

Blockchain Technology in Supply Chain Auditing: Enhancing Transparency and Reducing Information Asymmetry in Accounting Systems

Syamsul Hidayat^{1,*}, Ming Sheng Fang²

¹ Universitas Muhammadiyah Yogyakarta, Indonesia

² Department of Business Administration, Asia University, Taiwan

*Corresponding author: syamsul.hidayat@umy.ac.id

ARTICLE INFO

Article history

Received: 28 Februari 2026

Revised: 20 march 2026

Accepted: 25 August 2026

Published: 30 August 2026

Keywords

Blockchain
Supply-chain auditing
Inventory audit
Accounting information systems
Information asymmetry
Audit quality
Distributed ledger technology
Managerial accounting

JEL Classification

M41; M42; O33; L14

ABSTRACT

This article examines how blockchain technology may improve supply-chain auditing by strengthening traceability, evidential integrity, and the timeliness of accounting information while reducing information asymmetry among suppliers, focal firms, auditors, lenders, and investors. It develops an accounting-centered framework that distinguishes the technical immutability of recorded transactions from the reliability of the underlying events. Blockchain can create a shared, time-stamped record of inventory movements and related documents, but it cannot independently establish whether goods exist, quantities are accurate, or source data are truthful. Drawing on agency theory, information asymmetry, transaction cost economics, institutional theory, and the audit evidence framework, the article synthesizes recent research and professional guidance and proposes a testable model linking blockchain-enabled auditability to inventory audit quality and financial reporting transparency. The model treats data governance, system interoperability, internal controls, assurance design, and supplier participation as boundary conditions. It also identifies costs and risks, including implementation expense, privacy constraints, cyber vulnerabilities, oracle problems, consensus governance, and the danger of automating flawed processes. The methodological contribution is a replicable panel and field-study design with operational measures for inventory discrepancies, audit adjustments, audit effort, reporting timeliness, and disclosure quality. Because no original firm-level dataset or field experiment was supplied, the article does not report fabricated statistical estimates. Instead, it presents an evidence-based synthesis, hypotheses, implementation implications, and a research agenda for accounting and financial-technology scholarship.

© 2026 The Author(s). Published by PT Advanced Business Journal. This is an open-access article distributed under the terms of the [Creative Commons Attribution 4.0 International \(CC BY 4.0\)](#) license.

1. INTRODUCTION

Supply chains are increasingly managed through networks of organizations that exchange goods, invoices, purchase orders, shipment records, certificates, and payment information. Although these records support operational coordination, they are often stored in separate information systems controlled by different parties. The resulting fragmentation creates opportunities for duplicate records, delayed reconciliations, inconsistent inventory balances, and disputes about when ownership or custody changed. For accountants and auditors, the problem is not merely technological. It concerns whether evidence collected across organizational boundaries is complete, accurate, traceable, and sufficiently reliable to support financial statements (IAASB, 2022; Ramadhan, 2026).

Inventory is particularly exposed to these problems because it moves physically while its accounting representation moves through purchase, receipt, storage, production, transfer, and sales systems. A company may record a shipment as dispatched while the receiving party records it only after inspection; quantities can differ because of damage, measurement conventions, or timing; and supplier documents may not be reconciled promptly with warehouse and general-ledger records. Traditional audit procedures address these risks through observation, confirmations, document inspection, cut-off testing, analytical procedures, and reconciliations. Yet these procedures can be costly when records are dispersed, when manufacturing supply chains are exposed to disruption risk, or when audit evidence must be assembled after the reporting period (Fang, 2026; IAASB, 2022).

Blockchain technology has attracted attention because it can create a shared ledger in which transactions are time-stamped, linked cryptographically, and validated under a network's rules. In a supply-chain setting, a permissioned blockchain may record purchase-order events, dispatch confirmations, receipts, quality inspections, warehouse transfers, and related accounting references. Participants can then consult a common sequence of authorized records rather than independently maintaining incompatible transaction histories. When designed well, such infrastructure may improve traceability, reduce reconciliation effort, and make changes to recorded transactions more visible (NIST, 2021; ISO, 2022).

The accounting value of blockchain, however, should not be overstated. A distributed ledger can protect the integrity of data after entry, but it cannot guarantee that the original data were true. If a supplier records the wrong quantity, a sensor is miscalibrated, a barcode is attached to the wrong shipment, or an authorized user colludes with another participant, the ledger may preserve an inaccurate claim with great consistency. The central issue is therefore not whether blockchain makes records immutable, but whether the wider control environment makes the records trustworthy and relevant to audit objectives. Technology may strengthen the chain of custody for evidence without replacing professional skepticism, physical verification, or substantive testing (NIST, 2021; IAASB, 2022).

The research question is how blockchain adoption can improve the effectiveness of supply-chain auditing and the transparency of financial reporting. This question has managerial-accounting and financial-technology dimensions. For management, better traceability can reduce inventory uncertainty, support working-capital decisions, and improve exception handling. For external auditors, it may improve access to evidence and reduce time spent reconciling conflicting records. For financial statement users, more reliable transaction histories may strengthen confidence in inventory balances, cost of goods sold, and related disclosures. These potential benefits depend on the quality of data governance, the participation of suppliers, interoperability with enterprise systems, and the design of controls around the ledger.

Prior research has examined blockchain's potential in accounting, auditing, and supply-chain management, but several gaps remain. First, discussions of blockchain often emphasize general transparency or operational traceability without specifying the audit assertions and accounting outcomes through which value should arise. Second, technical properties such as immutability and consensus are sometimes treated as if they automatically establish the truth of physical events. Third, empirical findings are difficult to compare because studies use different definitions of adoption, different sectors, and different outcome measures. Recent reviews and empirical studies of blockchain and data-driven technologies in accounting and supply chains call for more careful attention to implementation conditions, governance, and the distinction between technological capability and realized organizational benefit (Casino et al., 2021; Pontjoharyo, 2026; Schmitz and Leoni, 2021).

This article addresses these gaps by developing a mechanism-based framework that connects blockchain-enabled traceability to inventory audit quality and financial reporting transparency. It asks three questions:

- RQ1.** Through which accounting and audit mechanisms can blockchain reduce information asymmetry in supply chains?
- RQ2.** Which organizational and technical conditions determine whether blockchain improves auditability rather than simply digitizing existing errors?
- RQ3.** How should researchers measure the resulting changes in inventory reliability, audit effort, and reporting quality?

The article aims to clarify both the promise and the limits of blockchain in accounting systems and to provide an empirical design that can be implemented in future field research.

The article makes four contributions. It places audit assertions and financial reporting outcomes at the center of blockchain evaluation; integrates agency, information asymmetry, transaction cost, and institutional explanations; identifies data governance, interoperability, supplier participation, and assurance design as key boundary conditions; and proposes a testable empirical strategy using operational and accounting indicators. Rather than asserting that blockchain necessarily improves audit quality, the article develops conditional hypotheses that can be evaluated with firm-level data. Because no original dataset or

experiment was supplied, the manuscript is an evidence synthesis and research framework, not a report of new regression results.

The remainder of the article is structured as follows. Section 2 reviews the technology, accounting use cases, theoretical foundations, and prior evidence. Section 3 develops the conceptual model and hypotheses. Section 4 explains the proposed methodology, measures, and identification strategy. Section 5 synthesizes the evidence and discusses the expected mechanisms and risks. Section 6 presents implications, limitations, and future research directions, followed by the conclusion and references.

2. LITERATURE REVIEW

2.1 Blockchain and distributed ledger technology

Blockchain is a type of distributed ledger in which records are grouped or linked using cryptographic techniques and accepted according to a consensus protocol. The ledger is replicated across participating nodes, and the protocol defines how new records are validated. In a permissionless network, participation may be broadly open; in a permissioned network, access and validation rights are restricted to approved participants. Supply-chain accounting applications often favor permissioned arrangements because commercial data can be confidential and participants require defined responsibilities, performance standards, and dispute procedures (NIST, 2021; ISO, 2022).

The term blockchain is often used as if it described one uniform technology. In practice, systems differ in consensus mechanism, access control, data visibility, transaction throughput, governance, and integration architecture. These design choices affect both the audit trail and the cost of operating the system. A shared ledger may provide a common transaction history, but it does not eliminate the need for master-data management, access controls, system backups, incident response, or business continuity. Nor does it remove the need to establish who is authorized to submit, validate, correct, or reverse a transaction.

For accounting purposes, a crucial distinction exists between recording a transaction and recognizing it under accounting standards. A blockchain entry may document a dispatch event, but the accounting treatment may depend on contractual terms, transfer of control, shipping terms, inspection rights, and the applicable financial reporting framework. A smart contract can automate a payment or status update when specified conditions are met, yet those conditions may not capture all legal or economic circumstances. Accounting policy remains a matter of standards, judgment, and evidence rather than a function that can be delegated automatically to code.

The cryptographic integrity of a ledger makes unauthorized alteration more detectable, but “immutable” should be interpreted carefully. Networks can implement correction transactions, governance changes, or exceptional recovery procedures. Data may also be stored off-chain, with only a hash or reference recorded on-chain. In such cases, the auditability of the full record depends on the availability, retention, and integrity of the off-chain source. The system’s control design should document what is stored, what is referenced, who can access the underlying documents, and how corrections are represented.

2.2 Supply-chain auditing and inventory assertions

Supply-chain auditing examines evidence generated across purchasing, logistics, warehousing, production, and distribution. For inventory, the auditor commonly considers existence, completeness, rights and obligations, valuation and allocation, and presentation. Blockchain may support these assertions in different ways. Time-stamped receipt records can help establish transaction sequence; linked purchase orders and shipping documents can support completeness and cut-off; custody records can clarify where goods were transferred; and controlled access can preserve a traceable history of approvals. None of these records alone proves physical existence or ownership, and the auditor must evaluate whether the evidence is relevant and reliable for the specific assertion.

Inventory audit risks are not confined to fraud. They also arise from process complexity, system latency, inconsistent units of measure, returns, shrinkage, obsolete stock, consignment arrangements, goods in transit, and differences between physical and book quantities. A blockchain implementation may reduce disputes about the history of recorded events, but it will not automatically resolve differences in product

codes, location identifiers, measurement standards, or contractual interpretation. Effective auditability requires a common data model and agreed definitions across the participating firms.

The value of a shared ledger may be greatest where many parties contribute to a transaction history and where the cost of reconciling separate records is high. For example, a manufacturer may receive goods from several suppliers, transporters, and third-party warehouses. If each party stores its own event record, the auditor may need to compare documents from multiple systems and resolve inconsistencies manually. A common ledger can make the sequence easier to reconstruct. Yet where one firm controls all relevant data and already operates a reliable integrated system, blockchain may add limited value compared with a well-designed centralized database and audit log.

2.3 Information asymmetry and agency theory

Information asymmetry occurs when one party has information that another party needs but cannot observe at comparable cost. In supply chains, suppliers know more about shipment preparation, product quality, and dispatch timing; warehouses know more about receipt and storage conditions; and focal firms may have limited visibility into events occurring outside their own systems. Managers also possess information about inventory adjustments and exceptions that external auditors and investors cannot observe directly. Such asymmetry can increase monitoring costs, create opportunities for opportunistic behavior, and weaken confidence in reported balances.

Agency theory predicts that monitoring and credible information can reduce conflicts between principals and agents. Shareholders rely on managers to maintain accurate inventory records, while managers rely on suppliers and logistics partners to report transactions correctly. Blockchain may reduce the scope for unilateral alteration by creating a shared and time-stamped transaction history. It may also make exceptions visible to multiple participants, improving accountability. However, the technology does not remove agency problems if participants can enter false data, collude, or exploit weak identity management. Governance of the network is therefore part of the control environment, not an optional technical detail.

The agency perspective also highlights the distribution of costs and benefits. A focal company may gain more transparency while suppliers bear the cost of data capture, system integration, and compliance. Smaller suppliers may resist adoption if they perceive the ledger as a tool for surveillance or bargaining-power asymmetry. Adoption is more likely to be sustainable when participation rules, access rights, dispute resolution, and data ownership are negotiated transparently. In accounting terms, a network that excludes important suppliers may produce a technically consistent but incomplete record of the actual supply chain.

2.4 Signaling and information quality

Signaling theory suggests that firms can communicate the quality of their control systems by adopting practices that are difficult to imitate credibly. Blockchain-enabled audit trails may signal stronger transaction governance when the system is independently assessed, used consistently across material transactions, and integrated with internal controls. Such a signal is more credible when external auditors can test system controls and reconcile ledger events with physical evidence and source documents. A public statement that a firm uses blockchain, without information about coverage or assurance, is a weak signal because it does not establish whether the system affects material accounting processes.

Information quality has several dimensions: accuracy, completeness, timeliness, relevance, consistency, and verifiability. Blockchain can contribute to integrity and traceability after data entry, and it can improve timeliness when events are recorded promptly. It does not by itself guarantee relevance, completeness, or physical accuracy. A ledger populated only with selected transactions may be incomplete; a record using inconsistent units may be difficult to compare; and a perfectly preserved entry can still be wrong. The research model therefore treats blockchain adoption as an enabling capability whose effects depend on data governance and source validation.

2.5 Transaction cost economics

Transaction cost economics explains organizational arrangements in terms of the costs of searching, negotiating, monitoring, and enforcing exchanges. Supply-chain records are often reconciled because

counterparties maintain separate systems and have different incentives or definitions. A shared ledger may reduce some coordination and verification costs by establishing a common transaction history. Smart contracts can automate routine status checks or settlement triggers, potentially lowering administrative effort. However, implementation, integration, governance, cybersecurity, training, and exception handling create new costs. Blockchain is economically justified only when the reduction in coordination and assurance costs exceeds the incremental costs and risks.

This framework implies that blockchain's value is contingent on transaction characteristics. The case is stronger when many independent parties exchange high volumes of traceable events, when disputes are frequent, and when a shared record is difficult to create through existing systems. The case is weaker when the supply chain is stable, one party controls the data, transactions are low-volume, or a conventional database already provides reliable access controls and audit trails. A sound investment decision should compare blockchain against realistic alternatives, not against a hypothetical paper-based process.

2.6 Institutional theory and assurance standards

Institutional theory highlights the influence of regulation, professional expectations, customer requirements, and industry norms on technology adoption. Companies may adopt blockchain because trading partners request traceability, regulators require stronger documentation, or auditors seek more reliable evidence. Such pressures can encourage standardization, but they can also produce symbolic adoption when organizations implement a platform primarily to signal innovation. The difference between substantive and symbolic adoption should be measured through actual process coverage, transaction volume, integration with accounting systems, and evidence of use in audit procedures.

Professional standards remain central because technology does not determine the sufficiency of audit evidence. Auditors must understand the information system, assess risks of material misstatement, evaluate relevant controls, and obtain evidence appropriate to the audit objective. Guidance on technology-related audit considerations emphasizes the need to assess data reliability and system controls rather than treating digital records as inherently trustworthy (IAASB, 2022). Blockchain implementation should therefore be aligned with the organization's control framework and the auditor's evidence strategy.

2.7 Recent evidence on blockchain in accounting and supply chains

Recent literature describes blockchain as a potentially useful infrastructure for traceability, shared records, and automated transaction processing, while also documenting barriers related to scalability, governance, privacy, interoperability, and the quality of off-chain data. Schmitz and Leoni (2021) discuss the implications of blockchain for accounting and auditing, emphasizing that the technology can change how transactions are recorded and verified but does not eliminate the need for professional judgment. Casino et al. (2021) review blockchain applications and identify persistent implementation and evaluation challenges. Pontjoharyo (2026), studying ASEAN-listed firms, finds that data-driven technologies improve financial decisions mainly when they are embedded in core financial processes, which highlights the importance of organizational context and the need for empirical evidence beyond conceptual enthusiasm.

Supply-chain studies often identify traceability and data sharing as major potential benefits, especially where participants need a common view of product movement. Yet adoption studies also report barriers involving cost, lack of standards, skills shortages, organizational resistance, and uncertainty about network governance. These barriers matter directly to accounting outcomes: a ledger that covers only a subset of suppliers or transactions may reduce reconciliation effort in one area while leaving material completeness risks elsewhere. A useful empirical study should therefore measure implementation depth and scope rather than rely on a binary adopted/not-adopted indicator.

The literature also warns that a blockchain solution can create new forms of information asymmetry. Technical administrators may control the rules of the network; larger firms may determine which data suppliers must provide; and participants may not understand how information can be accessed or used. A shared ledger does not necessarily mean equal access, equal bargaining power, or equal ability to interpret the data. Governance rules should therefore be examined as part of the explanation for transparency outcomes.

2.8 Research gap

The first gap is construct clarity. Studies frequently treat blockchain adoption, supply-chain transparency, and audit quality as related but insufficiently separated constructs. A company can adopt blockchain without using it for material inventory transactions; it can improve traceability without improving physical accuracy; and it can shorten reconciliation time without changing the quality of external audit evidence. The present framework distinguishes adoption intensity, auditability, inventory reliability, and financial reporting transparency as separate variables.

The second gap concerns the boundary between on-chain integrity and off-chain truth. Much of the conceptual appeal of blockchain rests on the difficulty of altering recorded information, but supply-chain events originate in the physical world. The system needs reliable identification, scanning, weighing, inspection, and authorization processes to connect physical goods with digital records. Research should examine whether source validation and internal controls moderate the association between blockchain and audit outcomes.

The third gap is outcome measurement. General claims about “greater transparency” are difficult to test unless they are translated into observable indicators. Suitable outcomes include inventory adjustment frequency, count-to-book discrepancies, audit adjustments attributable to inventory, reconciliation time, days to close, audit hours devoted to inventory, restatements, and the timeliness of reporting. These measures are not perfect substitutes for audit quality, but they make the mechanism more observable and allow comparisons across firms and periods.

The fourth gap is the limited integration of managerial accounting and financial reporting. Blockchain may affect not only external audit procedures but also internal decisions about stock levels, shrinkage, supplier performance, and working capital. A framework that considers both domains can test whether improved traceability translates into lower inventory uncertainty and more reliable financial reporting, or whether the benefits remain confined to operational visibility.

3. CONCEPTUAL FRAMEWORK AND HYPOTHESIS DEVELOPMENT

3.1 Blockchain adoption intensity and auditability

Blockchain adoption intensity should reflect the extent to which the ledger is embedded in material supply-chain processes. A binary adoption indicator can classify firms that run a limited pilot in the same category as firms that record most material inventory events on a production network. A more informative measure can combine the proportion of material transactions captured, the number of participating supply-chain tiers, integration with ERP and warehouse systems, the use of digital identities, and the extent to which audit procedures rely on the ledger. Each component should be defined in advance and supported by documentary evidence.

Higher adoption intensity can improve auditability through three mechanisms. First, a shared sequence of events may reduce the effort required to reconstruct transaction history. Second, cryptographic links and permissioned access can make unauthorized changes more detectable. Third, common transaction identifiers can facilitate reconciliation among purchase orders, shipping documents, goods receipts, inventory subledgers, and the general ledger. These benefits are expected to be stronger when data are entered promptly and source documents are linked to the relevant event.

The hypothesis is not that the ledger makes every inventory assertion true. Rather, greater adoption intensity is expected to improve the availability and traceability of audit evidence, conditional on controls over source data and physical verification. **H1:** Blockchain adoption intensity is positively associated with supply-chain auditability and inventory audit quality.

3.2 Auditability and inventory reliability

Auditability refers to the ability to trace transactions, inspect supporting evidence, reconstruct changes, and test controls. Inventory reliability refers to the degree to which recorded quantities and values correspond to the underlying economic events and applicable accounting requirements. Auditability can improve reliability when exceptions are identified earlier, reconciliations are more complete, and responsibility for

discrepancies is clearer. However, a traceable error remains an error. Physical counts, independent confirmations, valuation tests, and review of obsolescence remain necessary where they address risks that the ledger cannot resolve.

The model therefore treats auditability as a potential mediator between blockchain adoption and inventory reliability. Blockchain may first improve the traceability and accessibility of evidence, which then supports faster exception resolution and more accurate inventory records. The strength of this pathway depends on whether the organization acts on exceptions and whether control owners have authority to correct the underlying process. **H2:** Supply-chain auditability mediates the positive association between blockchain adoption intensity and inventory reliability.

3.3 Information asymmetry and financial reporting transparency

Information asymmetry can decline when participants share a reliable transaction history and can independently verify relevant events. In accounting systems, this may reduce differences between supplier, warehouse, procurement, and finance records. It can also improve the auditor's ability to reconcile transactions and understand the timing of goods movements. Better information availability may support more timely reporting and improve the consistency of inventory and cost-of-goods-sold figures.

The expected effect depends on the completeness of network participation. If key suppliers or warehouses remain outside the ledger, users may still rely on separate records for a material portion of transactions. A common ledger can also create false confidence if participants assume that recorded events are complete without testing whether all relevant events were captured. Thus, information asymmetry should be measured not only through the existence of shared access but also through reconciliation discrepancies, information delays, and the completeness of participating entities.

H3: Greater blockchain-enabled traceability is negatively associated with supply-chain information asymmetry. **H4:** Lower information asymmetry is associated with greater financial reporting transparency, reflected in fewer inventory-related adjustments and more timely reporting.

3.4 Data governance as a moderator

Data governance includes the rules for data ownership, validation, access, correction, retention, and accountability. It determines who can submit an event, who can validate it, how identities are verified, how disputes are resolved, and how off-chain records are protected. A network with weak governance can preserve unreliable data or allow participants to avoid recording unfavorable events. Strong governance improves the likelihood that blockchain records are complete, authorized, and fit for accounting use.

Governance should include both technical controls and organizational responsibilities. Technical controls may cover role-based access, cryptographic identity, logging, key management, and validation rules. Organizational controls may define responsibility for data entry, reconciliation, exception escalation, and independent review. External assurance can test selected controls, but assurance scope and competence must be explicit. **H5:** The positive association between blockchain adoption intensity and auditability is stronger when data governance and internal controls are more effective.

3.5 Interoperability and supplier participation

Interoperability is the ability of the ledger to exchange data reliably with ERP, warehouse management, procurement, logistics, and accounting systems. Without interoperability, employees may have to enter the same transaction more than once, creating additional opportunities for error. If the blockchain is not integrated with the inventory subledger and general ledger, its records may remain operationally interesting but financially disconnected. Standardized identifiers, common units of measure, application programming interfaces, and documented reconciliation routines are therefore essential to accounting value.

Supplier participation determines the breadth of the shared record. A focal company cannot reconstruct a complete chain of custody if material suppliers, carriers, or warehouses do not record relevant events. Participation may be limited by cost, skills, privacy concerns, and bargaining-power imbalances. The network should provide clear benefits and proportionate obligations to smaller suppliers. **H6:** Interoperability strengthens the positive association between blockchain adoption and inventory reliability. **H7:** Supplier

participation coverage strengthens the association between blockchain adoption and supply-chain transparency.

3.6 Costs, risks, and competing hypotheses

Blockchain implementation can increase capital expenditure, training needs, cybersecurity obligations, and coordination costs. It can also introduce dependence on platform vendors, create privacy concerns, and make error correction more complex if participants misunderstand how records should be amended. In some settings, a centralized database with strong controls may deliver similar benefits at lower cost. The net effect should therefore be evaluated against a realistic counterfactual rather than assumed to be positive merely because blockchain is a novel technology.

H8: The positive relationship between blockchain adoption and audit outcomes is weaker when implementation and governance costs are high relative to transaction complexity. This hypothesis recognizes that technology fit matters. The article does not assume that blockchain is optimal for every supply chain; instead, it predicts that benefits are greater where multiple parties need a shared, verifiable history and where the existing reconciliation burden is substantial.

Table 1. Summary of proposed hypotheses

Hypothesis	Relationship	Expected direction
H1	Blockchain adoption intensity → auditability / inventory audit quality	Positive
H2	Auditability mediates blockchain adoption → inventory reliability	Positive indirect effect
H3	Blockchain-enabled traceability → information asymmetry	Negative
H4	Information asymmetry → reporting transparency	Negative association with transparency outcomes
H5	Blockchain adoption × data governance → auditability	Positive interaction
H6	Blockchain adoption × interoperability → inventory reliability	Positive interaction
H7	Blockchain adoption × supplier participation → transparency	Positive interaction
H8	Blockchain adoption × relative implementation cost → audit outcomes	Negative interaction

Source: Authors' elaboration.

4. METHOD

4.1 Research design

The article combines a structured synthesis of recent literature with a proposed empirical design. The synthesis identifies theoretical mechanisms, implementation conditions, and measurement issues in blockchain-enabled supply-chain auditing. The empirical design is intended for a multi-firm panel study, supplemented where feasible by interviews or process-level case evidence. No original company-level dataset was provided or estimated for this manuscript; accordingly, the article does not present new coefficients, significance tests, or causal findings. The purpose is to establish a transparent and replicable research design for a subsequent empirical study.

A mixed-method design is appropriate because accounting outcomes are quantitative, while the processes that generate them often depend on local controls and interorganizational governance. A panel design can test whether adoption is associated with changes in inventory discrepancies, audit effort, or reporting timeliness. Case studies or interviews can explain why similar systems produce different outcomes across firms. The quantitative and qualitative components should be integrated through a common framework rather than treated as unrelated exercises.

4.2 Population, sampling, and observation window

The population may consist of manufacturing, retail, logistics, and distribution firms with material inventory balances and multi-tier supply chains. A purposive sample should include firms that have implemented a blockchain-enabled supply-chain platform and comparable firms using conventional digital systems. Firms with pilots should be distinguished from those with production deployment. The study should document the

implementation date, process coverage, participating entities, and the extent of integration with accounting systems.

A three- to five-year observation window before and after implementation is desirable when data availability permits. The window should be long enough to observe changes in controls and reporting outcomes, but not so long that major unrelated system transformations dominate the comparison. Firms undergoing mergers, ERP replacement, major warehouse redesign, or audit-firm changes should be flagged. The sample should include unsuccessful or discontinued implementations where information is available, reducing the risk of reporting only successful adopters.

4.3 Data sources and collection

The quantitative dataset should combine audited financial statements, inventory subledger summaries, internal audit reports, external audit adjustment logs where access is granted, system implementation records, and supply-chain transaction logs. Publicly available annual reports can support measures of reporting timeliness and financial statement restatements, but they are unlikely to provide detailed inventory discrepancy data. Access to internal audit and operations data would therefore materially strengthen the study. Data access agreements should specify confidentiality, anonymization, retention, and the permitted use of sensitive supplier information.

Blockchain adoption should be documented through implementation contracts, system architecture descriptions, process maps, user access matrices, and transaction coverage reports. The researcher should not infer meaningful adoption solely from a company's press release. Where data are stored off-chain, the study should document how source documents are linked, retained, and made available for audit. Data governance should be assessed using policy documents, system configuration evidence, and interviews with responsible personnel rather than self-reported maturity scores alone.

Qualitative evidence may be collected through semi-structured interviews with financial controllers, internal auditors, external auditors, supply-chain managers, IT/security staff, and participating suppliers. Interviews should examine how exceptions are identified, who can alter or correct records, how physical events are validated, how the system changes audit procedures, and which costs were not anticipated during implementation. Interview analysis should use a transparent coding scheme based on the conceptual model while allowing new themes to emerge from the data.

4.4 Variable operationalization

The principal independent variable is blockchain adoption intensity. A proposed index may combine the share of inventory transactions recorded on the network, the number of supply-chain tiers participating, the proportion of material suppliers onboarded, the level of integration with ERP and warehouse systems, and the extent to which the ledger is used in internal or external audit procedures. Each component should be normalized and documented. A binary adoption variable may be retained for robustness, but it should not replace measures of depth and coverage.

Auditability can be measured through the time required to trace a sample transaction from purchase order to receipt, warehouse movement, invoice, and general-ledger entry; the proportion of sampled transactions with complete linked evidence; the time required to resolve exceptions; and the number of manual reconciliations needed. These measures capture the availability and traceability of evidence, not audit quality in its entirety. Audit quality should also be considered through inventory-related audit adjustments, the nature of audit findings, and whether auditors can independently validate system controls.

Inventory reliability may be measured by physical-count discrepancies relative to recorded inventory, the frequency and magnitude of inventory adjustments, shrinkage, write-offs, obsolete inventory, and cut-off errors. These indicators are influenced by operational factors such as product mix, storage conditions, seasonality, and warehouse design. The analysis should normalize discrepancies by inventory value or transaction volume where appropriate and control for operational complexity. Inventory valuation errors should be distinguished from quantity errors because blockchain may affect their causes differently.

Financial reporting transparency can be operationalized through the timeliness of annual reporting, inventory-related restatements, audit adjustments, the number of late reconciliations, and the consistency of

reported inventory disclosures. No single proxy is a complete measure of transparency. Reporting timeliness may reflect regulatory deadlines and organizational resources, while restatements are relatively rare and can be affected by detection practices. The study should use multiple outcomes and avoid treating a decline in reported exceptions as evidence of improvement if the control system's detection capacity has also weakened.

Data governance can be measured through the presence and enforcement of access controls, data validation rules, identity management, change logging, exception escalation, correction procedures, independent review, and documented ownership of data. Interoperability can be measured through the proportion of transactions automatically reconciled across systems, the use of standardized identifiers, and the frequency of manual data conversion. Supplier participation can be measured as the share of material suppliers or transaction volume represented on the network. Implementation cost should include software, integration, training, assurance, ongoing governance, and supplier onboarding costs.

Table 2. Proposed variables and measures

Construct	Operational measure	Model role	Possible source
Blockchain adoption intensity	Transaction coverage, tier participation, ERP integration, audit use	Independent	System records; implementation documentation
Auditability	Evidence completeness, trace time, exception resolution time	Mediator / outcome	Audit files; transaction logs
Inventory reliability	Count-to-book discrepancy, adjustments, shrinkage, cut-off errors	Outcome	Inventory records; internal audit
Reporting transparency	Reporting lag, inventory adjustments, restatements, reconciliation delay	Outcome	Financial statements; audit logs
Data governance	Access controls, validation, correction protocols, independent review	Moderator	Policies; system settings; interviews
Interoperability	Automated matching, standardized identifiers, manual re-entry rate	Moderator	ERP and warehouse logs
Supplier participation	Share of material suppliers or transaction volume on network	Moderator	Supplier register; platform logs
Implementation cost	Initial and recurring cost relative to volume/complexity	Moderator / control	Project accounts; management records
Controls	Firm size, inventory intensity, ERP maturity, complexity, auditor tenure	Controls	Financial statements; surveys

Source: Authors' elaboration.

4.5 Baseline empirical model

A baseline panel specification may be written as:

$$AUDITOUT_{it} = \beta_0 + \beta_1 BLOCKCHAIN_{it} + \beta_2 GOVERNANCE_{it} + \beta_3 (BLOCKCHAIN \times GOVERNANCE)_{it} + \beta_4 CONTROLS_{it} + \mu_i + \tau_t + \varepsilon_{it} \quad (\text{Eq.1})$$

where AUDITOUT represents one of the defined outcomes, such as inventory discrepancy, traceability time, or inventory-related audit adjustments. BLOCKCHAIN measures adoption intensity; GOVERNANCE represents data-governance maturity; μ_i denotes firm fixed effects; and τ_t denotes year effects. The sign of β_1 depends on the outcome: a positive sign is expected for evidence completeness but a negative sign for discrepancy rates and reconciliation time.

To test mediation, the study can estimate whether blockchain adoption predicts auditability and whether auditability predicts inventory reliability after accounting for adoption and relevant controls. Indirect effects should be evaluated using bootstrap confidence intervals or a suitable multilevel mediation approach, depending on the data structure. The mediation model should not be interpreted causally unless temporal ordering and confounding assumptions are defensible. Where process data are available, the researcher should measure adoption before the auditability outcome and auditability before the financial reporting outcome.

A difference-in-differences design may be feasible when firms adopt blockchain at different times and a credible comparison group is available. The analysis should test pre-adoption trends, examine anticipation effects, and control for concurrent ERP or warehouse transformations. Adoption is likely to be endogenous: firms with stronger controls may be more likely to adopt, and firms experiencing inventory problems may adopt in response to those problems. Matching or weighting may improve comparability but cannot eliminate unobserved confounding. Results should be described as associations unless the identification design supports a causal interpretation.

4.6 Reliability, validity, and robustness

Construct validity requires separating technology presence from operational use. Adoption intensity should be verified using system logs and transaction coverage rather than relying solely on executive survey responses. Auditability measures should be independently defined and, where possible, extracted from audit workpapers or controlled tests. Inventory discrepancies should be measured consistently before and after implementation, with changes in counting frequency or warehouse procedures documented. If the implementation itself improves detection, recorded discrepancies may initially rise even as control quality improves; this possibility must be considered in interpretation.

Robustness checks should use alternative adoption measures, exclude pilot-only projects, distinguish permissioned from permissionless systems, and compare outcomes for transactions recorded on-chain with comparable transactions outside the network. The analysis should control for ERP upgrades, warehouse automation, acquisitions, auditor changes, and shifts in inventory composition. It should test whether results persist after excluding firms with unusually high transaction volumes or one dominant participant. Standard errors should account for clustering at the firm level and, where relevant, at the supply-chain network level.

Common-method bias is a concern if adoption, governance, and outcomes are all measured using a single survey respondent. Combining survey responses with system logs, financial statements, and audit records can reduce this risk. Selection bias is also likely because firms willing to disclose blockchain implementation may be more innovative or better managed. Researchers should document the characteristics of non-participants where possible and discuss the limits of generalization. Interviews can illuminate mechanisms but should not be used to claim prevalence without an appropriate sampling strategy.

5. EVIDENCE SYNTHESIS AND ANALYTICAL DISCUSSION

5.1 Interpreting blockchain's potential audit benefits

The literature suggests that blockchain can improve the traceability and integrity of transaction histories when the network is well governed and the relevant events are recorded consistently. For supply-chain auditing, the principal benefit is a more accessible chain of evidence across organizational boundaries. A shared ledger may reduce the time spent obtaining confirmations, matching documents, and reconstructing the sequence of inventory movements. These gains are most plausible where the existing process relies on multiple disconnected systems and where counterparties dispute the timing or status of transactions (Schmitz and Leoni, 2021; Casino et al., 2021).

The benefit should not be equated with the elimination of audit procedures. Auditors still need to assess the reliability of system-generated information, test relevant IT controls, inspect physical inventory where required, evaluate valuation and obsolescence, and consider rights and obligations. Blockchain evidence may be particularly useful for tracing transaction history and testing cut-off, but physical observation and independent confirmation can remain essential for existence and ownership. The technology changes the form and accessibility of evidence; it does not eliminate the need to judge whether that evidence addresses the audit assertion.

A central implication is that audit effort may be reallocated rather than simply reduced. Less time may be spent on routine reconciliation, while more time is needed to assess system governance, smart-contract logic, cybersecurity, access management, and the integrity of data entering the ledger. The net effect on audit fees or hours is therefore an empirical question. In the early stages of adoption, total audit effort may increase

because auditors need to understand a new system and test its controls. Benefits may emerge later if the system is stable, widely adopted, and sufficiently integrated with accounting processes.

5.2 The oracle problem and physical-world verification

The most important limitation is the connection between physical events and digital records. Blockchain can preserve a record that a shipment was received, but it cannot independently determine whether the shipment contained the stated goods or whether the quantity was measured accurately. The reliability of the ledger depends on the devices, people, procedures, and documents that generate the initial data. This is often described as the oracle problem: information from the physical world must enter the digital system through an external mechanism that can itself be wrong or manipulated.

Mitigating this problem requires layered controls. Unique product identifiers, tamper-evident seals, calibrated weighing devices, controlled scanning procedures, segregation of duties, independent inspection, and exception-based physical counts can increase confidence in the connection between goods and records. Sensors may automate data capture, but sensor calibration, maintenance, and device identity must be controlled. A robust design also requires procedures for damaged goods, partial shipments, returns, substitutions, and emergency corrections. These events are common in actual supply chains and should not be treated as exceptions outside the system design.

The accounting implication is that immutability can increase the persistence of an error if source validation is weak. An incorrect entry may be difficult to erase, but the system can record a correcting transaction that preserves the audit trail. Such a process can be more transparent than silent alteration, provided users understand the correction logic and auditors can trace the original and amended records. The goal is not to prevent all changes; it is to make changes authorized, explainable, and auditable.

5.3 From traceability to reduced information asymmetry

A shared ledger can reduce information asymmetry by allowing authorized participants to inspect the same sequence of transaction events. Suppliers can confirm dispatch, carriers can document custody, warehouses can record receipt, and finance teams can reconcile the evidence with invoices and inventory accounts. If the records are timely and complete, participants may spend less time requesting documents and resolving contradictory versions. This can improve the information environment for managers and auditors, especially in supply chains with many independent parties.

However, shared visibility is not identical to transparency. Network administrators may restrict access, participants may record only selected events, and commercially sensitive information may be concealed. Transparency should therefore be defined relative to the users and decisions involved. Auditors may require access to transaction-level evidence, while suppliers may need access only to their own transactions. Investors may need aggregated information rather than raw supplier data. A well-designed system balances auditability with confidentiality and legitimate limits on information sharing.

The effect on information asymmetry should be measured through observable changes in reconciliation differences, data latency, exception resolution, and the ability of authorized users to independently verify relevant events. Surveys of perceived transparency can complement these measures but should not substitute for them. If users report higher confidence while inventory discrepancies remain unchanged or increase, the result may indicate improved visibility without improved accuracy. This is an important distinction for both researchers and managers.

5.4 Implications for inventory valuation and managerial accounting

Inventory records affect the balance sheet, cost of goods sold, gross margin, working-capital analysis, and performance measurement. Errors in quantity or timing can distort purchase planning and replenishment decisions, while inaccurate valuation can affect profitability and asset values. Blockchain may improve managerial accounting when it connects transaction-level movements with reliable inventory records and supports faster investigation of discrepancies. Managers may be able to identify recurring supplier errors, unusual shrinkage, and delays in receipt confirmation more quickly than under periodic reconciliation processes.

The value of the system depends on whether operational information is converted into action. A dashboard showing repeated quantity discrepancies does not improve performance unless managers investigate root causes, assign responsibility, and change processes. Similarly, a ledger that reveals a delay between dispatch and receipt may support better working-capital decisions only if procurement, logistics, and finance teams coordinate their responses. Technology creates visibility; management routines determine whether visibility becomes better decisions.

Blockchain also does not decide the appropriate inventory valuation method. Cost formulas, net realizable value assessments, overhead allocation, and impairment considerations remain governed by applicable accounting standards and professional judgment. A ledger can improve the provenance of purchase prices, freight costs, and movement records, but it cannot automatically determine whether inventory is obsolete or whether future selling prices justify the carrying amount. Integration with cost accounting and inventory valuation systems is therefore essential.

5.5 Transparency in financial reporting and external audit

The expected link between blockchain and financial reporting transparency runs through the quality and timeliness of underlying transaction data. If purchase, receipt, movement, and sales records can be reconciled more consistently, finance teams may close inventory accounts with fewer manual adjustments. Auditors may be able to trace material transactions with less effort and identify unusual patterns earlier. These improvements can support more timely reporting and reduce some categories of inventory-related error, but only when the ledger captures the relevant transactions and is subject to effective controls.

External auditors must remain independent from management's claims about the technology. A firm's assertion that its blockchain is tamper-resistant should be treated as a claim to be evaluated, not as audit evidence in itself. The auditor should understand the network architecture, the permissions governing transaction entry, the validation process, the treatment of corrections, the reliability of off-chain data, and the controls over interfaces with the general ledger. If a third-party service provider operates the platform, the auditor may need evidence about that provider's controls and the responsibilities retained by the client.

The implementation may also change the distribution of audit risk. Routine transaction tracing could become easier, while IT general controls, cybersecurity, access rights, and automated rules become more consequential. A weakness in a smart contract or interface may affect many transactions consistently, creating a systemic risk. Auditors should therefore consider the scale of automated processing and test the controls that prevent or detect systematic errors. A common ledger can improve auditability, but it can also concentrate risk in the platform and its governance arrangements.

5.6 Privacy, confidentiality, and cybersecurity

Supply-chain records can reveal prices, volumes, customer relationships, production schedules, and supplier dependencies. Publishing all transaction details to all participants may create commercial and privacy risks. Permissioned networks can restrict visibility, but access rules must be carefully designed and independently reviewed. Sensitive information may be kept off-chain, with hashes or references stored on the ledger. This design reduces exposure but makes document retention, access continuity, and off-chain integrity part of the audit trail.

Cybersecurity risks include compromised credentials, stolen cryptographic keys, malicious software, denial-of-service attacks, and vulnerabilities in smart contracts or integration interfaces. Distributed replication may improve resilience against a single point of failure, but it does not guarantee availability or confidentiality. Governance should specify how keys are issued and revoked, how incidents are reported, how software is updated, and how the network recovers from a serious failure. The audit implications of such incidents should be incorporated into the organization's risk assessment.

Privacy and auditability may conflict. An auditor may need access to detailed transaction data, while a supplier may resist sharing commercially sensitive information with competitors. The network should define role-based access and legitimate audit access in advance. Data minimization, retention schedules, contractual protections, and clear dispute procedures can support adoption. These arrangements are not peripheral legal concerns; they shape whether the ledger can deliver a complete and usable audit trail.

5.7 Interoperability and legacy accounting systems

Many firms operate a combination of ERP, warehouse management, transport management, procurement, and supplier systems. A blockchain platform adds value only if the events recorded on the network can be connected to the systems that drive accounting recognition and reporting. If employees must re-enter information manually, the platform may create duplicate records and additional reconciliation work. If identifiers or units differ across systems, the ledger can preserve a consistent event history while leaving the underlying accounting records inconsistent.

Interoperability requires shared data definitions, stable identifiers, clear interface ownership, and exception-handling routines. Companies should determine which system is authoritative for each data element and how conflicting values are resolved. They should also establish whether blockchain records initiate accounting entries, support existing entries, or serve only as external evidence. The choice affects control design, segregation of duties, and the auditor's understanding of how information moves from operational events into the general ledger.

A practical implementation should compare the proposed blockchain architecture with alternatives such as a centralized database, electronic data interchange, digitally signed documents, or a shared cloud platform with strong audit logs. These alternatives may offer lower costs and simpler governance in supply chains with a trusted central coordinator. Blockchain is most defensible when decentralized validation and a common history across independent parties solve a specific problem that simpler tools cannot solve as effectively.

5.8 Implementation economics and organizational readiness

The financial case for blockchain should include total cost of ownership rather than initial software cost alone. Relevant expenses include system development or licensing, integration, migration, data cleaning, cybersecurity, training, supplier onboarding, governance administration, assurance, and ongoing upgrades. Benefits may include lower reconciliation effort, fewer disputes, reduced loss from inventory discrepancies, better audit evidence, and improved decision timeliness. Some benefits accrue to suppliers or customers rather than the implementing firm, which can complicate the business case and require a shared-value arrangement.

Organizational readiness matters because blockchain changes responsibilities and data-sharing practices. Employees may resist a system that makes errors and delays more visible. Suppliers may lack the technical resources to participate. Finance and IT teams may disagree about ownership of data and controls. A phased implementation with clear governance, user training, and defined exception procedures can help manage these challenges. The pilot should focus on a material process with measurable reconciliation costs and should establish a baseline before implementation.

Evaluation should compare actual outcomes against the baseline and a reasonable counterfactual. If reconciliation time falls after implementation but also falls at comparison firms because of a concurrent ERP upgrade, the change cannot be attributed to blockchain alone. If recorded discrepancies rise because the new system detects previously hidden errors, the initial increase may represent better control rather than worse performance. The evaluation should therefore combine outcome metrics with process evidence and document concurrent changes.

5.9 Interpreting the hypotheses and conditions for success

The evidence synthesis supports the plausibility of **H1**: blockchain adoption can improve auditability when it creates a reliable, shared history of material transactions. The strongest mechanism is likely to be improved traceability and easier reconstruction of evidence across organizational boundaries. However, the expected association may be weak when the ledger covers only a small portion of transactions, when data entry is unreliable, or when existing systems already provide efficient reconciliation.

H2 and H3 depend on whether better auditability leads to better inventory records and lower information asymmetry. This transition requires exception resolution, physical verification, and management accountability. A shared ledger that merely records transactions without changing reconciliation and control processes may have little effect on inventory reliability. Similarly, visibility can

increase without reducing asymmetry if access rights are unequal or key supply-chain participants remain outside the network.

H4 reflects the expectation that reduced information asymmetry supports more transparent reporting. Yet reporting timeliness and restatements are affected by many factors, including organizational resources, auditor requirements, regulatory deadlines, and management incentives. These outcomes should be interpreted jointly with more direct indicators of inventory reliability. A reduction in restatements is not necessarily evidence of better reporting if the probability of detecting and correcting errors also declines.

H5 through H7 emphasize boundary conditions. Strong data governance, interoperability, and supplier participation are likely to determine whether the technology's capabilities translate into accounting benefits. H8 recognizes that costs can offset those benefits. The framework therefore rejects a technology-deterministic explanation: blockchain is not expected to improve every outcome in every organization. Its effects should be strongest where the problem is interorganizational record fragmentation, governance is effective, source data are validated, and the ledger is integrated into material accounting processes.

6. DISCUSSION AND IMPLICATIONS

6.1 Theoretical contribution

The framework extends agency theory by treating shared transaction records as a possible monitoring mechanism across organizational boundaries. Traditional accounting controls often operate within one firm, whereas supply-chain inventory evidence depends on events generated by suppliers, carriers, warehouses, and customers. Blockchain may reduce the ability of one participant to alter the shared history unilaterally, but the agency problem persists in the entry, validation, and governance of data. The theoretical contribution is therefore conditional: distributed records can change monitoring costs without eliminating incentives for opportunism.

The information-asymmetry perspective explains why a shared ledger may improve accounting transparency, while transaction cost economics explains when the benefits justify the investment. These perspectives are complementary. Reduced information asymmetry can lower the cost of verifying transactions, but the technology also creates new coordination costs associated with governance, integration, and participation. The net value of adoption depends on whether the system reduces total transaction and assurance costs relative to a feasible alternative.

Institutional theory adds an explanation for symbolic adoption and differences across sectors. Firms may adopt blockchain because customers, regulators, or auditors expect traceability, even when the technology is not well aligned with their processes. The distinction between ceremonial and substantive adoption can be tested by examining process coverage, transaction volume, system integration, and actual use in audit procedures. This approach provides a more informative explanation than classifying firms simply as adopters or non-adopters.

6.2 Managerial implications

Management accountants should participate in blockchain design from the outset, rather than being asked to reconcile its outputs after the system has been deployed. They can help define transaction identifiers, accounting event rules, exception thresholds, inventory valuation interfaces, and evidence-retention requirements. Their role is to ensure that operational traceability connects to cost accounting, working-capital management, and financial reporting. Without this connection, blockchain can remain a logistics technology with limited accounting value.

Management accountants should also develop performance measures that distinguish efficiency from control effectiveness. Reconciliation hours, transaction matching rates, count discrepancies, inventory write-offs, and exception-resolution time can provide a balanced picture. A decline in manual work is useful, but it should not be celebrated if unresolved exceptions increase or physical verification weakens. Balanced measurement encourages management to evaluate whether the system improves both efficiency and reliability. A further responsibility is to assess the economic case. Managers should estimate total implementation costs, identify who receives the benefits, and define how suppliers will participate. Where

smaller suppliers face disproportionate onboarding costs, the focal firm may need to provide technical support or shared infrastructure. A system that excludes critical suppliers may fail to deliver the completeness required for accounting purposes.

Auditors should evaluate blockchain as part of the information system that generates evidence. This includes understanding access rights, validation rules, consensus arrangements, correction procedures, interfaces, and off-chain documents. Auditors should not rely on the ledger's cryptographic features without testing the controls that govern source data and transaction authorization. A strong audit approach combines system testing with substantive procedures targeted to the relevant assertions. Audit firms may need multidisciplinary teams that combine accounting, IT audit, cybersecurity, data analytics, and supply-chain expertise. Such teams can assess whether transaction records are complete, whether interfaces operate as intended, and whether the network's governance is sufficiently robust. Audit procedures may become more continuous or exception-based, but professional judgment remains essential. The auditor must still evaluate whether evidence is relevant, reliable, and sufficient for the audit conclusion.

Assurance providers should also communicate clearly about the scope of work performed. An assurance statement over a platform's cybersecurity controls does not necessarily establish the accuracy of physical inventory data. Assurance over selected transaction logs does not imply that all suppliers or all inventory movements are covered. Clear scope descriptions help users avoid overestimating what blockchain and associated assurance actually demonstrate.

6.3 Implications for technology governance and regulation

Technology governance should assign accountability for data ownership, identity management, platform changes, incident response, and dispute resolution. It should also establish how a participant exits the network, how records remain accessible, and how legal or regulatory retention requirements are met. Because a blockchain network may involve several independent organizations, governance agreements should be in place before the system becomes operationally critical.

Regulators and standard setters can support responsible adoption by clarifying how digital records may be used as audit evidence, how data privacy and retention rules apply, and how responsibility is allocated among network participants. They should avoid implying that one technology automatically produces higher-quality reporting. Technology-neutral principles focused on evidence reliability, controls, traceability, and accountability are more durable than prescriptive preferences for a particular platform.

6.4 Limitations and future research

The main limitation is that the article does not present new firm-level estimates. It develops an evidence-based framework and empirical protocol, but the proposed hypotheses require testing with actual system and accounting data. Future research should obtain multi-year observations from adopters and comparable non-adopters, document the scope and timing of implementation, and measure outcomes before and after deployment. Field access will be challenging because inventory discrepancies, audit adjustments, and system logs can be commercially sensitive.

Further research could compare blockchain with alternative digital infrastructures, including centralized shared databases, electronic data interchange, and digitally signed documents. Such comparisons would clarify whether observed improvements arise from blockchain-specific properties or from broader digitization and process redesign. Studies could also examine continuous auditing, automated confirmations, smart-contract controls, and the interaction between blockchain and Internet of Things sensors, while maintaining a clear distinction between technical traceability and evidence about physical truth.

7. CONCLUSION

This article examines blockchain technology as a potential mechanism for improving supply-chain auditing, inventory reliability, and financial reporting transparency. The central argument is that blockchain can make transaction histories more traceable and harder to alter unilaterally, which may reduce reconciliation effort and information asymmetry across supply-chain participants. These benefits are not automatic. They depend

on the reliability of data at entry, the completeness of network participation, integration with accounting systems, and the effectiveness of governance and internal controls.

The article's principal contribution is to connect blockchain adoption to specific accounting outcomes rather than treating transparency as an abstract benefit. It proposes that adoption intensity improves auditability, that auditability can support inventory reliability, and that data governance, interoperability, supplier participation, and implementation economics condition these relationships. It also emphasizes that blockchain does not replace physical verification, accounting judgment, or professional skepticism. An immutable record can preserve an inaccurate claim; the control environment must establish whether the claim is trustworthy.

For management accountants, blockchain should be evaluated through measurable changes in inventory discrepancies, reconciliation time, exception resolution, and the quality of working-capital information. For auditors, it changes the nature of evidence and the importance of IT controls but does not remove the need for substantive procedures. For executives, the business case should compare blockchain with less complex alternatives and include total cost of ownership. For regulators and assurance providers, the priority is to preserve technology-neutral requirements for evidence reliability, data governance, and accountability.

DECLARATIONS

Author contributions (CRediT). Syamsul Hidayat: Conceptualization, Methodology, Writing – original draft. Ming Sheng Fang: Validation, Supervision, Writing – review & editing.

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of interest. The authors declare no conflict of interest.

Data availability. No new data were created or analysed in this study. Data sharing is not applicable to this article.

Declaration of generative AI use. During the preparation of this work, we used ChatGPT solely for the purpose of checking grammar, proofreading, and improving the linguistic clarity and readability of the manuscript. After using this tool, we reviewed and edited the content as needed and takes full responsibility for the content of the publication.

REFERENCES

- AICPA & CIMA. (2022). Blockchain and accounting: A guide for finance professionals. Association of International Certified Professional Accountants. <https://www.aicpa-cima.com/>
- Alles, M. G. (2022). Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. *Accounting Horizons*, 36(3). <https://publications.aaahq.org/accounting-horizons>
- Appelbaum, D., & Nehmer, R. (2022). Auditing in the digital era: Technology, evidence, and professional judgment. *Accounting Horizons*, 36(3). <https://publications.aaahq.org/accounting-horizons>
- Casino, F., Dasaklis, T. K., & Patsakis, C. (2021). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 63, 101620. <https://doi.org/10.1016/j.tele.2021.101620>
- COSO. (2023). Achieving effective internal control over sustainability reporting (ICSR). Committee of Sponsoring Organizations of the Treadway Commission. <https://www.coso.org/>
- Dai, J., & Vasarhelyi, M. A. (2021). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, 35(2), 5–21. <https://publications.aaahq.org/jis>
- Deloitte. (2021). Blockchain and the supply chain: New opportunities for transparency and efficiency. Deloitte Insights. <https://www.deloitte.com/>
- European Commission. (2021). Proposal for a regulation on harmonised rules on fair access to and use of data (Data Act). <https://eur-lex.europa.eu/>
- European Union Agency for Cybersecurity. (2023). ENISA threat landscape 2023. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>
- EY. (2023). Blockchain technology and the future of finance and supply chain. EY Insights. <https://www.ey.com/>
- Fang, M. S. (2026). The impact of supply chain risk management on financial performance: Evidence from the Southeast Asian manufacturing sector. *Advanced Business Journal*, 2(1), 45–55. <https://doi.org/10.65875/6f1b9z89>
- Financial Action Task Force. (2021). Opportunities and challenges of new technologies for AML/CFT. FATF. <https://www.fatf-gafi.org/>
- GS1. (2021). EPCIS and Core Business Vocabulary standard, version 2.0. GS1. <https://www.gs1.org/standards/epcis>
- GS1. (2022). GS1 standards and blockchain: Traceability and interoperability resources. GS1. <https://www.gs1.org/>
- IAASB. (2022). Technology position: Exploring the use of technology in the audit, with a focus on data analytics. International Auditing and Assurance Standards Board. <https://www.iaasb.org/>

- IBM Institute for Business Value. (2022). Blockchain for supply chain: Trust, transparency and transformation. IBM. <https://www.ibm.com/thought-leadership/institute-business-value>
- IFAC. (2021). Technology and the future of the profession: A resource for professional accountants. International Federation of Accountants. <https://www.ifac.org/>
- IFAC. (2023). Digital transformation and the accountancy profession: Insights and resources. International Federation of Accountants. <https://www.ifac.org/>
- IFRS Foundation. (2021). Effects of climate-related matters on financial statements. Educational material. <https://www.ifrs.org/news-and-events/news/2020/11/educational-material-on-the-effects-of-climate-related-matters-on-financial-statements/>
- ISACA. (2022). Blockchain: A governance and risk perspective. ISACA. <https://www.isaca.org/>
- ISO. (2022). ISO 23257:2022 Blockchain and distributed ledger technologies—Reference architecture. International Organization for Standardization. <https://www.iso.org/standard/75093.html>
- ISO. (2022). ISO 27001:2022 Information security management systems—Requirements. International Organization for Standardization. <https://www.iso.org/standard/27001>
- Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. *International Journal of Production Economics*, 231, 107831. <https://doi.org/10.1016/j.ijpe.2020.107831>
- KPMG. (2022). Technology risk and blockchain: Governance, controls and assurance. KPMG. <https://kpmg.com/>
- Liu, M., Wu, K., & Xu, J. J. (2021). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in Auditing*, 15(2), A19–A29. <https://doi.org/10.2308/CIIA-2020-009>
- Moll, J., & Yigitbasoglu, O. (2021). The role of internet-related technologies in shaping the work of accountants: New directions for accounting research. *The British Accounting Review*, 53(6), 100833. <https://doi.org/10.1016/j.bar.2019.04.002>
- NIST. (2021). Blockchain technology overview. National Institute of Standards and Technology. <https://www.nist.gov/publications/blockchain-technology-overview>
- NIST. (2022). Cybersecurity framework 2.0 concept paper and resources. National Institute of Standards and Technology. <https://www.nist.gov/cyberframework>
- OECD. (2021). The digital transformation of SMEs. OECD Publishing. <https://doi.org/10.1787/bdb9256a-en>
- OECD. (2022). OECD digital security risk management for economic and social prosperity. OECD Publishing. <https://www.oecd.org/digital/>
- OECD. (2023). OECD digital economy outlook 2023. OECD Publishing. <https://doi.org/10.1787/bb167041-en>
- Pontjoharyo, V. I. (2026). How big data analytics influences financial decisions in ASEAN companies? *Advanced Business Journal*, 2(1), 12–21. <https://doi.org/10.65875/mbfj3x61>
- PwC. (2021). Time for trust: The trillion-dollar reasons to rethink blockchain. PwC. <https://www.pwc.com/>
- Queiroz, M. M., Telles, R., & Bonilla, S. H. (2021). Blockchain and supply chain management integration: A systematic review of the literature. *Supply Chain Management: An International Journal*, 26(2), 241–254. <https://doi.org/10.1108/SCM-03-2018-0143>
- Ramadhan, R. A. (2026). How corporate governance influences earnings management: Evidence from Indonesian. *Advanced Business Journal*, 2(1), 1–11. <https://doi.org/10.65875/6rymqy52>
- Rozario, A. M., & Thomas, C. (2021). Reengineering the audit with blockchain and smart contracts. *Journal of Emerging Technologies in Accounting*, 18(1), 21–35. <https://publications.aaahq.org/jeta>
- Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2021). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 59(7), 2117–2135. <https://doi.org/10.1080/00207543.2020.1834728>
- Schmitz, J., & Leoni, G. (2021). Accounting and auditing at the time of blockchain technology: A research agenda. *Australian Accounting Review*, 31(1), 46–55. <https://doi.org/10.1111/auar.12304>
- UNCTAD. (2021). Technology and innovation report 2021: Catching technological waves. United Nations Conference on Trade and Development. <https://unctad.org/publication/technology-and-innovation-report-2021>
- UNCTAD. (2023). Digital economy report 2023: The power of data for development. United Nations Conference on Trade and Development. <https://unctad.org/publication/digital-economy-report-2023>
- W3C. (2022). Decentralized identifiers (DIDs) v1.0. World Wide Web Consortium. <https://www.w3.org/TR/did-core/>
- W3C. (2022). Verifiable credentials data model v1.1. World Wide Web Consortium. <https://www.w3.org/TR/vc-data-model/>
- Wang, Y., Han, J. H., & Beynon-Davies, P. (2021). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Management: An International Journal*, 26(1), 62–84. <https://doi.org/10.1108/SCM-03-2018-0148>
- World Bank. (2021). World development report 2021: Data for better lives. World Bank. <https://www.worldbank.org/en/publication/wdr2021>
- World Bank. (2022). GovTech maturity index, 2022 update. World Bank. <https://www.worldbank.org/en/programs/govtech/gtmi>
- World Bank. (2023). Digital progress and trends report 2023. World Bank. <https://www.worldbank.org/>
- World Bank. (2023). Global economic prospects, June 2023. World Bank. <https://www.worldbank.org/en/publication/global-economic-prospects>
- World Economic Forum. (2021). Redesigning trust: Blockchain deployment toolkit. World Economic Forum. <https://www.weforum.org/>
- World Economic Forum. (2023). Building trust in the digital economy: Blockchain and data governance. World Economic Forum. <https://www.weforum.org/>

World Trade Organization. (2022). World trade report 2022: Climate change and international trade. WTO.
https://www.wto.org/english/res_e/booksp_e/wtr22_e/wtr22_e.htm