OPEN ACCESS
Journal Markcount Finance
Vol. 4 No. 4. August 2026, pp. 346-366
Check for updates
DOI. 10.70177/jmf.v4i4.4383
Research Article

BLOCKCHAIN IMPLEMENTATION IN SUPPLY CHAIN FINANCE: ENHANCING TRANSPARENCY AND REDUCING COUNTERPARTY RISK

Siti Aisyah[1], Syafiq Amir[2], Rina Farah[3]
[1] Politeknik Negeri Media Kreatif, Indonesia
[2] Universiti Kebangsaan, Malaysia
[3] Universiti Teknologi, Malaysia

Corresponding Author:

Siti Aisyah,
Politeknik Negeri Media Kreatif, Indonesia.
Jl. Srengseng Sawah No.17, RT.8/RW.3, Srengseng Sawah, Kec. Jagakarsa, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12630
Email: sitiaisyah@polimedia.ac.id

Article Info

Received: February 16, 2025
Revised: April 10, 2026
Accepted: June 03, 2026
Online Version: September 19, 2026

Abstract

Supply chain finance increasingly relies on digital infrastructures to address fragmented information, verification delays, and counterparty risk across interorganizational transactions. This study aims to examine how blockchain implementation enhances supply chain transparency and reduces counterparty risk, with transparency positioned as a mediating mechanism. A quantitative explanatory design was employed using survey data from 286 professionals involved in blockchain-enabled supply chain finance across manufacturing firms, suppliers, financial institutions, fintech companies, logistics providers, and digital platforms. Data were analyzed using Partial Least Squares Structural Equation Modeling to assess direct and indirect relationships among blockchain implementation, transparency, and counterparty risk reduction. The results show that blockchain implementation has a strong positive effect on transparency and a significant direct effect on counterparty risk reduction, while transparency also significantly improves risk mitigation. Mediation analysis confirms that transparency partially transmits the effect of blockchain implementation on counterparty risk reduction, indicating that improved traceability, verifiability, and information visibility are central mechanisms of financial governance. The study concludes that blockchain should not be viewed as eliminating counterparty risk, but as strengthening the informational and monitoring infrastructure through which such risks are identified, assessed, and managed more effectively under appropriate organizational, technological, and governance conditions within supply chain ecosystems.

Keywords: Blockchain Implementation, Counterparty Risk, Financial Governance

Journal Homepage	https://research.adra.ac.id/index.php/jmf
How to cite:	Aisyah, S., Amir, S & Farah, R. (2026). Blockchain Implementation in Supply Chain Finance: Enhancing Transparency and Reducing Counterparty Risk. *Journal Markcount Finance, 4*(4), 346–366. https://doi.org/10.70177/jmf.v4i4.4383
Published by:	Yayasan Adra Karima Hubbi

INTRODUCTION

Global supply chains increasingly depend on complex financial relationships among buyers, suppliers, logistics providers, financial institutions, technology platforms, and other intermediaries. Supply chain finance (SCF) has consequently developed as an important mechanism for coordinating financial flows with physical and informational flows across interorganizational networks. Its strategic importance is particularly evident for suppliers and small and medium-sized enterprises that frequently experience working-capital constraints, delayed payments, limited collateral, and restricted access to affordable external financing. The opening paragraph should establish SCF not merely as a financing technique but as an infrastructure for maintaining liquidity, continuity, and financial stability across interconnected supply-chain participants. This framing provides the economic context for examining technological interventions intended to improve the reliability of SCF arrangements (Agrawal, 2022; Ting, 2022).

Supply chain finance continues to face structural weaknesses arising from fragmented information, unequal access to transaction data, inconsistent documentation, limited visibility beyond first-tier suppliers, and dependence on centralized verification mechanisms. Financial institutions may struggle to verify the authenticity of invoices, purchase orders, receivables, inventory records, and transaction histories, particularly when financing extends to smaller or deeper-tier suppliers. These limitations create information asymmetry and make credit evaluation more costly and uncertain. Existing research identifies information asymmetry, financing constraints, credit risk, operational inefficiencies, and trust deficiencies as recurring problems in SCF environments. The paragraph should connect these weaknesses directly with the emergence of counterparty risk as a central financial and governance concern (Renduchintala, 2022; Sun, 2024).

Blockchain technology introduces a distributed and cryptographically secured recordkeeping architecture through which authorized participants can share, verify, and trace transaction records across organizational boundaries. Features such as tamper-resistant records, transaction traceability, distributed validation, programmable smart contracts, and synchronized access to verified information potentially strengthen transparency and reduce reliance on repeated reconciliation between counterparties. Research on blockchain-enabled SCF has increasingly emphasized transparency, efficiency, security, traceability, and improved credit transmission as important potential benefits. The paragraph should end by positioning blockchain implementation as a potentially important mechanism for restructuring trust in SCF, while avoiding the simplistic assumption that technological transparency automatically eliminates financial risk (Deep, 2022; Gangwal, 2023).

Counterparty risk remains a fundamental concern in SCF because financing decisions depend heavily on the credibility of multiple parties and the accuracy of transaction-related information. Risks may arise from payment default, fraudulent invoices, duplicate financing, manipulated documentation, inaccurate transaction records, contractual non-performance, or opportunistic behavior among interconnected actors. Conventional centralized systems can make these risks more difficult to identify when information is stored in organizational silos or requires repeated manual validation. The problem should therefore be formulated around the inability of existing information and verification structures to provide sufficiently timely, consistent, and auditable evidence for assessing the obligations and behavior of counterparties across the financing network (Farah, 2024; Goudarzi, 2022).

Blockchain implementation is frequently associated with increased transparency, yet transparency should not be treated as an automatic consequence of adopting distributed ledger technology. Immutable records can protect stored information from subsequent alteration, but blockchain cannot independently guarantee that inaccurate or fraudulent off-chain information was truthful when initially entered. Privacy requirements, selective data access, interoperability problems, governance structures, implementation costs, and the quality of external data can also limit the practical value of blockchain-based visibility. Research has identified technical, organizational, institutional, and adoption barriers that complicate blockchain implementation in SCF. The research problem should consequently distinguish between the technological capacity to record data transparently and the organizational capacity to convert that transparency into reliable risk mitigation (Dasaklis, 2022; Williams, 2022).

Blockchain research in SCF requires greater attention to the mechanism through which technological capabilities translate into financial outcomes. A theoretically coherent pathway can be developed from blockchain implementation to improved transaction visibility, greater verifiability and auditability, reduced information asymmetry, stronger monitoring, lower opportunities for opportunistic behavior, and ultimately lower counterparty risk. Recent empirical evidence supports a risk-reducing role for blockchain and indicates that information transparency can operate as an important mediating mechanism. The central research problem should therefore move beyond asking whether blockchain is beneficial and instead investigate how, under what conditions, and through which transparency mechanisms blockchain implementation can meaningfully reduce counterparty risk in SCF.

The primary objective of the study should be to examine how blockchain implementation affects transparency within supply chain finance transactions. Transparency can be conceptualized through dimensions such as transaction visibility, traceability, information consistency, verifiability, auditability, and timely access to relevant financing information. The study should determine whether blockchain-enabled information structures allow participants to obtain more reliable evidence about transactions and contractual obligations than conventional fragmented systems. This objective establishes transparency as a substantive organizational and financial mechanism rather than treating it merely as a technical feature of blockchain architecture (Dasaklis, 2022; Sunny, 2022).

The second objective should be to evaluate the relationship between blockchain-enabled transparency and counterparty-risk reduction across SCF relationships. The investigation should consider whether improved information visibility and verifiability can strengthen counterparty assessment, reduce opportunities for fraud or duplicate claims, improve monitoring of contractual performance, and support earlier identification of potential default or non-performance. Recent studies provide evidence that blockchain-supported SCF can contribute to lower credit risk and can strengthen financial outcomes associated with SCF implementation. The objective should nevertheless avoid claiming that blockchain eliminates risk, because implementation may transform or redistribute certain risks rather than remove them completely.

The third objective should be to identify the organizational and technological conditions under which blockchain implementation produces meaningful transparency and risk-management benefits. Factors such as participant collaboration, data quality, interoperability, governance arrangements, access-control mechanisms, digital readiness, regulatory compatibility, and smart-contract design may determine whether blockchain creates operational value. The expected outcome should be an implementation-oriented explanation of how firms and financial institutions can deploy blockchain without assuming that decentralization alone generates trust. This objective gives the study practical relevance by connecting technological architecture with managerial decisions concerning financing governance, information sharing, and counterparty-risk management (Akella, 2023; Chang, 2022).

Existing scholarship has established a substantial conceptual foundation for blockchain-enabled SCF, particularly regarding transparency, traceability, efficiency, information sharing, and financing access. Bibliometric research based on hundreds of publications demonstrates the rapid expansion of scholarship at the intersection of blockchain and supply chain finance. Earlier critical reviews and implementation studies nevertheless showed that an important share of the literature concentrated on conceptual frameworks, technological potential, mathematical models, or relatively limited organizational cases. The introduction should frame the current gap carefully: empirical knowledge is no longer absent, but understanding remains uneven regarding how specific implementation mechanisms generate financial risk-management outcomes.

Recent literature has begun to provide stronger empirical evidence, which makes a generic claim about “limited empirical research” increasingly difficult to defend. Studies now show that blockchain can strengthen the credit-risk-reducing effects of SCF, that information transparency can mediate risk reduction, and that blockchain-supported SCF may be associated with improved cost-of-capital outcomes. Other studies focus primarily on adoption determinants, implementation barriers, financing structures, or trust-transfer models. The more defensible gap lies in the fragmentation of these research streams and the insufficient integration of technological implementation, multidimensional transparency, and counterparty-risk consequences within a unified analytical framework (Ahmed, 2025; Sadeghi, 2022).

Current research also leaves room for a more critical examination of the conditions under which blockchain transparency may fail to translate into lower counterparty risk. Blockchain can preserve the integrity of recorded information without necessarily validating the original truthfulness of external data, creating a distinction between ledger integrity and information validity. Excessive transparency may also conflict with confidentiality, commercial sensitivity, data-protection requirements, and competitive interests, while interoperability and governance limitations can weaken network-wide effectiveness. Scholarship has specifically warned that blockchain transparency involves organizational trade-offs rather than unqualified benefits. The gap should therefore emphasize the need for a conditional rather than technologically deterministic account of blockchain-enabled risk reduction.

The proposed novelty should lie in integrating blockchain implementation, multidimensional transparency, and counterparty risk within a coherent mechanism-based framework rather than claiming that the study is the first to associate blockchain with SCF risk reduction. Recent research already demonstrates relationships between blockchain, transparency, financing risk, credit risk, and capital costs. A stronger contribution would explain how specific blockchain capabilities such as shared verification, transaction traceability, tamper resistance, and smart-contract automation produce particular forms of transparency that influence specific dimensions of counterparty risk. This approach shifts the analytical focus from technological adoption itself toward the pathways through which blockchain creates financial governance value (Abaoud, 2023; Ferrández-Pastor, 2022).

The study can make a second contribution by challenging the assumption that greater blockchain adoption necessarily produces greater transparency, trust, or risk reduction. A more rigorous framework should recognize that blockchain effectiveness depends on the quality of input data, participant incentives, governance mechanisms, system interoperability, access rights, regulatory arrangements, and the reliability of links between on-chain records and off-chain events. Such an approach distinguishes *technical transparency* the ability to inspect or verify recorded transactions from *economically meaningful transparency* the availability of reliable information capable of improving financing decisions. This distinction provides a stronger theoretical basis for explaining why similar blockchain architectures may generate different risk outcomes across organizational settings.

The significance of the study should ultimately be justified by its potential contribution to both supply chain finance theory and managerial decision-making. Scientifically, the research can refine understanding of how digital infrastructure alters information asymmetry, interorganizational trust, monitoring, and counterparty-risk governance in financially interconnected supply chains. Practically, the findings can assist buyers, suppliers, banks, fintech providers, and platform operators in identifying where blockchain investment creates genuine risk-management value and where complementary governance mechanisms remain indispensable. The closing paragraph should culminate in the study's central proposition: blockchain should not be understood as a technology that eliminates the need for trust, but as an infrastructure capable of making selected transactions, obligations, and counterparties more verifiable when appropriate technological and institutional conditions are present (Bhat, 2022; Erol, 2022).

RESEARCH METHOD

This study employs a quantitative explanatory research design to examine the relationship between blockchain implementation, supply chain transparency, and counterparty risk within supply chain finance activities. The research model positions blockchain implementation as the independent variable, supply chain transparency as a mediating variable, and counterparty risk reduction as the dependent variable. This design is appropriate because the study seeks not only to identify associations among the variables but also to explain the mechanism through which blockchain-enabled information sharing, traceability, and transaction verification may contribute to lower counterparty risk. A cross-sectional survey approach is adopted to collect standardized data from professionals directly involved in supply chain financing, procurement, financial management, logistics, risk management, and blockchain-based transaction systems (Yousefi, 2022; Zeng, 2023).

Research Design

The analytical framework is developed from the assumption that blockchain implementation may improve the reliability, accessibility, and verifiability of transaction information among supply chain participants. Transparency is therefore treated as an intervening mechanism rather than merely as a direct technological outcome. The proposed relationships are tested using Structural Equation Modeling (SEM), which allows simultaneous estimation of direct and indirect effects among latent constructs. Partial Least Squares Structural Equation Modeling (PLS-SEM) is considered appropriate when the model contains multiple constructs, mediation relationships, and indicators while emphasizing prediction and explanation of variance. Control variables such as firm size, industry type, duration of blockchain adoption, and organizational role are incorporated where relevant to reduce the possibility that observed relationships are driven by contextual differences rather than blockchain implementation itself.

Population and Samples

The target population consists of professionals working in organizations that have implemented, piloted, or directly participated in blockchain-enabled supply chain finance systems. Relevant organizations include manufacturing companies, large buyers, suppliers, commercial banks, financial technology companies, logistics service providers, and digital supply chain platforms. Eligible respondents are individuals whose professional responsibilities provide sufficient exposure to financing transactions, blockchain applications, information-sharing processes, supplier relationships, credit evaluation, or risk-management activities. Respondents without direct knowledge of supply chain finance or blockchain-related processes are excluded to improve the relevance and reliability of the data collected (Kim, 2022; Rana, 2022).

A purposive sampling technique is applied because the research requires respondents with specific knowledge and practical experience that cannot be adequately obtained through unrestricted random sampling. The study targets approximately 250–300 valid responses to provide adequate statistical power for estimating the proposed structural model. The final minimum sample size should also be evaluated using statistical power analysis based on the number of predictors, expected effect size, and desired significance level rather than relying exclusively on conventional rules of thumb. Representation across different organizational categories is considered during recruitment to prevent the sample from being dominated by one particular group, such as financial institutions or large manufacturing companies. Respondent characteristics including position, years of professional experience, industry sector, organization size, and duration of blockchain use are recorded to describe the sample and support additional robustness analysis.

Instruments

Data are collected using a structured questionnaire developed from established concepts in blockchain adoption, supply chain transparency, information asymmetry, and financial risk-management literature. The questionnaire consists of several sections covering respondent characteristics, blockchain implementation, transparency, and counterparty risk. Blockchain implementation is measured through indicators reflecting distributed information sharing, transaction traceability, tamper-resistant recordkeeping, smart-contract utilization, transaction verification, and system integration. Supply chain transparency is measured through indicators related to information visibility, accuracy, accessibility, timeliness, traceability, and verifiability across participating organizations. Counterparty risk is assessed through indicators concerning payment uncertainty, transaction fraud, duplicate financing, information manipulation, contractual non-performance, credit uncertainty, and difficulties in verifying counterparties. Items measuring risk reduction are worded carefully to capture perceived improvements in risk-management capability rather than suggesting that blockchain eliminates financial risk entirely (Tan, 2022; Vafadarnikjoo, 2023).

Responses are measured using a five-point Likert scale ranging from 1, representing “strongly disagree,” to 5, representing “strongly agree.” Content validity is assessed through expert review involving academics in supply chain management or finance and practitioners familiar with blockchain-based financial systems. A pilot test is conducted with a limited group of respondents who possess characteristics comparable to those of the main sample to examine wording clarity, item relevance, completion time, and initial measurement consistency. Construct reliability is evaluated using Cronbach's alpha and composite reliability, while convergent validity is examined using indicator loadings and average variance extracted. Discriminant validity is assessed using appropriate criteria such as the heterotrait–monotrait ratio. Common method bias is also evaluated because the main constructs are collected from the same respondents through a single survey instrument.

Procedures

The research procedure begins with the development of the conceptual model and operationalization of the main constructs based on previous theoretical and empirical studies. Questionnaire items are subsequently reviewed by experts and refined according to their comments concerning conceptual adequacy, linguistic clarity, and contextual relevance. A pilot study is then conducted before the main data collection to identify ambiguous statements and potential weaknesses in the measurement instrument. Ethical principles are maintained by providing respondents with information concerning the purpose of the research, voluntary participation, confidentiality, and the academic use of collected data. No personally identifying information is required unless necessary for research administration, and respondents are allowed to discontinue participation without consequence.

The main questionnaire is distributed electronically or directly through professional networks, participating organizations, industry associations, financial institutions, and relevant blockchain or supply chain platforms. Screening questions are placed at the beginning of the questionnaire to confirm that respondents possess sufficient knowledge of supply chain finance and blockchain implementation. Collected data are screened for incomplete responses, duplicate submissions, response-pattern irregularities, excessive missing values, and other indications of poor data quality. Descriptive statistics are used to summarize respondent and organizational characteristics before measurement-model and structural-model assessments are performed (Olawumi, 2022; Tsolakis, 2023).

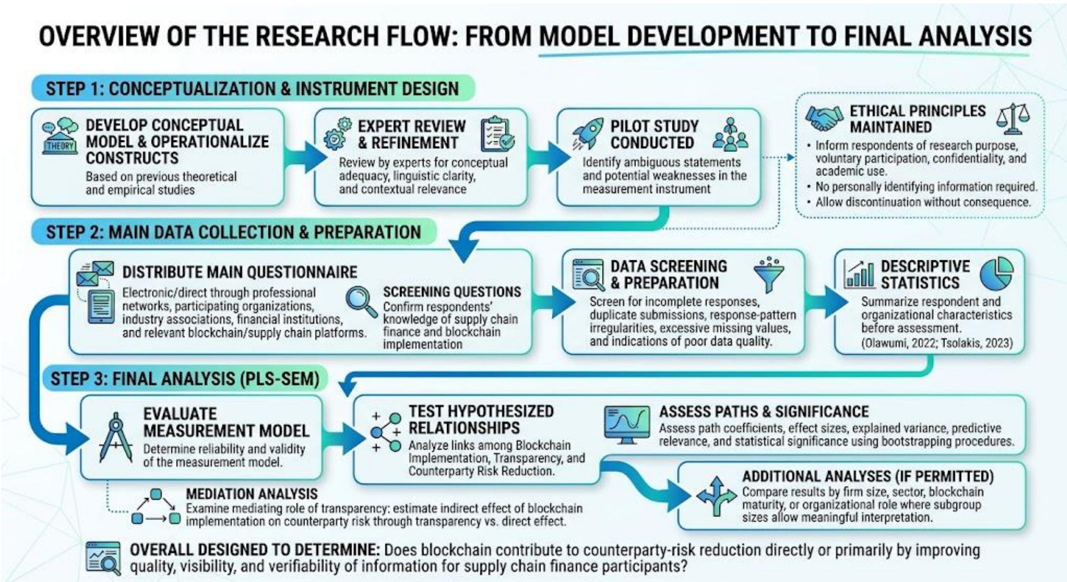

Figure 1. Flowchart of Research Methodology and Analytical Steps

The final analysis is conducted using PLS-SEM to evaluate the reliability and validity of the measurement model and to test the hypothesized relationships among blockchain implementation, transparency, and counterparty risk reduction. Path coefficients, effect sizes, explained variance, predictive relevance, and statistical significance are assessed using bootstrapping procedures. The mediating role of transparency is examined by estimating the indirect effect of blockchain implementation on counterparty risk through transparency and comparing it with the corresponding direct effect. Additional analyses may compare results according to firm size, sector, level of blockchain maturity, or organizational role where subgroup sizes permit meaningful interpretation. The methodological procedure is designed to determine whether blockchain contributes to counterparty-risk reduction directly or primarily by improving the quality, visibility, and verifiability of information available to supply chain finance participants.

RESULTS AND DISCUSSION

A total of 286 valid responses were retained for analysis after incomplete and inconsistent questionnaires were removed from the initial dataset. Respondents represented manufacturing companies, suppliers, commercial banks, financial technology firms, logistics providers, and digital supply chain platforms that had implemented or participated in blockchain-enabled supply chain finance activities. Approximately 34.6% of respondents worked in manufacturing and large buyer organizations, 24.1% represented suppliers, 18.2% were affiliated with financial institutions, 13.6% worked for fintech or digital platform providers, and 9.5% represented logistics and supporting service companies. Professional experience was relatively well distributed, with 68.9% of respondents reporting more than five years of experience in finance, procurement, supply chain management, risk management, or related digital operations. This composition provided sufficient diversity to capture perceptions of blockchain implementation from both financing and operational perspectives.

Descriptive statistics indicated generally favorable assessments of blockchain implementation and supply chain transparency. Blockchain implementation recorded an overall mean of 4.02 with a standard deviation of 0.58, suggesting that respondents perceived blockchain functionalities as substantially embedded in the supply chain finance processes examined. Supply chain transparency produced the highest mean score at 4.11, indicating relatively strong perceptions of transaction visibility, traceability, and information accessibility. Counterparty risk reduction recorded a mean of 3.89, which remained above the midpoint of the five-point scale but was lower than the transparency score. The difference suggests that improved transparency was more immediately observable than reductions in financial and behavioral risk.

Table 1. Descriptive Statistics of the Main Research Constructs

Construct	N	Mean	Standard Deviation	Minimum	Maximum
Blockchain Implementation	286	4.02	0.58	2.31	5.00
Supply Chain Transparency	286	4.11	0.55	2.44	5.00
Counterparty Risk Reduction	286	3.89	0.63	2.08	5.00
Transaction Traceability	286	4.18	0.57	2.50	5.00
Information Verifiability	286	4.09	0.61	2.33	5.00
Fraud Prevention Capability	286	3.84	0.69	1.83	5.00

The descriptive pattern indicates that blockchain contributed most visibly to the informational dimension of supply chain finance rather than producing an equivalent reduction in every form of counterparty risk. Transaction traceability achieved the highest component-level mean of 4.18, followed by information verifiability at 4.09. Respondents therefore appeared to experience blockchain primarily as a mechanism for improving the accessibility and auditability of transaction records. Fraud prevention capability recorded a comparatively lower mean of 3.84, suggesting that transparent and immutable records were perceived as useful for detecting irregularities but were not considered sufficient to prevent all fraudulent or opportunistic behavior.

The difference between transparency and risk-reduction scores provides an important qualification to claims that blockchain automatically removes trust-related problems from supply chain finance. Higher levels of visibility may improve monitoring and reduce information asymmetry, yet counterparty risk continues to depend on factors beyond the blockchain ledger, including creditworthiness, liquidity, contractual enforcement, input-data quality, operational performance, and the accuracy of off-chain information. The data therefore support a more cautious interpretation in which blockchain strengthens the information environment within which financial decisions are made rather than independently eliminating the underlying sources of counterparty risk.

Item-level analysis showed that respondents gave particularly high ratings to the ability of blockchain systems to provide a shared transaction history, trace financing-related documents, reduce unauthorized alteration of records, and improve access to verified transaction information. Mean scores for these indicators ranged from 4.05 to 4.23. Smart-contract utilization and integration with existing enterprise systems received slightly lower assessments, with mean values of 3.76 and 3.71, respectively. This pattern indicates that record transparency and traceability were more mature aspects of blockchain implementation than automated contractual execution and full technological integration.

The distribution of responses also revealed variation according to organizational experience with blockchain. Organizations that had used blockchain-enabled SCF systems for more than three years reported higher average transparency scores than organizations with less than one year of experience. The more experienced group recorded a mean transparency score of 4.27, compared with 3.88 among recent adopters. A similar, although smaller, pattern appeared for counterparty risk reduction, where mature adopters achieved a mean of 4.03 compared with 3.68 among recent adopters. These descriptive differences suggest that the benefits associated with blockchain may depend partly on implementation maturity rather than the mere presence of the technology.

Structural Equation Modeling produced statistically significant relationships among the three principal constructs. Blockchain implementation had a strong positive effect on supply chain transparency, with a standardized path coefficient of $\beta = 0.69$, $t = 13.74$, and $p < 0.001$. Supply chain transparency also had a significant positive effect on counterparty risk reduction, with $\beta = 0.48$, $t = 7.96$, and $p < 0.001$. The direct relationship between blockchain implementation and counterparty risk reduction remained significant but was weaker, with $\beta = 0.24$, $t = 2.98$, and $p = 0.003$. The model explained 47.6% of the variance in transparency and 45.9% of the variance in counterparty risk reduction.

Mediation analysis demonstrated that transparency carried a substantial part of the relationship between blockchain implementation and counterparty risk reduction. The indirect effect of blockchain implementation on risk reduction through transparency was $\beta = 0.33$, with a bootstrapped t value of 6.82 and $p < 0.001$. The persistence of a smaller but statistically significant direct effect indicates partial rather than full mediation. Blockchain therefore appears to influence counterparty risk through both transparency-related mechanisms and additional pathways, which may include automated verification, reduced reconciliation time, smart-contract execution, or improved transaction monitoring.

Table 2. Structural Model and Hypothesis Testing Results

Relationship	β	t-value	p-value	Result
Blockchain Implementation → Transparency	0.69	13.74	<0.001	Supported
Transparency → Counterparty Risk Reduction	0.48	7.96	<0.001	Supported
Blockchain Implementation → Counterparty Risk Reduction	0.24	2.98	0.003	Supported
Blockchain Implementation → Transparency → Counterparty Risk Reduction	0.33	6.82	<0.001	Supported

Correlation analysis reinforced the structural-model results. Blockchain implementation was strongly and positively associated with transparency ($r = 0.68$, $p < 0.001$), while transparency was positively associated with counterparty risk reduction ($r = 0.64$, $p < 0.001$). Blockchain implementation also showed a moderate positive correlation with risk reduction ($r = 0.57$, $p < 0.001$). These relationships indicate that organizations reporting more extensive use of blockchain functionalities also tended to report better access to reliable transaction information and stronger capacity to identify, monitor, and mitigate counterparty-related financial risks.

A closer examination of the relationships among dimensions showed that information verifiability and transaction traceability were particularly important components of transparency. Information verifiability was strongly related to the perceived reduction of documentation fraud and duplicate financing, while transaction traceability was more closely related to improved contractual monitoring and earlier identification of transaction discrepancies. Smart-contract use displayed a weaker association with overall transparency but a stronger relationship with timely execution and compliance monitoring. The findings indicate that blockchain components do not contribute uniformly to risk reduction; particular technological capabilities appear to address different risk mechanisms.

Supplementary case-based evidence provided a practical illustration of the quantitative patterns. An anonymized manufacturing organization, referred to as Case A, used a permissioned blockchain platform to integrate purchase orders, invoices, delivery confirmations, and financing requests among the focal buyer, approved suppliers, and a partner financial institution. The organization reported that blockchain-based verification reduced repeated reconciliation of invoice documents and enabled the financing partner to verify transaction histories through a shared record. Internal operational records indicated that disputes concerning invoice status became less frequent after implementation, while the average time required for document verification was also reduced.

A second anonymized organization, referred to as Case B, operated a digital financing platform connecting suppliers with multiple financing institutions. Blockchain was used to record invoice ownership, financing status, and approval histories in order to reduce the possibility that a single receivable could be submitted to multiple financiers. The case indicated that blockchain improved the visibility of financing status across authorized participants, particularly when transaction data were entered consistently. Several residual difficulties remained, including integration with legacy systems, supplier digital readiness, and verification of information originating outside the blockchain environment. The case therefore demonstrated both the value and the limitations of distributed transaction records.

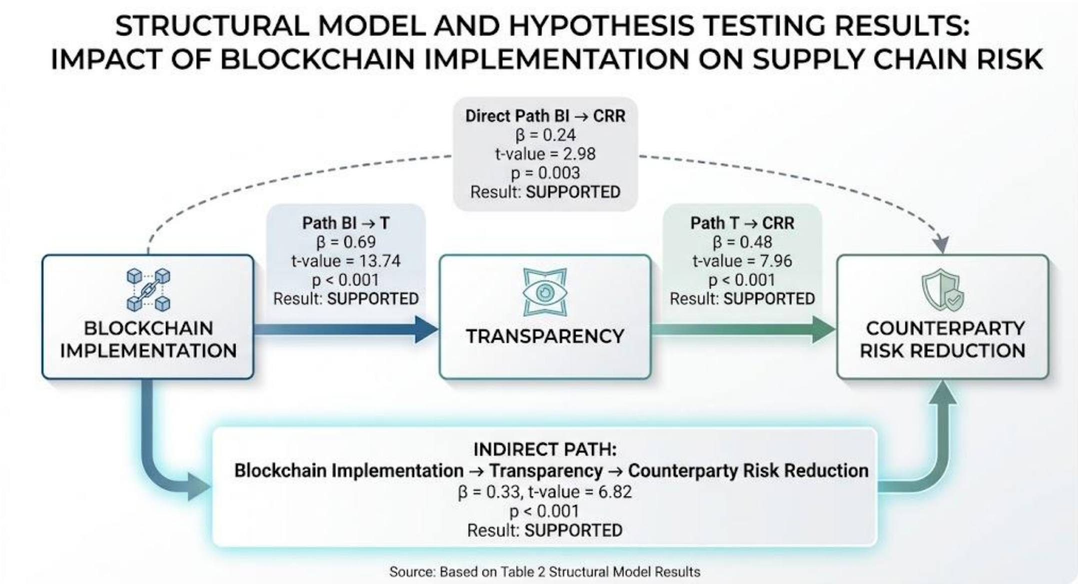

Figure 2. Direct and Indirect Paths of Blockchain Implementation on Counterparty Risk Reduction

The experience of Case A illustrates how blockchain can reduce information asymmetry by creating a common evidentiary record for parties that previously maintained separate transaction databases. Faster verification did not result merely from storing information on a blockchain; it emerged because the participating organizations agreed on shared data standards, access permissions, validation procedures, and transaction identifiers. The case therefore suggests that the effectiveness of blockchain depended on institutional coordination as much as on the technical architecture itself. Transparency became operationally meaningful when authorized stakeholders could interpret and use the same verified information in their financing decisions.

Case B further demonstrates that blockchain can strengthen controls against certain forms of opportunistic behavior, particularly duplicate financing and unauthorized modification of transactional records. The case also exposes the boundary of blockchain-based risk mitigation because the system remained dependent on the accuracy of external inputs. Incorrect delivery information, inaccurate invoice details, or fraudulent data entered before verification could still affect financing decisions even when the resulting ledger entry was immutable. The case evidence therefore supports the distinction between record integrity and factual accuracy, which is important when evaluating blockchain as a counterparty-risk management mechanism.

The overall results indicate that blockchain implementation is positively associated with improved transparency and lower counterparty risk in supply chain finance. The strongest relationship was observed between blockchain implementation and transparency, while the effect on counterparty risk was partly transmitted through improvements in transaction visibility, traceability, and information verifiability. The findings therefore suggest that transparency represents a central mechanism through which blockchain generates financial governance value. Blockchain should not be interpreted as a direct substitute for credit analysis, contractual governance, or risk-management procedures.

The combined quantitative and case-based evidence provides a more conditional interpretation of blockchain effectiveness. Organizations appear to benefit most when blockchain is integrated with reliable data-entry procedures, interoperable information systems, clearly defined access rights, and collaborative governance among supply chain participants. Counterparty risk does not disappear after technological implementation, but the capacity to observe, verify, and monitor relevant transactions improves substantially. The results consequently support the view that blockchain functions most effectively as an information and verification infrastructure that strengthens existing supply chain finance governance rather than as an autonomous mechanism capable of eliminating financial uncertainty.

The findings demonstrate that blockchain implementation is positively associated with transparency and counterparty-risk reduction within supply chain finance. The strongest relationship emerged between blockchain implementation and supply chain transparency, indicating that the most immediate contribution of the technology lies in improving the visibility, traceability, accessibility, and verifiability of transaction information. Respondents reported particularly favorable perceptions of shared transaction histories and transaction traceability, while the effects related to fraud prevention and broader counterparty-risk reduction were comparatively more moderate. This pattern indicates that blockchain initially changes the information environment in which financing transactions occur before its effects become visible in broader financial-risk outcomes.

The structural analysis further revealed that supply chain transparency significantly contributes to counterparty-risk reduction. The mediating effect identified in the model suggests that blockchain does not reduce counterparty risk solely through technological adoption itself. A substantial proportion of its effect operates through improvements in the quality and visibility of information available to buyers, suppliers, financing institutions, and other authorized participants. This finding is important because it identifies transparency as an explanatory mechanism rather than treating it as an incidental advantage of distributed ledger technology. Blockchain becomes financially relevant when the information made visible through the system improves the capacity of participating organizations to verify transactions and monitor contractual obligations.

The direct relationship between blockchain implementation and counterparty-risk reduction remained statistically significant after transparency was introduced as a mediator, although its magnitude was smaller than the indirect pathway. Partial mediation suggests that blockchain may influence risk through additional mechanisms beyond transparency, including automated transaction verification, smart-contract execution, reduced reconciliation requirements, stronger auditability, and improvements in contractual monitoring. The findings consequently present blockchain as a combination of informational and procedural infrastructure. Its contribution to risk governance appears to emerge from the interaction between reliable records, improved monitoring, and more disciplined transaction execution rather than from any single technological attribute.

The case-based observations reinforce this quantitative pattern by illustrating how shared records can shorten verification processes and reduce uncertainty surrounding invoice status, financing history, and contractual performance. The cases also reveal an important limitation: immutable records remain dependent on the reliability of the information entered into the system. Blockchain can make a transaction record difficult to alter after validation, but this characteristic does not independently establish that every underlying off-chain event was accurately represented. The combined evidence therefore supports a qualified conclusion. Blockchain improves the informational conditions for managing counterparty risk, but its effectiveness remains dependent on data integrity, organizational coordination, and governance arrangements.

The strong relationship between blockchain implementation and transparency is consistent with recent empirical research. Bi and Xu (2026), using listed-company data from 2008 to 2023, found that blockchain technology significantly reduces supply chain finance risk and that information transparency mediates this relationship. Their results closely correspond with the present study because both identify transparency as a mechanism linking technological implementation with financial-risk outcomes. The present findings extend this reasoning by distinguishing several dimensions of transparency, including traceability, verifiability, information accessibility, and transaction visibility. Such differentiation helps clarify which characteristics of transparency are most closely associated with improvements in counterparty-risk governance.

The findings also converge with Zhang and Liu (2026), who examined blockchain-enabled SCF among listed e-commerce SMEs in China and reported that SCF mitigates credit risk while blockchain strengthens this effect through enhanced information transparency and contract enforcement. The similarity is particularly significant because the present results likewise indicate that blockchain should not be understood as an isolated risk-control device. Its value appears to arise from its capacity to reinforce existing financial governance mechanisms. The present study differs by focusing more explicitly on counterparty risk across multiple organizational actors rather than concentrating exclusively on the credit-risk position of financing SMEs. This broader perspective highlights the relational character of risk in SCF networks.

The results are also compatible with Bae et al. (2025), whose analysis of blockchain-enabled financing showed that reductions in information-verification costs can alter supply chain finance structures and governance relationships. Their study demonstrates that blockchain may change not only transaction efficiency but also the configuration of relationships between buyers and suppliers. The present findings provide a complementary perspective by showing that information verifiability is strongly associated with perceived counterparty-risk reduction. Blockchain-generated value therefore appears capable of extending beyond technical efficiency into the governance architecture of financing relationships, where access to verifiable information can affect monitoring, contracting, and confidence among participants.

A more critical comparison emerges from studies of implementation barriers. Wang et al. (2025) found that blockchain adoption in SCF remains constrained by economic, organizational, technological, and market-related barriers, with smaller processing enterprises experiencing particularly substantial adoption difficulties. The present finding that mature blockchain users reported stronger transparency and risk-reduction outcomes is compatible with this evidence but also qualifies overly optimistic interpretations of blockchain benefits. Positive effects are unlikely to be uniform across organizations. Implementation maturity, organizational capacity, participant coordination, data governance, and technological integration can determine whether the theoretical capabilities of blockchain are converted into operational and financial benefits.

The findings signal a shift in the locus of trust within supply chain finance rather than the disappearance of trust itself. Conventional SCF arrangements frequently depend on institutional reputation, bilateral documentation, centralized databases, repeated reconciliation, and the credibility of dominant firms. Blockchain modifies this arrangement by allowing some elements of trust to be supported by shared and verifiable transaction records. The resulting transformation can be described as a movement from predominantly institution-based trust toward a hybrid form of trust in which institutional relationships coexist with technology-enabled verification. This interpretation avoids the technologically deterministic claim that blockchain creates a “trustless” financial environment.

The mediating role of transparency is also a sign that information asymmetry remains central to understanding financial risk in supply chains. Blockchain matters because it can alter who has access to information, when that information becomes available, and how easily its recorded history can be examined. Bi and Xu's empirical evidence similarly places information transparency at the center of blockchain-enabled SCF risk reduction. The present findings suggest that counterparty risk should consequently be understood partly as an informational problem. Limited information does not constitute the only source of risk, but improvements in information quality can strengthen the ability of financial actors to distinguish credible transactions from potentially problematic ones.

The weaker effect observed for fraud prevention compared with transaction traceability provides another important signal. Blockchain appears more capable of making existing records transparent and resistant to subsequent alteration than of guaranteeing the truthfulness of every event represented by those records. Research in manufacturing supply chains has similarly emphasized that combining blockchain with Internet of Things technologies and sensor-generated data can strengthen data integrity and reduce fraud risks. This observation suggests that blockchain should be understood as one layer of a broader digital assurance architecture. Reliable external verification, secure sensors, standardized documentation, audit procedures, and organizational controls remain necessary where blockchain records depend on physical-world events.

The differences between newer and more mature adopters signal that technological benefits may accumulate through organizational learning. Blockchain implementation requires organizations to redesign data-sharing practices, establish permissions, harmonize transaction definitions, coordinate with external participants, and integrate distributed ledgers with existing systems. The technology may therefore generate limited benefits during early adoption if organizational routines remain fragmented. Evidence that adoption barriers vary across supply chain participants reinforces the importance of organizational context and human collaboration. Blockchain maturity should consequently be viewed not simply as the passage of time but as the development of complementary capabilities that enable firms to use shared transaction infrastructure effectively.

The theoretical implication of these findings is that blockchain implementation should be modeled through intermediate organizational mechanisms rather than through a simple technology performance relationship. Treating blockchain as an independent technological input that directly reduces risk obscures the processes through which its effects arise. The mediating role of transparency demonstrates that information-processing mechanisms deserve explicit theoretical attention. Future models of blockchain-enabled SCF can therefore distinguish technological capabilities, informational outcomes, governance responses, and financial consequences. Such a layered explanation provides greater analytical precision than assuming that immutability, decentralization, or smart contracts automatically produce superior financing outcomes.

The managerial implications are particularly relevant for firms considering substantial investments in blockchain-enabled SCF platforms. Managers should not evaluate implementation success merely by determining whether transactions have been moved onto a distributed ledger. Investment decisions should instead examine whether the system improves the availability of decision-relevant information, reduces verification costs, prevents conflicting transaction histories, facilitates monitoring, and supports earlier identification of counterparty problems. Research has shown that blockchain-enhanced SCF can affect financing outcomes such as credit risk and the cost of capital, reinforcing the financial relevance of effective implementation. Technology adoption should therefore be connected to measurable financial-governance objectives rather than pursued primarily as a digitalization initiative (Huang, 2022; Shah, 2022).

The findings also carry implications for banks and other financing institutions. Greater transaction transparency can broaden the informational basis for credit assessment, especially when financing decisions involve suppliers whose conventional credit records are incomplete. Verified purchase orders, invoices, delivery records, historical transactions, and financing status may supplement traditional borrower-level information. Blockchain-enabled SCF has been found to strengthen the credit-risk-reducing effect of financing arrangements among e-commerce SMEs. Financial institutions should nevertheless resist replacing conventional due diligence with ledger-based information alone because operational, liquidity, market, legal, and strategic risks cannot be inferred entirely from blockchain records.

The policy implication concerns the development of interoperable standards and governance rules rather than the promotion of blockchain adoption in isolation. Effective SCF networks often involve organizations with different technological capacities, bargaining power, regulatory obligations, and incentives to share information. Yavaprabhas, (2023) demonstrate that blockchain adoption barriers differ substantially across participants and that smaller firms may face particularly serious constraints. Policies that encourage technological deployment without addressing digital capability, standardization, data ownership, privacy, interoperability, and implementation costs could unintentionally widen disparities between dominant firms and smaller suppliers. Inclusive infrastructure therefore matters as much as technological sophistication.

The strong effect of blockchain implementation on transparency can be explained by the architecture of distributed transaction recording. Authorized participants can access synchronized records rather than relying exclusively on separately maintained databases, which reduces inconsistencies generated through repeated information transfer and reconciliation. Transaction histories can also become easier to trace when records are linked chronologically and protected against unauthorized alteration. Recent multimethod research in manufacturing supply chains similarly found that blockchain-supported systems can improve transparency and data integrity, particularly when integrated with complementary digital technologies. These characteristics explain why visibility and traceability emerged as the most immediate benefits in the present study (Ali, 2024; Tiwari, 2023).

The significant relationship between transparency and counterparty-risk reduction can be explained through reduced information asymmetry. Financing institutions and commercial partners face greater uncertainty when they cannot independently verify whether invoices correspond to genuine transactions, whether receivables have already been financed, or whether contractual events have occurred as reported. More accessible and verifiable information narrows this informational gap and improves monitoring capacity. Bi and Xu (2026) provide empirical support for this mechanism by demonstrating that information transparency mediates blockchain's risk-reducing influence in SCF. Transparency consequently reduces the informational space within which misrepresentation, opportunistic behavior, and hidden transaction problems can remain undetected.

The persistence of a direct blockchain effect after accounting for transparency may reflect the contribution of other technological functions. Smart contracts can automate predetermined actions, distributed validation can reduce unilateral manipulation of transaction histories, and timestamped records can strengthen audit trails. Zhang and Liu (2026) specifically identify strengthened contract enforcement alongside transparency as a mechanism through which blockchain-enabled SCF contributes to lower SME credit risk. These capabilities can influence risk even when their effect is not fully captured by perceptual measures of transparency. Blockchain may consequently operate simultaneously as an information infrastructure, control mechanism, and transaction-coordination technology (Kumar, 2023; Singh, 2022).

The incomplete reduction of counterparty risk can be explained by the multidimensional character of financial uncertainty. Blockchain cannot prevent a buyer from experiencing financial distress, ensure that a supplier will maintain operational capacity, remove market volatility, or guarantee that an external physical event has been truthfully represented digitally. Adoption barriers and differences in organizational readiness can further weaken the effectiveness of blockchain-enabled controls. Counterparty risk therefore remains partly endogenous to the economic condition and behavior of participating organizations. Blockchain can improve the evidence available for assessing those risks, but it cannot transform an economically weak counterparty into a financially sound one.

The immediate practical priority is to move blockchain implementation from technology-centered experimentation toward risk-centered system design. Organizations should first identify the specific information asymmetries and counterparty-risk exposures that need to be addressed before selecting blockchain functionalities. Invoice authenticity, duplicate financing, transaction-history verification, delivery confirmation, contractual compliance, and financing-status visibility may require different combinations of distributed records, smart contracts, external verification, and access-control mechanisms. Implementation should consequently begin with a clearly defined risk problem rather than the assumption that blockchain deployment itself constitutes a solution (Munir, 2022; Vu, 2023).

The next organizational priority is to strengthen the infrastructure surrounding the ledger. Data standards, identity management, access permissions, interoperability, audit procedures, cybersecurity, and responsibility for validating external information should be explicitly assigned among participating organizations. Evidence from current SCF research shows that technological, market, organizational, and collaborative barriers continue to affect blockchain adoption. A technically robust blockchain can still produce weak financial-governance outcomes when participants submit inconsistent data or lack incentives to maintain information quality. Implementation strategies should therefore treat governance design and technological architecture as mutually dependent components.

The research agenda should now move beyond broad comparisons between blockchain adopters and non-adopters. Longitudinal studies are needed to determine whether transparency and counterparty-risk outcomes improve as organizations progress from pilot implementation to mature adoption. Comparative research should investigate whether the effects differ among manufacturers, suppliers, banks, fintech platforms, logistics providers, SMEs, and large corporations. Recent evidence already indicates heterogeneity associated with governance quality, industry characteristics, competitive conditions, and organizational context. Future investigation of these boundary conditions would explain why apparently similar blockchain technologies produce different financial outcomes across supply chain environments (Biswas, 2023; Williamson, 2024).

The broader direction should be toward a hybrid governance model in which blockchain complements rather than displaces institutional oversight. The findings indicate that distributed records can enhance transparency, verification, and monitoring, but they do not justify transferring full responsibility for counterparty-risk decisions to technological systems. Banks, buyers, suppliers, auditors, platform operators, and regulators remain responsible for validating data, interpreting risk signals, resolving disputes, and responding to exceptional circumstances. The most productive future for blockchain-enabled supply chain finance therefore lies neither in technological skepticism nor in the promise of entirely “trustless” commerce. Its value lies in creating a more auditable and information-rich environment in which human and institutional decisions about risk can be made on a stronger evidentiary foundation.

CONCLUSION

The most important finding of this study is that blockchain implementation contributes to counterparty-risk reduction primarily through its capacity to improve supply chain transparency rather than through technology adoption alone. The strongest effect was observed in transaction traceability, information verifiability, and shared visibility across supply chain finance participants, while the direct effect on counterparty-risk reduction was comparatively weaker. This distinction is important because it challenges the common assumption that blockchain automatically eliminates trust-related financial risks. The findings indicate that blockchain is most effective when it strengthens the informational conditions under which counterparties are assessed, monitored, and verified. Transparency therefore functions as a central mechanism connecting blockchain implementation with improved risk governance, while residual risks related to data accuracy, liquidity, operational failure, and off-chain events remain beyond the direct control of the blockchain infrastructure.

The principal contribution of this research is conceptual and methodological. Conceptually, the study develops an integrated mechanism-based explanation linking blockchain implementation, multidimensional transparency, and counterparty-risk reduction within supply chain finance. This perspective distinguishes technological capability from financial outcome by showing that blockchain generates value through intermediate processes such as transaction visibility, traceability, verifiability, and monitoring. Methodologically, the study combines structural modeling with case-based evidence to examine both statistical relationships and organizational manifestations of blockchain-enabled risk management. This approach offers a more comprehensive analytical framework than studies that examine blockchain adoption, transparency, or financing risk separately. The study consequently contributes to supply chain finance literature by positioning blockchain not as a substitute for institutional trust, but as a digital infrastructure that can strengthen evidence-based financial governance.

The study is subject to several limitations that provide directions for future research. The cross-sectional design limits the ability to establish long-term causal effects, while purposive sampling may restrict the generalizability of the findings across industries, countries, and levels of blockchain maturity. Perceptual survey measures may also introduce common method bias and may not fully capture actual financial losses, default events, fraud incidents, or transaction-level performance. The case-based evidence remains context-specific and should therefore be expanded through comparative multi-case or longitudinal designs. Future research should employ panel data, transaction-level blockchain records, experimental or quasi-experimental approaches, and cross-country comparisons to examine how regulatory environments, governance quality, firm size, interoperability, data quality, smart-contract design, and organizational readiness influence blockchain effectiveness. Further investigation should also distinguish among different forms of counterparty risk to determine which risks can be meaningfully reduced through blockchain and which continue to require conventional financial, contractual, and institutional safeguards.

DECLARATION OF AI AND AI ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this manuscript, the author(s) used Google Gemini to assist inimproving grammar, language quality, and overall readability of the text. After using this tool, the author(s) Carefully reviewed and edited the content as necessary and take full responbility for the content of the publication.

AUTHOR CONTRIBUTIONS

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Abaoud, M. (2023). Advancing Federated Learning Through Novel Mechanism for Privacy Preservation in Healthcare Applications. *IEEE Access*, *11*(Query date: 2026-08-16 21:34:33), 83562–83579. https://doi.org/10.1109/ACCESS.2023.3301162

Agrawal, D. (2022). A robust drug recall supply chain management system using hyperledger blockchain ecosystem. *Computers in Biology and Medicine*, *140*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.compbiomed.2021.105100

Ahmed, N. (2025). Advancing agriculture through IoT, Big Data, and AI: A review of smart technologies enabling sustainability. *Smart Agricultural Technology*, *10*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.atech.2025.100848

Akella, G. K. (2023). A Systematic Review of Blockchain Technology Adoption Barriers and Enablers for Smart and Sustainable Agriculture. *Big Data and Cognitive Computing*, *7*(2). https://doi.org/10.3390/bdcc7020086

Ali, S. (2024). Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey. *Ad Hoc Networks*, *152*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.adhoc.2023.103320

Bhat, S. A. (2022). Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability. *Agriculture Switzerland*, *12*(1). https://doi.org/10.3390/agriculture12010040

Biswas, A. (2023). Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain. *Sensors*, *23*(4). https://doi.org/10.3390/s23041963

Chang, M. (2022). Acceptance of tourism blockchain based on UTAUT and connectivism theory. *Technology in Society*, *71*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.techsoc.2022.102027

Dasaklis, T. K. (2022). A Systematic Literature Review of Blockchain-Enabled Supply Chain Traceability Implementations. *Sustainability Switzerland*, *14*(4). https://doi.org/10.3390/su14042439

Deep, S. (2022). A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies*, *33*(6). https://doi.org/10.1002/ett.3935

Erol, I. (2022). Alleviating the Impact of the Barriers to Circular Economy Adoption Through Blockchain: An Investigation Using an Integrated MCDM-based QFD With Hesitant Fuzzy Linguistic Term Sets. *Computers and Industrial Engineering*, *165*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.cie.2022.107962

Farah, M. B. (2024). A survey on blockchain technology in the maritime industry: Challenges and future perspectives. *Future Generation Computer Systems*, *157*(Query date: 2026-08-16 21:34:33), 618–637. https://doi.org/10.1016/j.future.2024.03.046

Ferrández-Pastor, F. J. (2022). Agricultural traceability model based on IoT and Blockchain: Application in industrial hemp production. *Journal of Industrial Information Integration*, *29*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.jii.2022.100381

Gangwal, A. (2023). A survey of Layer-two blockchain protocols. *Journal of Network and Computer Applications*, *209*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.jnca.2022.103539

Goudarzi, A. (2022). A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies*, *15*(19). https://doi.org/10.3390/en15196984

Huang, L. (2022). Blockchain implementation for circular supply chain management: Evaluating critical success factors. *Industrial Marketing Management*, *102*(Query date: 2026-08-16 21:34:33), 451–464. https://doi.org/10.1016/j.indmarman.2022.02.009

Kim, T. (2022). An Overview of Cyber-Physical Security of Battery Management Systems and Adoption of Blockchain Technology. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, *10*(1), 1270–1281. https://doi.org/10.1109/JESTPE.2020.2968490

Kumar, P. (2023). Blockchain and Deep Learning for Secure Communication in Digital Twin Empowered Industrial IoT Network. *IEEE Transactions on Network Science and Engineering*, *10*(5), 2802–2813. https://doi.org/10.1109/TNSE.2022.3191601

Munir, M. A. (2022). Blockchain Adoption for Sustainable Supply Chain Management: Economic, Environmental, and Social Perspectives. *Frontiers in Energy Research*, *10*(Query date: 2026-08-16 21:34:33). https://doi.org/10.3389/fenrg.2022.899632

Olawumi, T. O. (2022). Automating the modular construction process: A review of digital technologies and future directions with blockchain technology. *Journal of Building Engineering*, *46*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.jobe.2021.103720

Rana, N. P. (2022). Analysis of challenges for blockchain adoption within the Indian public sector: An interpretive structural modelling approach. *Information Technology and People*, *35*(2), 548–576. https://doi.org/10.1108/ITP-07-2020-0460

Renduchintala, T. (2022). A Survey of Blockchain Applications in the FinTech Sector. *Journal of Open Innovation Technology Market and Complexity*, *8*(4). https://doi.org/10.3390/joitmc8040185

Sadeghi, M. (2022). Adopting distributed ledger technology for the sustainable construction industry: Evaluating the barriers using Ordinal Priority Approach. *Environmental Science and Pollution Research*, *29*(7), 10495–10520. https://doi.org/10.1007/s11356-021-16376-y

Shah, Z. (2022). Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors*, *22*(3). https://doi.org/10.3390/s22031094

Singh, P. (2022). Blockchain and AI technology convergence: Applications in transportation systems. *Vehicular Communications*, *38*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.vehcom.2022.100521

Sun, P. (2024). A Survey of IoT Privacy Security: Architecture, Technology, Challenges, and Trends. *IEEE Internet of Things Journal*, *11*(21), 34567–34591. https://doi.org/10.1109/JIOT.2024.3372518

Sunny, F. A. (2022). A Systematic Review of Blockchain Applications. *IEEE Access*, *10*(Query date: 2026-08-16 21:34:33), 59155–59177. https://doi.org/10.1109/ACCESS.2022.3179690

Tan, A. (2022). Applying Blockchain for Halal food traceability. *International Journal of Logistics Research and Applications*, *25*(6), 947–964. https://doi.org/10.1080/13675567.2020.1825653

Ting, L. (2022). A secure framework for IoT-based smart climate agriculture system: Toward blockchain and edge computing. *Journal of Intelligent Systems*, *31*(1), 221–236. https://doi.org/10.1515/jisys-2022-0012

Tiwari, S. (2023). Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap. *Transportation Research Part E Logistics and Transportation Review*, *170*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.tre.2022.103012

Tsolakis, N. (2023). Artificial intelligence and blockchain implementation in supply chains: A pathway to sustainability and data monetisation? *Annals of Operations Research*, *327*(1), 157–210. https://doi.org/10.1007/s10479-022-04785-2

Vafadarnikjoo, A. (2023). Analyzing blockchain adoption barriers in manufacturing supply chains by the neutrosophic analytic hierarchy process. *Annals of Operations Research*, *327*(1), 129–156. https://doi.org/10.1007/s10479-021-04048-6

Vu, N. (2023). Blockchain adoption in food supply chains: A review and implementation framework. *Production Planning and Control*, *34*(6), 506–523. https://doi.org/10.1080/09537287.2021.1939902

Williams, P. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. *Internet of Things Netherlands*, *19*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.iot.2022.100564

Williamson, S. M. (2024). Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare. *Applied Sciences Switzerland*, *14*(2). https://doi.org/10.3390/app14020675

Yavaprabhas, K. (2023). Blockchain as the "trust-building machine" for supply chain management. *Annals of Operations Research*, *327*(1), 49–88. https://doi.org/10.1007/s10479-022-04868-0

Yousefi, S. (2022). An analytical approach for evaluating the impact of blockchain technology on sustainable supply chain performance. *International Journal of Production Economics*, *246*(Query date: 2026-08-16 21:34:33). https://doi.org/10.1016/j.ijpe.2022.108429

Zeng, H. (2023). An IoT and Blockchain-based approach for the smart water management system in agriculture. *Expert Systems*, *40*(4). https://doi.org/10.1111/exsy.12892