines layer-2 blockchain activity	Does not measure SCF fraud reduction
X. Wang and Xu (2023)	Smart contracts and trade finance	Models financing and contractual incentives	Does not estimate a fraud-detection rate
Franke et al. (2024)	Blockchain information provision	Models benefits and limits of data participation	Does not verify underlying receivables

6.3 Measuring governance outcomes

A credible evaluation begins by specifying the outcome. Possible operational measures include the share of receivables matched to independent evidence, time from issue to verified financing, frequency of unresolved data discrepancies, and time needed to reconstruct an evidence trail. Financial outcomes include financing rates, advance ratios, approval rates, transaction costs, and payment delay. Security and governance measures include unauthorized access, delayed status updates, unresolved correction requests, and the time required to revoke a compromised credential. These indicators should be interpreted alongside firm size and transaction type so that a system is not judged successful solely because it serves less risky or better documented firms.

For an alerting model, precision is the proportion of reviewed alerts confirmed as relevant under a defined investigation standard; recall is the share of known relevant cases that the model identifies. The false-positive rate uses non-fraudulent cases as its denominator. Each measure depends on how cases are labeled and on which alerts receive investigation. A high overall accuracy can be uninformative when confirmed fraud is rare. Investigators should therefore report the base rate, the number and maturity of labels, the volume of alerts that can actually be reviewed, and the financial and non-financial costs of both missed cases and incorrect flags. A legal finding of fraud, an internal compliance breach, and a model alert should be coded separately.

Comparisons also require an appropriate baseline. A simple decrease in recorded fraud after a platform launch may reflect less investigation, a change in definitions, economic conditions, or selection of participants. A stronger design could compare similar transactions or firms before and after adoption, while examining changes in investigative effort and reporting. Where a randomized rollout is feasible and ethical, it can clarify whether an intervention changed outcomes; otherwise, well-documented observational designs can use matched comparisons, event studies, and sensitivity analyses. No design should claim a counterfactual effect without considering possible spillovers and changes in the composition of cases.

A numerical illustration shows why operational evaluation matters. Suppose, solely for illustration, that 1% of 10,000 transactions are fraudulent, an alerting rule identifies 80% of fraudulent transactions, and 5% of legitimate transactions also trigger an alert. The rule would flag 80 fraudulent and 495 legitimate transactions, so approximately 14% of its alerts would concern fraud. These numbers are hypothetical, not estimates for an SCF market. They show that even a seemingly low false-positive rate can create a substantial review

burden when fraud is rare, and that thresholds should be chosen together with investigation capacity and the consequences of error. Examples of governance evaluation measures are summarized in Table 5.

Table 5. Examples of Measures for Evaluating Governance

Measure	What it can reveal	Interpretation or limitation
Evidence independence and coverage	Whether important claims have independent corroboration	Count common control and missing sources, not just documents
Alert precision and recall	How alerts relate to confirmed relevant cases	Depends on base rates, label quality and review selection
False-positive burden	Cost of incorrectly flagged legitimate transactions	Report rate, number, delay and review capacity
Confirmed incidents and losses	Observed fraud or compliance outcomes	Detection effort and legal disposition affect measurement
Financing access and cost	Approval, rates, advance ratio and processing time	Compare similar firms and consider changes in payment terms
Correction and appeal time	Whether errors can be remedied	A fast process must also be accessible and fair

6.4 Financial-risk evidence and documented platform research

Research directly linking economic relationships and financial risk offers a useful evidence base. C. Li et al. (2023) use supplier–customer information to study accounting fraud, and A. Huang et al. (2023) examine whether changes in credit ratings add information for predicting accounting fraud. Both papers investigate financial misreporting rather than directly adjudicated collusive factoring. Their results should therefore be used to design and evaluate candidate signals, not to infer that a platform has reduced buyer–supplier collusion.

Wu et al. (2022) analyze machine-learning prediction of credit ratings using supply-chain relationships. Their study is relevant to feature construction and credit-risk assessment, but a rating is a broader outcome than fraud. Van Vlasselaer et al. (2017) examine network-based fraud detection in a social-security setting; transfer to SCF requires new data and validation. Researchers should document who creates the labels, how the network is built, and which observations are available at the time of prediction.

X. Wang and Xu (2023) analyze smart-contract mechanisms in trade finance, while Wuttke et al. (2019) examine supplier adoption of SCF. These studies provide analytical and empirical perspectives on financing and participation. They cannot, without direct fraud outcomes and an appropriate comparison, establish the authenticity of every transaction on a platform or a causal reduction in collusion. Separately, Cong et al. (2023) examine smart-contract scaling; the difference in setting and outcome should remain explicit.

Analytical work also indicates that the value of transparency depends on strategic structure. Dong et al. (2023) compare financing arrangements in a multi-tier supply chain, and Iyengar et al. (2024) analyze blockchain adoption under manufacturer market power. These models are not empirical tests of collusive factoring. They illustrate why researchers must specify who controls the technology, who benefits from the information, and how financing and operational decisions interact.

7. Challenges and Future Research Directions

7.1 Establishing data independence rather than counting records

Future systems should represent not only the existence of documents but also their lineage and control. A useful data model would identify who created a record, who had authority to sign it, whether the source is connected to another participant, which system transmitted it, and whether the source changed after the financing decision. Researchers could compare three configurations: evidence controlled by one commercial group, evidence from multiple but affiliated providers, and evidence from independent providers. The hypothesis is that independence improves the value of corroboration, but its effect should be evaluated against collection costs, coverage, and the possibility that an apparently independent provider is compromised.

One research design would use audited transaction histories to test whether independently sourced delivery, payment, and registration records identify discrepancies earlier than firm-supplied documents alone. The study should report missingness and identify whether participating firms are representative. A second design could assess simulated data-tampering incidents in an authorized test environment to measure whether audit logs allow the responsible entry and credential to be identified. Such tests can establish operational capabilities under controlled conditions; they cannot be treated as observed real-world fraud prevention without field evidence.

7.2 Building reliable labels for coordinated behavior

A central obstacle is the scarcity of verified examples of collusion. Many datasets record default, late payment, or internal alerts but do not establish whether two parties knowingly coordinated. Labels should therefore distinguish the observed anomaly, the investigative finding, and any legal disposition. Investigations should document when evidence became available and whether the allegation was substantiated, dismissed, or unresolved. Privacy-preserving collaboration between financial institutions and researchers could improve coverage, but access agreements and legal authority are needed because transaction and investigation records are sensitive.

Benchmark datasets should avoid presenting synthetic cases as if they were discovered cases. Simulated examples are valuable for testing whether a system can process certain patterns and recover a planted relationship, but the design of those patterns determines what the model can learn. Evaluation should include temporal holdouts, unseen organizations, changes in fraud tactics, and cases with incomplete or conflicting records. Differences in base rates and investigation capacity across institutions should be reported so that operational precision is not confused with model discrimination. A public benchmark would be useful only if its construction and privacy risks are transparent.

7.3 Modeling strategic adaptation and unequal power

A fraud-governance mechanism can change the behavior it seeks to observe. Once participants know that direct ownership links are monitored, they may use intermediaries or shift transactions to another channel; legitimate firms may also change behavior because a new process is expensive or difficult to understand. Future models should consider these adaptive responses, the costs of evasion, and the possibility that detection in one network displaces risk to another. Changes in observed alerts alone cannot distinguish deterrence from displacement.

The assumption that a buyer and supplier act as one alliance should be relaxed when the question concerns how collusion forms. A multi-agent model could allow a dominant buyer to propose an arrangement, a supplier to accept or refuse, a verifier to inspect, and a financier to adjust terms. Alternative scenarios should allow an insider to misrepresent authority, a supplier to report pressure, and an honest firm to be wrongly flagged. Parameters for bargaining power, monitoring, and sanctions should be estimated or bounded using

interviews, transaction records, enforcement data, and institutional knowledge rather than selected solely to produce a preferred equilibrium.

7.4 Evaluating platform adoption and causal effects

A promising empirical agenda compares fraud-related and financing outcomes across adopters and appropriately selected comparison groups. Researchers should document what "adoption" means: announcing a blockchain initiative, joining a consortium, recording a limited set of documents, and relying on a platform for financing decisions are materially different exposures. Adoption dates may also vary across buyers and suppliers. Treating all exposure as a single binary indicator can conceal the mechanisms of interest (Cong et al., 2023; Lumineau et al., 2021; Wuttke et al., 2019; X. Wang & Xu, 2023).

A staged rollout can provide useful variation if timing is not entirely determined by expected performance. An event-study or difference-in-differences analysis should examine pre-existing trends, concurrent policy changes, sample composition, and spillovers to nonparticipating firms. If an institution randomizes the order in which eligible transactions receive an additional verification process, the evaluation should include consent, safeguards, and an assessment of interference between connected firms. In either case, outcomes should include confirmed fraud and investigation capacity where available, as well as ordinary credit and operational metrics. If fraud events are too rare for precise estimation, authors should say so rather than substitute a broad credit score and label it a fraud measure.

For staggered adoption, researchers can define a cohort by the period in which a firm first uses a specified verification feature and estimate cohort-by-time effects against a defensible comparison group. De Chaisemartin and D'Haultfœuille (2020) show that two-way fixed-effects estimators can assign problematic weights when treatment effects differ across groups and periods. Alternative estimators still require credible identification assumptions; a flat pre-treatment pattern alone does not prove parallel trends after adoption. Researchers should specify anticipation, treatment reversals, missing outcomes, network spillovers, and the level at which uncertainty is clustered.

Credit data and model-generated variables require separate validation. Studies of financial technology and digital footprints examine lending and prediction using contexts outside SCF (Berg et al., 2020; Gopal & Schnabl, 2022), while Wu et al. (2022) use supply-chain relationships for credit-rating prediction. Model transparency can itself affect the behavior of those being scored (Bauer & Gill, 2024), and research on algorithmic fairness examines disparate impacts in settings that include insurance pricing (Fu et al., 2022; Zhang & Xu, 2024). Research on systematic prediction mistakes also shows why biased forecasts require careful assessment (Rambachan, 2024). These studies support careful validation, not an assumption that a single model is equally accurate or fair for all suppliers.

7.5 Making AI decisions auditable and contestable

AI governance should cover data acquisition, model development, validation, deployment, monitoring, investigation, and correction. Research on algorithmic assessments and fairness (Bauer & Gill, 2024; Fu et al., 2022; Zhang & Xu, 2024) highlights how disclosure and the behavior of affected parties can interact with the design of a model. For this application, practical controls include documenting intended use and exclusions, retaining model versions and training periods, testing temporal stability, recording manual overrides, and monitoring error patterns across relevant groups. Explanations should accompany, not replace, evidence about accuracy, validity, and the availability of review.

An explanation should identify actionable information without disclosing protected investigative techniques or exposing sensitive information about another firm. A supplier might be told that a document date or ownership identifier needs confirmation, while an investigator reviews a broader risk pattern under controlled access. A correction should be traceable and should propagate to authorized systems when an erroneous

record affected earlier decisions. Research should examine whether explanations and appeals actually reduce erroneous exclusion, rather than assuming that displaying feature scores is sufficient.

7.6 Privacy, interoperability, and evidence

SCF information can reveal prices, supplier relationships, shipment routes, and financing terms. Broad visibility of every transaction is therefore neither necessary nor always desirable. A permissioned design can restrict access by role, keep sensitive documents off chain, and record cryptographic commitments or authorized status changes. Privacy-enhancing methods may enable limited verification across institutions, but they introduce costs and dependencies that must be assessed. A hash of a document, particularly one with predictable content, should not automatically be treated as anonymous data.

Cross-platform interoperability requires common identifiers and rules for authoritative updates, not just a technical connection. A unique identifier within one platform may not prevent a duplicate claim on another. Effective reconciliation requires agreement on matching fields, access rights, correction rules, and the handling of contested matches. Researchers should compare registry-based, platform-to-platform, and trusted-intermediary approaches, evaluating both false matches and missed duplicates. Evidence admissibility and digital-signature requirements vary across jurisdictions; legal analysis must be tied to the relevant contract and current law rather than assumed from the existence of a timestamp (Babich & Hilary, 2020; Hastig & Sodhi, 2020).

7.7 Aligning incentives, costs, and inclusion

The net value of an intelligent blockchain arrangement depends on who pays for onboarding, integration, data provision, independent checks, model operation, audit, and dispute resolution. A technology may reduce a bank's processing cost while increasing suppliers' compliance burden. It may also produce a more detailed risk profile without improving a smaller firm's access to affordable financing. Evaluations should therefore report costs and benefits by participant where possible, including implementation and continuing costs rather than only a platform's transaction volume.

Bargaining and cost-sharing models offer useful starting points (Dong et al., 2023; Kouvelis & Zhao, 2018). They should be complemented with interviews and transaction-level evidence about whether smaller firms can choose a provider, correct errors, and understand charges. Research on buyer intermediation highlights why payment terms and the distribution of financing benefits deserve explicit attention (Tunca & Zhu, 2018). A governance arrangement should also include accessible routes for firms with limited digital infrastructure or unusual transaction patterns, so that the absence of extensive historical data is not automatically treated as evidence of high fraud risk.

7.8 Designing proportionate supervision

A practical supervisory approach can use evidence-based checkpoints instead of a calendar-based declaration of technological maturity. Relevant checkpoints include the independence and coverage of data sources, the rate at which disputed records are corrected, node-control concentration, system-security incidents, audit access, and the accuracy and fairness of alerts. These indicators can inform which transactions require closer review and which routine checks may be simplified. They should not be used as mechanical thresholds until their reliability and unintended consequences have been tested.

A mature governance arrangement also needs escalation and recovery procedures. When an alert is credible, the responsible authority must be able to preserve relevant evidence, limit further exposure where legally justified, and provide an avenue for challenge. When the alert is incorrect, the firm should be able to correct the record and obtain timely reconsideration. An independent audit can check whether the platform's records match original evidence and whether investigators had access to the relevant data. Research should compare

the effectiveness and cost of these institutional arrangements, including whether measures deter misconduct or merely relocate it.

7.9 Comparing distributed ledgers with feasible alternatives

A rigorous technology evaluation needs a credible alternative to blockchain. A centralized registry with strong access controls, independent audit, signed records, and effective update procedures may address some of the same problems. Likewise, a shared database operated by a trusted third party can synchronize financing status without requiring each participant to maintain a ledger. The choice should depend on who can be trusted to administer the system, whether participants need an independently verifiable history, how disputes will be resolved, and the total costs of operation. A comparison between an automated blockchain platform and an entirely manual legacy process can overstate the contribution of the ledger if digitization itself explains much of the improvement.

Future studies should compare systems with similar data and oversight but different governance architectures. Relevant outcomes include the speed and completeness of status updates, the ability to detect unauthorized changes, service availability, onboarding costs, and the practical burden of recovering from a compromised credential. When a permissioned ledger is chosen, the comparison should account for node concentration and the authority of administrators. A system with transparent records and weak governance may perform worse than a conventional system with strong independent controls. This comparison also makes it possible to identify the circumstances in which a shared ledger is worth its added complexity.

7.10 Research transparency and reporting of negative outcomes

The evidence base would improve if researchers documented unsuccessful integrations, discontinued pilots, and controls that generated too many false alerts. Publication and access incentives may favor case studies of functioning platforms over studies of systems that failed to attract participants or could not obtain reliable independent data. Selective visibility makes the apparent benefits of technology difficult to interpret. Platform studies should report the number and characteristics of participants where available, the data actually captured, periods of operation, missing information, governance changes, and reasons for withdrawal or redesign.

Where disclosure is legally and commercially possible, researchers can preregister their primary outcomes and analytical plan, release code and data dictionaries, and provide a clear account of changes made after results were observed. Confidential transaction data need not be published indiscriminately; secure analysis environments, synthetic examples for code testing, and independent replication can provide alternative forms of scrutiny. Reporting uncertainty, null findings, and the limits of access to data helps distinguish an attractive design from a mechanism with demonstrated real-world value. The proposed research agenda and suitable study designs are summarized in Table 6.

Table 6. Future Research Agenda and Suitable Designs

Research priority	Testable question	Possible evidence or design
Independent data	Does source independence improve discrepancy detection?	Audited transaction histories and matched comparisons
Collusive networks	Which relationships identify coordinated behavior?	Temporal graphs with documented investigation outcomes
Technology adoption	Which features change access, cost or confirmed risk?	Staged rollout, event study or suitable comparison groups
AI accountability	Do explanations and appeals reduce erroneous exclusion?	Prospective tests with audit logs and reviewed outcomes

Research priority	Testable question	Possible evidence or design
Alternative architectures	When does a ledger outperform a governed shared database?	Comparable systems with common data and oversight
Costs and power	How are benefits and burdens distributed across actors?	Supplier surveys, contracts, fee data and interviews

8. Conclusion

Collusion and fraud in supply chain finance arise when participants can make a financing claim appear credible while concealing the true nature, ownership, or status of the underlying transaction. Blockchain records, AI-supported analysis, smart contracts, and external data can each address part of this problem. Their contribution depends on the quality and independence of data, the incentives and authority of participants, and the availability of human and institutional review. A ledger can strengthen the traceability of an assertion, while the assessment of whether that assertion reflects an authentic trade requires additional evidence and accountable decisions.

The proposed five-layer framework connects risk formation to technological mechanisms, incentives, coordinated oversight, and measurable outcomes. Existing theoretical models, prototypes, qualitative studies, observational research, and empirical studies illuminate different parts of this framework. They should not be combined into a general claim that intelligent blockchain has already eliminated collusive financing fraud. Future work should use better labeled transaction data, credible comparisons, explicit treatment of unequal bargaining power, and practical safeguards for errors and disputes. Progress will be strongest when financing access, risk reduction, operational cost, and accountability are evaluated together.

Acknowledgement

I acknowledge the scholarly contributions of the authors whose published work is cited in this review.

Author Contributions

Conceptualization, Methodology, Investigation, Formal Analysis, Data Curation, Validation, Visualization, Writing – Original Draft, Writing – Review & Editing, and Project Administration, Y.L. I have read and approved the final manuscript and take responsibility for the work.

Funding

I received no external funding for this review.

Conflicts of Interest

I declare no conflicts of interest.

Ethical Approval and Consent

This review analyzes published literature and did not involve new data collection from human participants or animals.

Data Availability Statement

The sources examined in this review are identified in the reference list. No new primary dataset was generated.

Declaration of Generative AI Use

I used generative AI tools to assist with manuscript formatting and declaration drafting. I reviewed the AI-assisted material and take responsibility for the final manuscript.

References

Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500. https://doi.org/10.2307/1879431

Babich, V., & Hilary, G. (2020). OM forum—Distributed ledgers and operations: What operations management researchers should know about Blockchain technology. *Manufacturing & Service Operations Management*, *22*(2), 223–240. https://doi.org/10.1287/msom.2018.0752

Bauer, K., & Gill, A. (2024). Mirror, mirror on the wall: Algorithmic assessments, transparency, and self-fulfilling prophecies. *Information Systems Research*, *35*(1), 226–248. https://doi.org/10.1287/isre.2023.1217

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, *76*(2), 169–217. https://doi.org/10.1086/259394

Belavina, E., Marinesi, S., & Tsoukalas, G. (2020). Rethinking crowdfunding platform design: Mechanisms to deter misconduct and improve efficiency. *Management Science*, *66*(11), 4980–4997. https://doi.org/10.1287/mnsc.2019.3482

Berg, T., Burg, V., Gombović, A., & Puri, M. (2020). On the rise of FinTechs: Credit scoring using digital footprints. *The Review of Financial Studies*, *33*(7), 2845–2897. https://doi.org/10.1093/rfs/hhz099

Biais, B., & Gollier, C. (1997). Trade credit and credit rationing. *Review of Financial Studies*, *10*(4), 903–937. https://doi.org/10.1093/rfs/10.4.903

Bianchi, E. C., & Mohliver, A. (2016). Do good times breed cheats? Prosperous times have immediate and lasting implications for CEO misconduct. *Organization Science*, *27*(6), 1488–1503. https://doi.org/10.1287/orsc.2016.1101

Chen, J., Qi, A., & Dawande, M. (2020). Supplier centrality and auditing priority in socially responsible supply chains. *Manufacturing & Service Operations Management*, *22*(6), 1199–1214. https://doi.org/10.1287/msom.2019.0790

Chen, L., & Lee, H. L. (2017). Sourcing under supplier responsibility risk: The effects of certification, audit, and contingency payment. *Management Science*, *63*(9), 2795–2812. https://doi.org/10.1287/mnsc.2016.2466

Chen, S., Zhang, Q., & Zhou, Y. P. (2019). Impact of supply chain transparency on sustainability under NGO scrutiny. *Production and Operations Management*, *28*(12), 3002–3022. https://doi.org/10.1111/poms.12973

Chen, X., Hsu, V. N., Lai, G., & Li, Y. (2023). Supply chain short-term financing for responsible production at small and medium-sized enterprises. *Production and Operations Management*, *32*(12), 4154–4171. https://doi.org/10.1111/poms.14082

Chen, Y., & Özer, Ö. (2019). Supply chain contracts that prevent information leakage. *Management Science*, *65*(12), 5619–5650. https://doi.org/10.1287/mnsc.2018.3200

Chod, J. (2017). Inventory, risk shifting, and trade credit. *Management Science*, *63*(10), 3207–3225. https://doi.org/10.1287/mnsc.2016.2515

Chod, J., Lyandres, E., & Yang, S. A. (2019). Trade credit and supplier competition. *Journal of Financial Economics*, *131*(2), 484–505. https://doi.org/10.1016/j.jfineco.2018.08.008

Chod, J., Trichakis, N., & Tsoukalas, G. (2019). Supplier diversification under buyer risk. *Management Science*, *65*(7), 3150–3173. https://doi.org/10.1287/mnsc.2018.3095

Chod, J., Trichakis, N., Tsoukalas, G., Aspegren, H., & Weber, M. (2020). On the financing benefits of supply chain transparency and Blockchain adoption. *Management Science*, *66*(10), 4378–4396. https://doi.org/10.1287/mnsc.2019.3434

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*(5), 1754–1797. https://doi.org/10.1093/rfs/hhz007

Cong, L. W., Hui, X., Tucker, C., & Zhou, L. (2023). Scaling smart contracts via layer-2 technologies: Some empirical evidence. *Management Science*, *69*(12), 7306–7316. https://doi.org/10.1287/mnsc.2023.00281

Corbett, C. J., Zhou, D., & Tang, C. S. (2004). Designing supply contracts: Contract type and information asymmetry. *Management Science*, *50*(4), 550–559. https://doi.org/10.1287/mnsc.1030.0173

Cui, Y., Gaur, V., & Liu, J. (2024). Supply chain transparency and Blockchain design. *Management Science*, *70*(5), 3245–3263. https://doi.org/10.1287/mnsc.2023.4851

Cui, Y., Hu, M., & Liu, J. (2023). Value and design of traceability-driven blockchains. *Manufacturing & Service Operations Management*, *25*(3), 1099–1116. https://doi.org/10.1287/msom.2022.1161

Cuñat, V. (2007). Trade credit: Suppliers as debt collectors and insurance providers. *Review of Financial Studies*, *20*(2), 491–527. https://doi.org/10.1093/rfs/hhl015

de Chaisemartin, C., & D'Haultfœuille, X. (2020). Two-way fixed effects estimators with heterogeneous treatment effects. *American Economic Review*, *110*(9), 2964–2996. https://doi.org/10.1257/aer.20181169

Dennis, S. A., & Johnstone, K. M. (2018). A natural field experiment examining the joint role of audit partner leadership and subordinates' knowledge in fraud brainstorming. *Accounting, Organizations and Society*, *66*, 14–28. https://doi.org/10.1016/j.aos.2018.02.001

Devalkar, S. K., & Krishnan, H. (2019). The impact of working capital financing costs on the efficiency of trade credit. *Production and Operations Management*, *28*(4), 878–889. https://doi.org/10.1111/poms.12954

Dong, L., Qiu, Y., & Xu, F. (2023). Blockchain-enabled deep-tier supply chain finance. *Manufacturing & Service Operations Management*, *25*(6), 2021–2037. https://doi.org/10.1287/msom.2022.1123

Ersahin, N., Giannetti, M., & Huang, R. (2024). Trade credit and the stability of supply chains. *Journal of Financial Economics*, *155*, 103830. https://doi.org/10.1016/j.jfineco.2024.103830

Fama, E. F. (1980). Agency problems and the theory of the firm. *Journal of Political Economy*, *88*(2), 288–307. https://doi.org/10.1086/260866

Franke, B., Fritz, Q. G., & Stenzel, A. (2024). The (limited) power of Blockchain networks for information provision. *Management Science*, *70*(2), 971–990. https://doi.org/10.1287/mnsc.2023.4718

Fu, R., Aseri, M., Singh, P. V., & Srinivasan, K. (2022). "Un"fair machine learning algorithms. *Management Science*, *68*(6), 4173–4195. https://doi.org/10.1287/mnsc.2021.4065

Gao, Q., Lin, M., & Sias, R. (2023). Words matter: The role of readability, tone, and deception cues in online credit markets. *Journal of Financial and Quantitative Analysis*, *58*(1), 1–28. https://doi.org/10.1017/S0022109022000850

Gofman, M., & Wu, Y. (2022). Trade credit and profitability in production networks. *Journal of Financial Economics*, *143*(1), 593–618. https://doi.org/10.1016/j.jfineco.2021.05.054

Gopal, M., & Schnabl, P. (2022). The rise of finance companies and FinTech lenders in small business lending. *The Review of Financial Studies*, *35*(11), 4859–4901. https://doi.org/10.1093/rfs/hhac034

Gualandris, J., Longoni, A., Luzzini, D., & Pagell, M. (2021). The association between supply chain structure and transparency: A large-scale empirical study. *Journal of Operations Management*, *67*(7), 803–827. https://doi.org/10.1002/joom.1150

Guan, X., Liu, B., Chen, Y. J., & Wang, H. (2020). Inducing supply chain transparency through supplier encroachment. *Production and Operations Management*, *29*(3), 725–749. https://doi.org/10.1111/poms.13133

Gulati, R., & Nickerson, J. A. (2008). Interorganizational trust, governance choice, and exchange performance. *Organization Science*, *19*(5), 688–708. https://doi.org/10.1287/orsc.1070.0345

Ha, A. Y., Shang, W., & Wang, Y. (2023). Supplier audit information sharing and responsible sourcing. *Management Science*, *69*(1), 308–324. https://doi.org/10.1287/mnsc.2022.4358

Hamilton, E. L., & Smith, J. L. (2021). Error or fraud? The effect of omissions on management's fraud strategies and auditors' evaluations of identified misstatements. *The Accounting Review*, *96*(1), 225–249. https://doi.org/10.2308/tar-2017-0355

Hastig, G. M., & Sodhi, M. S. (2020). Blockchain for supply chain traceability: Business requirements and critical success factors. *Production and Operations Management*, *29*(4), 935–954. https://doi.org/10.1111/poms.13147

Huang, A. H., Kraft, P., & Wang, S. (2023). The usefulness of credit ratings for accounting fraud prediction. *The Accounting Review*, *98*(7), 347–376. https://doi.org/10.2308/tar-2021-0874

Huang, X. (2022). Financing disruptive suppliers: Payment advance, timeline, and discount rate. *Production and Operations Management*, *31*(3), 1115–1134. https://doi.org/10.1111/poms.13597

Iyengar, G., Saleh, F., Sethuraman, J., & Wang, W. (2024). Blockchain adoption in a supply chain with manufacturer market power. *Management Science*, *70*(9), 6158–6178. https://doi.org/10.1287/mnsc.2022.02505

Jacobs, B. W., & Singhal, V. R. (2017). The effect of the Rana Plaza disaster on shareholder wealth of retailers: Implications for sourcing strategies and supply chain governance. *Journal of Operations Management*, *49–51*, 52–66. https://doi.org/10.1016/j.jom.2017.01.002

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360. https://doi.org/10.1016/0304-405x(76)90026-x

Klapper, L., Laeven, L., & Rajan, R. (2012). Trade credit contracts. *Review of Financial Studies*, *25*(3), 838–867. https://doi.org/10.1093/rfs/hhr122

Kouvelis, P. (2023). OM Forum—Supply chain finance redefined: A supply chain-centric viewpoint of working capital, hedging, and risk management. *Manufacturing & Service Operations Management*, *25*(6), 2074–2084. https://doi.org/10.1287/msom.2022.0606

Kouvelis, P., & Xu, F. (2021). A supply chain theory of factoring and reverse factoring. *Management Science*, *67*(10), 6071–6088. https://doi.org/10.1287/mnsc.2020.3788

Kouvelis, P., & Zhao, W. (2012). Financing the newsvendor: Supplier vs. bank, and the structure of optimal trade credit contracts. *Operations Research*, *60*(3), 566–580. https://doi.org/10.1287/opre.1120.1040

Kouvelis, P., & Zhao, W. (2018). Who should finance the supply chain? Impact of credit ratings on supply chain decisions. *Manufacturing & Service Operations Management*, *20*(1), 19–35. https://doi.org/10.1287/msom.2017.0669

Lee, H. H., Zhou, J., & Wang, J. (2018). Trade credit financing under competition and its impact on firm performance in supply chains. *Manufacturing & Service Operations Management*, *20*(1), 36–52. https://doi.org/10.1287/msom.2017.0640

Li, C., Li, N., & Zhang, F. (2023). Using economic links between firms to detect accounting fraud. *The Accounting Review*, *98*(1), 399–421. https://doi.org/10.2308/tar-2021-0313

Li, L., & Zhang, H. (2008). Confidentiality and information sharing in supply chain coordination. *Management Science*, *54*(8), 1467–1481. https://doi.org/10.1287/mnsc.1070.0851

Li, T., Tong, S., & Zhang, H. (2014). Transparency of information acquisition in a supply chain. *Manufacturing & Service Operations Management*, *16*(3), 412–424. https://doi.org/10.1287/msom.2014.0478

Li, T., & Zhang, X. (2024). Development trajectory of Blockchain platforms: The role of multirole. *Information Systems Research*, *35*(3), 1296–1323. https://doi.org/10.1287/isre.2022.0243

Love, I., Preve, L. A., & Sarria-Allende, V. (2007). Trade credit and bank credit: Evidence from recent financial crises. *Journal of Financial Economics*, *83*(2), 453–469. https://doi.org/10.1016/j.jfineco.2005.11.002

Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain governance—A new way of organizing collaborations? *Organization Science*, *32*(2), 500–521. https://doi.org/10.1287/orsc.2020.1379

Murfin, J., & Njoroge, K. (2015). The implicit costs of trade credit borrowing by large firms. *Review of Financial Studies*, *28*(1), 112–145. https://doi.org/10.1093/rfs/hhu051

Ning, J. (2022). Strategic trade credit in a supply chain with buyer competition. *Manufacturing & Service Operations Management*, *24*(4), 2183–2201. https://doi.org/10.1287/msom.2022.1103

Norman, C. S., Rose, A. M., & Rose, J. M. (2010). Internal audit reporting lines, fraud risk decomposition, and assessments of fraud risk. *Accounting, Organizations and Society*, *35*(5), 546–557. https://doi.org/10.1016/j.aos.2009.12.003

Patterson, E. R., Smith, J. R., & Tiras, S. L. (2019). The effects of auditor tenure on fraud and its detection. *The Accounting Review*, *94*(5), 297–318. https://doi.org/10.2308/accr-52370

Petersen, M. A., & Rajan, R. G. (1997). Trade credit: Theories and evidence. *Review of Financial Studies*, *10*(3), 661–691. https://doi.org/10.1093/rfs/10.3.661

Pun, H., Swaminathan, J. M., & Hou, P. (2021). Blockchain adoption for combating deceptive counterfeits. *Production and Operations Management*, *30*(4), 864–882. https://doi.org/10.1111/poms.13348

Rambachan, A. (2024). Identifying prediction mistakes in observational data. *The Quarterly Journal of Economics*, *139*(3), 1665–1711. https://doi.org/10.1093/qje/qjae013

Reindorp, M., Tanrisever, F., & Lange, A. (2018). Purchase order financing: Credit, commitment, and supply chain consequences. *Operations Research*, *66*(5), 1287–1303. https://doi.org/10.1287/opre.2018.1727

Rui, H., & Lai, G. (2015). Sourcing with deferred payment and inspection under supplier product adulteration risk. *Production and Operations Management*, *24*(6), 934–946. https://doi.org/10.1111/poms.12313

Shen, B., Dong, C., & Minner, S. (2022). Combating copycats in the supply chain with permissioned Blockchain technology. *Production and Operations Management*, *31*(1), 138–154. https://doi.org/10.1111/poms.13456

Sodhi, M. S., Seyedghorban, Z., Tahernejad, H., & Samson, D. (2022). Why emerging supply chain technologies initially disappoint: Blockchain, IoT, and AI. *Production and Operations Management*, *31*(6), 2517–2537. https://doi.org/10.1111/poms.13694

Sodhi, M. S., & Tang, C. S. (2019). Research opportunities in supply chain transparency. *Production and Operations Management*, *28*(12), 2946–2959. https://doi.org/10.1111/poms.13115

Sternberg, H., Mathauer, M., & Hofmann, E. (2023). Technology management in multi-tier chains: A case study of agency in logistics service outsourcing. *Journal of Operations Management*, *69*(4), 536–557. https://doi.org/10.1002/joom.1219

Stikeleather, B. R. (2016). When do employers benefit from offering workers a financial reward for reporting internal misconduct? *Accounting, Organizations and Society*, *52*, 1–14. https://doi.org/10.1016/j.aos.2016.06.001

Trotman, K. T., & Wright, W. F. (2012). Triangulation of audit evidence in fraud risk assessments. *Accounting, Organizations and Society*, *37*(1), 41–53. https://doi.org/10.1016/j.aos.2011.11.003

Tunca, T. I., & Zhu, W. (2018). Buyer intermediation in supplier finance. *Management Science*, *64*(12), 5631–5650. https://doi.org/10.1287/mnsc.2017.2863

Van Vlasselaer, V., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2017). GOTCHA! Network-based fraud detection for social security fraud. *Management Science*, *63*(9), 3090–3110. https://doi.org/10.1287/mnsc.2016.2489

Wang, W., & Cai, G. (2024). Curtailing bank loan and loan insurance under risk regulations in supply chain finance. *Management Science*, *70*(4), 2682–2698. https://doi.org/10.1287/mnsc.2023.4827

Wang, X., & Xu, F. (2023). The value of smart contract in trade finance. *Manufacturing & Service Operations Management*, *25*(6), 2056–2073. https://doi.org/10.1287/msom.2022.1126

Whang, S. (2010). Timing of RFID adoption in a supply chain. *Management Science*, *56*(2), 343–355. https://doi.org/10.1287/mnsc.1090.1121

Wu, J., Zhang, Z., & Zhou, S. X. (2022). Credit rating prediction through supply chains: A machine learning approach. *Production and Operations Management*, *31*(4), 1613–1629. https://doi.org/10.1111/poms.13634

Wuttke, D. A., Rosenzweig, E. D., & Heese, H. S. (2019). An empirical analysis of supply chain finance adoption. *Journal of Operations Management*, *65*(3), 242–261. https://doi.org/10.1002/joom.1023

Yan, X., Chen, L., & Ding, X. (2024). Optimal cash management with payables finance. *Operations Research*, *72*(5), 1806–1826. https://doi.org/10.1287/opre.2022.0196

Yang, S. A., Bakshi, N., & Chen, C. J. (2021). Trade credit insurance: Operational value and contract choice. *Management Science*, *67*(2), 875–891. https://doi.org/10.1287/mnsc.2019.3571

Yang, S. A., & Birge, J. R. (2018). Trade credit, risk sharing, and inventory financing portfolios. *Management Science*, *64*(8), 3667–3689. https://doi.org/10.1287/mnsc.2017.2799

Zha, Y., Chen, K., Dong, L., & Yu, Y. (2024). Financing supplier through retailer's credit. *Production and Operations Management*, *33*(3), 721–736. https://doi.org/10.1177/10591478241231869

Zhang, N., & Xu, H. (2024). Fairness of ratemaking for catastrophe insurance: Lessons from machine learning. *Information Systems Research*, *35*(2), 469–488. https://doi.org/10.1287/isre.2022.1195

Zhou, W., Hu, Y., Lin, T., & Ding, Z. (2022). Trade credit and buyer financing. *Journal of Systems Science and Systems Engineering*, *31*(3), 288–312. https://doi.org/10.1007/s11518-022-5530-z

Zhou, W., Lin, T., & Cai, G. (2020). Guarantor financing in a four-party supply chain game with leadership influence. *Production and Operations Management*, *29*(9), 2035–2056. https://doi.org/10.1111/poms.13196