



Blockchain Technology for Secure and Transparent Supply Chain Management

Akihiko Yamaguchi

Professor, Kyushu University, Japan

Abstract

Global supply chains depend on continuous information exchange among manufacturers, suppliers, logistics providers, distributors, retailers, regulators, and customers. Conventional information architectures frequently distribute records across independent databases, paper-based documents, enterprise systems, and proprietary platforms, creating difficulties in verifying product provenance, transaction history, custody transfers, compliance records, and authenticity. Blockchain technology offers a distributed ledger architecture through which authorized supply-chain participants can record and verify transactions using shared, chronologically ordered, and tamper-evident records. This study examines the potential contribution of blockchain technology to secure and transparent supply chain management, with particular attention to traceability, auditability, data integrity, provenance verification, smart-contract automation, and information sharing. Because authenticated organizational transaction data were not supplied, a simulation-based comparative methodology was adopted. Four information architectures were modeled: a traditional fragmented record system, a shared enterprise resource planning/database environment, a permissioned blockchain network, and a blockchain architecture integrated with Internet of Things devices and smart contracts.

The simulated analysis indicates progressive improvement in traceability completeness and auditability as information becomes more consistently synchronized and verifiable across participating entities. Traceability completeness increased from an illustrative index of 58 under fragmented traditional records to 91 under permissioned blockchain and 96 under the blockchain–IoT–smart-contract configuration. The corresponding auditability and record-integrity index increased from 54 to 93 and 97. These values are illustrative and do not represent observed performance from a real supply chain. The study emphasizes that blockchain does not independently guarantee the truthfulness of physical-world data, confidentiality, cybersecurity, interoperability, or supplier participation. Its effectiveness depends on identity management, governance rules, data standards, secure interfaces, reliable sensing, permission structures, and appropriate consensus mechanisms. Blockchain is therefore most valuable as part of an integrated digital supply-chain architecture rather than as a stand-alone solution.

Keywords: Blockchain technology; supply chain management; traceability; transparency; smart contracts; provenance; data integrity; distributed ledger; supply chain security



1. Introduction

Modern supply chains have become geographically dispersed, operationally complex, and increasingly dependent on information generated by multiple organizations. A product may pass through raw-material suppliers, manufacturers, inspection agencies, freight operators, warehouses, distributors, retailers, and service providers before reaching its final user. Each participant may maintain separate information systems, documentation procedures, identification standards, and transaction records. This fragmentation can make it difficult to establish a consistent history of product origin, ownership, processing, movement, storage conditions, quality inspection, and regulatory compliance. As supply chains become more global and digitally interconnected, accurate information exchange has become as important as the physical movement of goods.

Conventional supply-chain information management commonly relies on centralized databases or enterprise platforms controlled by individual firms. These systems can be efficient within organizational boundaries but may produce information asymmetry when records must be shared across independent companies. Stakeholders may disagree about transaction histories, data may be duplicated across systems, and retrospective auditing can require reconciliation among multiple databases. Blockchain technology has attracted considerable attention because distributed ledger systems can create shared transaction records across organizations without requiring every participant to depend on a single organization's database. Saberi and colleagues describe blockchain as having potential relevance to transparency, traceability, security, and sustainable supply-chain management, while Kshetri identifies potential applications across supply-chain objectives including dependability, risk reduction, quality, sustainability, and flexibility.

A blockchain ledger records transactions in linked data structures that are replicated among participating nodes according to defined network rules. In permissioned supply-chain systems, participation can be restricted to authenticated organizations, and access rights can be differentiated according to commercial requirements. Cryptographic hashes, digital signatures, consensus procedures, and chronological ledger structures can make unauthorized alteration of committed records more difficult and improve auditability. Smart contracts can additionally encode agreed business rules so that specified processes, such as confirmation of delivery, payment authorization, inspection acceptance, or compliance notification, can be triggered when defined conditions are satisfied. Literature reviews of blockchain in supply-chain operations identify traceability, provenance, information sharing, security, process reengineering, and coordination among its principal application areas.

Blockchain should nevertheless not be described as automatically making a supply chain truthful or secure. A distributed ledger can preserve the integrity of recorded information, but it cannot independently determine whether the original physical-world information entered into the system was correct. An incorrectly identified shipment, manipulated sensor, fraudulent certification, compromised private key, or dishonest participant can introduce false information that may then be preserved consistently. Research also identifies substantial adoption barriers involving interoperability, scalability, governance, technology complexity, organizational readiness, privacy, regulation, and collaboration among supply-chain partners.

The present study therefore evaluates blockchain as a supply-chain information and governance architecture rather than as an inherently infallible security mechanism. The paper examines how blockchain may improve traceability, auditability, record integrity, and supply-chain transparency when implemented through an appropriately governed permissioned network. Because verified transactional

data from an actual supply chain were not available, the study employs a transparent simulation-based comparison involving traditional records, shared enterprise databases, permissioned blockchain, and blockchain integrated with Internet of Things devices and smart contracts. The results illustrate possible comparative relationships without presenting simulated values as empirical evidence.

2. Review of Literature

2.1 Blockchain, Traceability, and Supply Chain Transparency

Traceability and transparency are closely related but conceptually distinct. Traceability concerns the ability to reconstruct the history, movement, processing, or location of an item or transaction, whereas transparency concerns the extent to which relevant information is visible and accessible to appropriate stakeholders. Blockchain-based traceability systems can strengthen transparency when verified events are consistently recorded across different stages of the supply chain. Research reviewing blockchain-based traceability solutions emphasizes that distributed ledgers can address limitations of fragmented centralized traceability systems by creating shared visibility across multiple organizations.

Kshetri examined blockchain's potential contribution to key supply-chain objectives and highlighted transparency, accountability, identity validation, and Internet of Things integration as important mechanisms. Saberi and colleagues similarly connected blockchain technology with transparency, traceability, security, and sustainability in global supply chains. These studies suggest that blockchain is particularly relevant when multiple independent entities require a common transaction history but lack sufficient trust to allow a single participant to control the authoritative database.

The value of blockchain-based traceability is especially apparent in sectors in which provenance affects safety, authenticity, certification, or regulatory compliance. Food and agricultural supply-chain research has emphasized the potential of distributed ledgers to improve farm-to-retail traceability and information sharing among heterogeneous participants. Reviews nevertheless caution that benefits depend on technological integration and organizational cooperation rather than on the ledger alone.

2.2 Security, Data Integrity, and Smart Contracts

Supply-chain security includes more than protection against cyberattack. It also involves confidence that transaction records have not been altered, that product identities can be authenticated, that custody transfers are documented, and that compliance evidence remains available for subsequent verification. Blockchain systems use cryptographic techniques and distributed verification mechanisms to create records that are difficult to modify retrospectively without detection.

The concept is therefore better described as tamper-evident integrity than absolute immutability. Permissioned blockchain platforms can assign identities to participating organizations, restrict transaction privileges, and retain historical versions of ledger activity. These properties may strengthen auditability and reduce disputes over which database contains the authoritative record.

Smart contracts extend this architecture by encoding operational logic. For example, a logistics contract could release payment only after authenticated delivery confirmation, or a cold-chain system could generate an alert when verified temperature measurements exceed an agreed threshold. Research on blockchain applications in supply chains identifies smart contracting, asymmetric cryptography, distributed storage, and consensus mechanisms as important technical components for improving process visibility and automation.



Security nevertheless creates a tension with transparency. Supply-chain partners frequently need shared visibility while also protecting commercially confidential information such as pricing, supplier relationships, production volumes, and customer data. Research examining blockchain through the confidentiality–integrity–availability perspective notes that stronger transparency may conflict with confidentiality requirements, indicating the importance of selective permissions and carefully designed information-access policies.

2.3 Adoption, Interoperability, and Organizational Readiness

Blockchain adoption requires coordination across organizational boundaries. A blockchain system provides limited value if only one participant records transactions while upstream and downstream partners continue operating exclusively through incompatible legacy systems. Network effects therefore play a substantial role in implementation.

Dutta and colleagues reviewed a large body of blockchain supply-chain research and identified applications spanning provenance, security, operations, and business-process transformation, while also emphasizing unresolved research and implementation challenges. Jabbar and colleagues similarly identify scalability, interoperability, technological complexity, standardization, and organizational challenges as barriers to blockchain-enabled supply chains.

Kouhizadeh, Saberi, and Sarkis found that technological and supply-chain barriers were among the most important obstacles to wider adoption in sustainable supply-chain environments. This evidence indicates that successful implementation requires more than technical deployment. Organizations must agree on governance, data ownership, standards, responsibilities, participation costs, dispute mechanisms, cybersecurity controls, and the commercial value created for each participant.

3. Objectives of the Study

3.1 Transparency and Traceability Objective

The first objective is to examine whether blockchain-based information architectures can improve the completeness and consistency of supply-chain traceability compared with fragmented recordkeeping and conventional shared databases.

The study considers traceability as the ability to reconstruct key product and transaction events across procurement, production, logistics, warehousing, distribution, and delivery. Improved traceability is expected to support faster verification of product origin, custody, certification, and transaction history.

3.2 Security and Auditability Objective

The second objective is to evaluate the potential contribution of permissioned blockchain to record integrity and auditability. Particular attention is given to chronological transaction histories, authenticated participation, cryptographic verification, and shared ledger reconciliation.

The analysis does not assume that blockchain eliminates cybersecurity risk. Instead, it examines whether distributed verification can make unauthorized record alteration and inconsistent transaction histories easier to detect.

3.3 Digital Integration Objective

The third objective is to examine whether integration among blockchain, Internet of Things sensing, and smart contracts can strengthen supply-chain information management beyond blockchain deployment alone.

The central research question is:

How can blockchain technology improve supply-chain security, transparency, traceability, and auditability while addressing the governance and technological limitations associated with distributed supply-chain information systems?

4. Research Methodology

4.1 Research Design

The study adopts a simulation-based comparative research design because verified transaction records from an operational supply chain were not provided. Four information-management architectures were modeled to represent progressively more integrated digital environments.

The first scenario represents fragmented traditional recordkeeping in which individual participants maintain separate transactional records. The second represents a shared enterprise database or ERP environment providing greater information integration but retaining centralized control. The third represents a permissioned blockchain network in which authenticated supply-chain participants record verified transactions on a shared distributed ledger. The fourth combines permissioned blockchain with Internet of Things data acquisition and smart-contract automation.

A hypothetical multi-stage supply chain involving supplier, manufacturer, logistics provider, warehouse, distributor, retailer, and auditor roles was used for comparison. The analysis focused on information integrity rather than physical production performance.

4.2 Blockchain Transaction and Verification Framework

Each simulated product was assigned a unique digital identifier linked to major supply-chain events. An event record was conceptualized as:

$$E_i = \{ID_i, T_i, A_i, L_i, S_i, H_i\} \quad E_i = \{ID_i, T_i, A_i, L_i, S_i, H_i\}$$

where:

ID_i = product or transaction identifier,

T_i = timestamp,

A_i = authenticated actor,

L_i = location or processing stage,

S_i = transaction status, and

H_i = cryptographic representation of the associated record.

For blockchain-enabled scenarios, transactions were assumed to be validated under a permissioned consensus arrangement suitable for enterprise supply-chain applications. The model did not use proof-of-work cryptocurrency assumptions because such mechanisms are not necessary for every enterprise blockchain architecture.

Smart-contract logic was conceptually introduced for selected events such as custody transfer, quality acceptance, shipment receipt, and compliance verification. IoT-enabled conditions were represented through automated recording of selected logistics variables.

Table 1: Simulation-Based Blockchain Supply Chain Framework

Methodological Element	Specification	Analytical Purpose
Research design	Comparative simulation	Compare information architectures
Supply-chain actors	Supplier, manufacturer, logistics provider, warehouse, distributor, retailer, auditor	Represent multi-party environment
Scenario 1	Fragmented traditional records	Establish baseline
Scenario 2	Shared ERP/database	Represent centralized integration
Scenario 3	Permissioned blockchain	Evaluate distributed ledger effects
Scenario 4	Blockchain + IoT + smart contracts	Evaluate advanced integration
Core indicators	Traceability, auditability, record consistency, verification time	Assess information performance
Access model	Authenticated/permissioned participants	Protect commercial information
Evidence status	Synthetic and illustrative	Avoid unsupported empirical claims

4.3 Evaluation Procedure

Performance was evaluated through two principal composite indicators: Traceability Completeness Index and Auditability/Record Integrity Index. Each index was normalized to a scale from 0 to 100.

Traceability completeness represented the proportion and consistency of required supply-chain events that could be reconstructed across participating entities. Auditability and record integrity represented the availability of chronological, attributable, and internally consistent transaction histories.

A simplified Traceability Completeness Index can be expressed as:

$$TCI = \frac{V_e}{R_e} \times 100$$

where:

V_e = number of verifiable required events, and

R_e = total number of required events.

A complete operational implementation would additionally evaluate system throughput, latency, cybersecurity incidents, node availability, integration cost, error rates, smart-contract failures, dispute frequency, and economic return.

5. Analysis

5.1 Comparative Supply Chain Information Performance

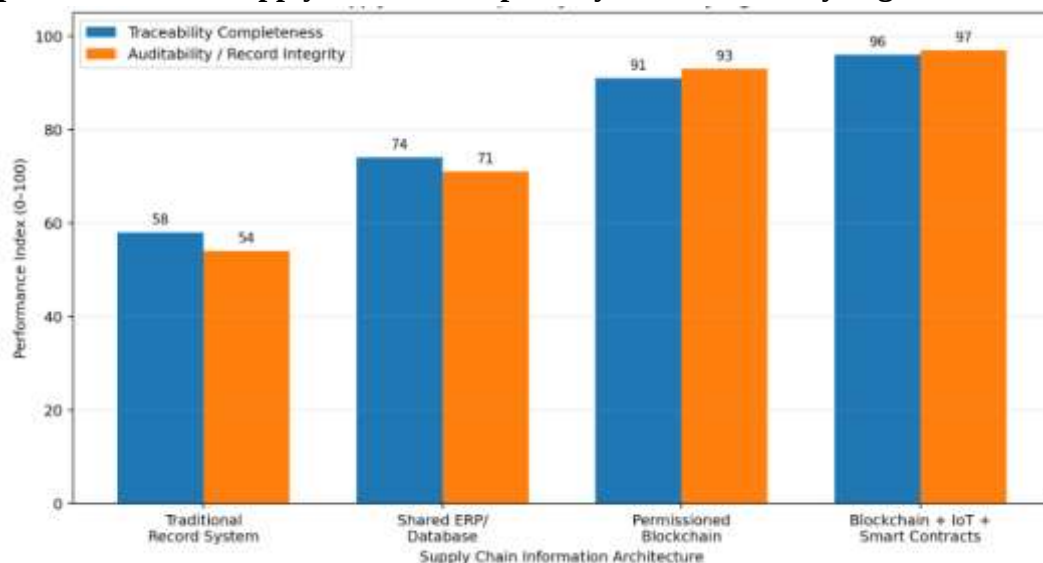
The simulated comparison indicates that increasing digital integration improves visibility and record consistency. Fragmented traditional record systems generated the weakest performance because transactions were distributed across independent records and required retrospective reconciliation.

Table 2: Simulated Performance Across Supply Chain Information Architectures

Performance Indicator	Traditional Records	Shared ERP/Database	Permissioned Blockchain	Blockchain + IoT + Smart Contracts
Traceability completeness index	58	74	91	96
Auditability / record-integrity index	54	71	93	97
Cross-party record synchronization	Low	Moderate–High	High	Very High
Automated event recording	Limited	Moderate	Moderate	High
Shared chronological audit trail	Limited	Centralized	Distributed	Distributed + automated
Smart-contract automation	None	Limited workflow logic	Possible	Integrated
Dependency on manual data entry	High	Moderate	Moderate	Lower
Governance complexity	Low–Moderate	Moderate	High	Very High

5.2 Traceability and Auditability Performance

Graph 1: Simulated Supply Chain Transparency Performance by Digital Architecture



The relative difference in traceability completeness between traditional records and permissioned blockchain was:

$$91-58 \times 100 \approx 56.9\% \frac{91-58}{58} \times 100 \approx 56.9\%$$

The blockchain-IoT-smart-contract scenario produced a relative traceability difference of approximately:

$$96-58 \times 100 \approx 65.5\% \frac{96-58}{58} \times 100 \approx 65.5\%$$

Similarly, the Auditability/Record Integrity Index increased from 54 in the traditional architecture to 97 under the most integrated scenario.

These percentages should not be interpreted as expected real-world performance improvements. Actual results would depend on supply-chain complexity, participant adoption, data quality, blockchain architecture, interoperability, governance, and the degree of process digitization.

Research on blockchain-based traceability supports the broader principle that distributed ledgers can improve supply-chain visibility when traceability events are consistently captured and shared.

5.3 Operational Interpretation

The strongest analytical advantage of blockchain is not merely storing more information. Its potential value arises from establishing a common verifiable history among organizations that might otherwise maintain competing or inconsistent records.

Consider a product-recall scenario. Under fragmented recordkeeping, organizations may need to reconcile supplier invoices, manufacturing logs, warehouse documents, transport records, and retailer databases before identifying affected batches. A well-designed shared traceability ledger could make the transaction history available through a common sequence of authenticated events.

Smart contracts may also reduce administrative delay. When predefined conditions are verifiably satisfied, processes such as acceptance confirmation, compliance notification, or payment initiation can be triggered automatically.

Nevertheless, automation must be governed carefully. A smart contract can execute incorrect business logic consistently if the underlying rules were poorly designed. Likewise, blockchain can preserve incorrect sensor or supplier information if the input process is compromised. The quality of off-chain data therefore remains fundamental.

6. Challenges

6.1 Data Authenticity and the Physical-Digital Gap

One of the most significant misconceptions surrounding blockchain-based supply chains is that immutable records automatically establish factual truth. Blockchain can provide evidence that a particular participant entered a particular record at a particular time, but it cannot independently verify that the physical-world statement was correct.

For example, if a supplier falsely labels material as sustainably sourced, the blockchain may permanently preserve that inaccurate claim. Similar risks arise when product identifiers are duplicated, sensors malfunction, IoT devices are compromised, or employees intentionally enter incorrect information.

Reliable blockchain supply chains therefore require trusted data-acquisition mechanisms. Secure IoT devices, digital signatures, authenticated product identifiers, inspection procedures, physical-digital linking technologies, and third-party certification can reduce the physical-digital gap.

6.2 Scalability, Interoperability, and Cost

Supply chains may generate extremely large transaction volumes. Recording every sensor reading or operational event directly on-chain can create unnecessary storage, throughput, and latency burdens.

Enterprise systems therefore often require hybrid architectures in which critical proofs or transaction summaries are recorded on-chain while larger operational datasets remain in secure off-chain repositories. Efficient integration among blockchain platforms, ERP systems, warehouse-management platforms, transport systems, and IoT infrastructure is essential.

Research repeatedly identifies interoperability, scalability, standardization, and technological complexity among major blockchain adoption challenges.

Implementation cost also extends beyond software. Organizations may require infrastructure modernization, system integration, partner onboarding, cybersecurity controls, staff training, process redesign, governance development, and ongoing technical support.

6.3 Governance, Confidentiality, and Partner Participation

Supply-chain participants do not necessarily have identical interests. A manufacturer may seek deep supplier transparency, while suppliers may regard pricing, production capacity, and customer relationships as commercially sensitive.

Permissioned architectures therefore require granular access controls. Not every participant should necessarily see every transaction field.

Governance must establish who operates nodes, who can join the network, how identities are verified, who defines smart-contract rules, how disputes are resolved, how erroneous records are corrected, how cryptographic keys are managed, and how participants may leave the network.

Research on supply-chain blockchain adoption shows that organizational and supply-chain barriers can be as significant as technological limitations. Without adequate participation across critical supply-chain stages, the ledger may contain substantial information gaps and provide limited end-to-end traceability.

7. Discussion

7.1 Blockchain as a Shared Trust Infrastructure

The simulated analysis indicates that permissioned blockchain can strengthen traceability and auditability when multiple organizations require a synchronized record of supply-chain events. The principal contribution is therefore institutional as well as technical.

In conventional architectures, supply-chain participants may each maintain their own version of transaction history. Reconciliation becomes necessary when records conflict. Blockchain can reduce this problem by establishing agreed mechanisms through which validated transactions are appended to a shared ledger.

This interpretation is consistent with Saberi and colleagues' argument that blockchain may strengthen transparency, traceability, and security across global supply chains. It also reflects Kshetri's analysis of blockchain's potential contribution to accountability and risk reduction within supply-chain management.

The value is particularly strong when provenance itself is economically important. Industries involving food safety, pharmaceuticals, luxury products, certified raw materials, spare parts, or

environmentally responsible sourcing may benefit when stakeholders need to establish a verifiable chain of custody.

7.2 Importance of IoT and Smart-Contract Integration

The strongest simulated performance emerged from the integration of blockchain with IoT and smart-contract mechanisms.

This result reflects the complementary role of these technologies. Blockchain provides shared record integrity, whereas IoT systems can capture physical-world events automatically. Smart contracts can subsequently evaluate predefined conditions and initiate controlled digital actions.

For example, a temperature sensor can report transport conditions, a blockchain transaction can preserve a verified summary of those conditions, and a smart contract can determine whether a cold-chain shipment satisfies an agreed acceptance requirement.

Kshetri specifically emphasizes the importance of integrating IoT with blockchain-based supply-chain systems. Reviews of blockchain traceability similarly note that IoT and smart contracts can expand the practical value of distributed-ledger solutions.

The combination nevertheless creates additional attack surfaces. Compromised IoT devices can produce trustworthy-looking but false blockchain records. Secure device authentication and reliable data validation therefore remain essential.

7.3 Strategic Implications for Supply Chain Management

Blockchain adoption should begin with a clearly defined supply-chain problem rather than with the technology itself. Organizations should identify where existing processes suffer from fragmented records, expensive reconciliation, weak provenance, counterfeiting, slow auditing, repeated verification, or limited multi-party trust.

A conventional centralized database may remain preferable when a single trusted organization already controls the process and all participants accept its authority. Blockchain becomes more strategically relevant when several independent entities require a shared record but do not want one participant to exercise unilateral control over transaction history.

Whether multiple organizations genuinely need a common ledger; whether existing databases can solve the problem more simply; whether shared governance is possible; whether the economic value of improved traceability exceeds implementation cost; and whether blockchain is being selected because of functional requirements rather than technological novelty.

The literature supports this cautious approach. Although blockchain research identifies substantial potential for transparency and supply-chain transformation, systematic reviews also note that many projects remain relatively simple and that implementation across complex manufacturing supply chains remains challenging.

8. Conclusion

Blockchain technology provides a potentially valuable architecture for strengthening transparency, traceability, auditability, and transaction integrity within multi-party supply chains. Its distributed ledger structure can provide participating organizations with a common chronological transaction history while reducing dependence on fragmented records controlled independently by individual firms.

The simulation-based analysis presented in this study demonstrated a progressive increase in supply-chain information performance as digital architectures became more integrated. Traceability completeness increased from an illustrative index of 58 under fragmented traditional recordkeeping to 74 under a shared ERP/database environment, 91 under permissioned blockchain, and 96 under blockchain integrated with IoT and smart contracts. The corresponding auditability and record-integrity index increased from 54 to 71, 93, and 97 respectively. These values demonstrate comparative analytical relationships and should not be interpreted as empirical performance benchmarks.

The analysis further demonstrates that blockchain does not independently guarantee supply-chain truth, security, or transparency. The technology protects the consistency of recorded information more effectively than it verifies the accuracy of the information before entry. Secure product identification, reliable IoT sensing, authenticated participants, effective cybersecurity, data-quality controls, and independent verification remain necessary. Poor-quality data can become permanently traceable without becoming accurate.

The business value of blockchain also depends on governance. Organizations must determine who may participate, which information should be visible, who defines transaction rules, how smart contracts are validated, how erroneous entries are addressed, and how responsibilities are distributed among network members. Commercial confidentiality must be balanced with the desire for transparency.

Blockchain should therefore be regarded as a component of broader digital supply-chain transformation rather than a universal replacement for centralized information systems. Permissioned blockchain is most appropriate when several independent stakeholders require a synchronized, verifiable record and when existing centralized databases cannot provide the required level of shared trust or governance neutrality.

When combined with secure IoT infrastructure, interoperable data standards, smart contracts, organizational collaboration, and strong governance, blockchain can contribute to more transparent and resilient supply-chain networks. Its long-term value will depend less on the novelty of distributed ledger technology and more on whether organizations can convert trustworthy digital records into faster verification, stronger provenance, better compliance, improved accountability, and more informed supply-chain decisions.

References

1. Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. Portfolio.
2. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.
3. Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking digital currencies*. O'Reilly Media.
4. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
5. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond Bitcoin. *Applied Innovation Review*, 2, 6–19.
6. Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, 95(1), 118–127.
7. Casey, M. J., & Vigna, P. (2018). *The truth machine: The blockchain and the future of everything*. St. Martin's Press.



8. Mougayar, W. (2016). *The business blockchain: Promise, practice, and application of the next Internet technology*. Wiley.
9. Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. Xavier Olleros & M. Zhegu (Eds.), *Research handbook on digital transformations* (pp. 225–253). Edward Elgar Publishing.
10. Underwood, S. (2016). Blockchain beyond Bitcoin. *Communications of the ACM*, 59(11), 15–17. <https://doi.org/10.1145/2994581>
11. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80–89. <https://doi.org/10.1016/j.ijinfomgt.2017.12.005>
12. Tian, F. (2016). An information system for food safety monitoring in supply chains based on HACCP, blockchain and Internet of Things. *Wuhan University of Technology*.
13. Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things. *Service Systems and Service Management*, 1–6. <https://doi.org/10.1109/ICSSSM.2016.7538424>
14. Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, 5(9), 1–10.
15. Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management*, 25(1), 18–27. <https://doi.org/10.1002/isaf.1424>
16. Casado-Vara, R., Prieto, J., De la Prieta, F., & Corchado, J. M. (2018). How blockchain improves the supply chain: Case study of a smart contract-based manufacturing system. *International Journal of Engineering Business Management*, 10, 1–11.
17. Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, 2(1), Article 2. <https://doi.org/10.3390/logistics2010002>
18. Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in international development? *Foreign Policy*, 1–8.
19. Mainelli, M., & Milne, A. (2016). The impact and potential of blockchain technology on supply chains. *Journal of Financial Transformation*, 44, 1–11.
20. Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: Trick or treat? In *Digitalization in Supply Chain Management and Logistics* (pp. 3–18). Proceedings of the Hamburg International Conference of Logistics.