

Blockchain-Based Frameworks for Secure Engineering Data Management

Xiaodong Lin

Professor, University of Guelph, Canada

Abstract

The increasing digitization of engineering activities has resulted in large volumes of interconnected data generated through computer-aided design, manufacturing systems, industrial sensors, simulation environments, project management platforms, and digital engineering applications. Although these data support engineering decision-making and operational efficiency, conventional centralized data-management architectures remain vulnerable to unauthorized modification, data loss, access-control failures, and limited traceability. Blockchain technology provides a decentralized and tamper-evident approach for strengthening engineering data management by recording transactions and data-related events within distributed ledgers. This paper examines blockchain-based frameworks for secure engineering data management, emphasizing data integrity, authentication, traceability, access governance, and collaborative information exchange. A conceptual research approach is adopted to examine blockchain mechanisms relevant to engineering environments, including distributed ledgers, cryptographic hashing, smart contracts, consensus mechanisms, and permissioned network architectures. The analysis demonstrates that blockchain can provide stronger accountability and provenance for engineering information while reducing dependence on centralized repositories.

The study further evaluates the role of permissioned blockchain systems in collaborative engineering environments where organizations require controlled participation and confidential information exchange. Results indicate that blockchain-based architectures are particularly valuable for engineering workflows involving multiple stakeholders, including design collaboration, supply-chain coordination, asset lifecycle management, manufacturing records, and maintenance documentation. However, implementation challenges remain associated with scalability, storage requirements, interoperability, computational overhead, privacy, governance, and integration with legacy engineering systems. The paper proposes a conceptual framework that combines blockchain with secure identity management, encrypted off-chain storage, smart contracts, and controlled access mechanisms. The framework provides a foundation for developing trustworthy engineering data ecosystems in which data provenance, accountability, and integrity are continuously maintained. The study concludes that blockchain should be considered a complementary security layer rather than a universal replacement for existing engineering information-management infrastructures.

Keywords: Blockchain technology; Engineering data management; Data security; Distributed ledger; Smart contracts; Data integrity; Engineering information systems; Digital engineering; Traceability; Cybersecurity.

1. Introduction

Engineering organizations increasingly depend on digital information throughout the design, production, operation, and maintenance lifecycle. Engineering drawings, computer-aided design models, simulation outputs, sensor measurements, quality records, maintenance histories, and project documentation are continuously generated and exchanged among engineers, manufacturers, contractors, suppliers, and asset operators. The growing volume and complexity of this information create significant requirements for secure storage, reliable access, traceability, and controlled collaboration. Conventional engineering data-management systems frequently depend on centralized databases and repositories, which can create single points of failure and increase organizational dependence on trusted administrators.

Data integrity is particularly important because engineering decisions frequently depend on the accuracy and historical reliability of digital records. Unauthorized modification of a design specification, manufacturing parameter, inspection record, or maintenance document can potentially affect product quality, safety, cost, and operational performance. Traditional access-control mechanisms can restrict who is allowed to modify information, but they do not always provide an independently verifiable record of every change. Blockchain technology addresses this limitation by maintaining transaction histories through cryptographically linked records distributed across participating nodes. This structure can improve transparency and make unauthorized retrospective modification considerably more difficult.

Blockchain was initially developed as a foundation for digital transactions, but its underlying characteristics have attracted attention across engineering and industrial applications. Distributed ledgers can record events associated with engineering information without requiring all participants to rely on a single centralized authority. Cryptographic hashing supports data integrity, while digital signatures can authenticate transactions and establish accountability. Smart contracts can further automate predefined business and engineering rules, such as approval workflows, document validation, compliance verification, and controlled data-sharing procedures.

Engineering environments, however, differ from public blockchain applications because organizations often require confidentiality, restricted participation, high transaction performance, and integration with established information systems. Permissioned blockchain architectures are therefore particularly relevant because network membership can be controlled while retaining distributed verification and immutable transaction histories. Such systems can support collaboration between organizations without requiring unrestricted access to sensitive engineering information. Blockchain can also be combined with encrypted databases, cloud platforms, digital twins, Internet of Things systems, and enterprise resource-planning environments.

The objective of this study is to examine the potential of blockchain-based frameworks for secure engineering data management and develop a conceptual architecture suitable for collaborative engineering environments. The study focuses on the relationship between blockchain mechanisms and engineering security requirements, evaluates major application areas, and identifies implementation challenges. By integrating blockchain with cryptographic protection, identity management, smart contracts, and secure off-chain storage, the proposed framework seeks to establish a reliable foundation for trustworthy engineering information exchange.

2. Objectives

2.1 Strengthening Engineering Data Integrity

The first objective is to examine how blockchain mechanisms can improve the integrity and authenticity of engineering information. Engineering data may pass through multiple organizational systems during

its lifecycle, creating opportunities for accidental or unauthorized alteration. Blockchain-based records can provide tamper-evident transaction histories that document data creation, modification, approval, and transfer events. This objective therefore focuses on evaluating cryptographic hashes, digital signatures, distributed validation, and immutable records as mechanisms for strengthening confidence in engineering data.

A second dimension of this objective is the improvement of data provenance. Engineering organizations need to understand where information originated, who interacted with it, and when specific changes occurred. Blockchain can establish chronological records of engineering transactions while connecting individual events with authenticated participants. Such capabilities can support audits, quality assurance, regulatory verification, and dispute resolution. The objective is therefore not simply to protect engineering information from unauthorized changes but also to establish a reliable historical record that supports accountability throughout the engineering lifecycle.

2.2 Developing Secure Collaborative Engineering Environments

The second objective is to investigate how blockchain can facilitate secure information sharing among engineering stakeholders. Modern engineering projects frequently involve distributed teams, suppliers, manufacturers, contractors, and external service providers. These participants may use different systems and operate under different organizational policies. Blockchain-based frameworks can provide a shared verification layer while allowing organizations to maintain control over sensitive data. The objective focuses on creating secure mechanisms for authentication, authorization, transaction validation, and controlled information exchange.

The study also aims to identify architectural mechanisms that can make blockchain practical for engineering applications. Rather than storing large engineering files directly on the blockchain, the proposed approach considers encrypted off-chain storage with blockchain-based integrity references. Smart contracts can regulate access and automate approval procedures, while identity-management mechanisms can ensure that only authorized stakeholders participate in transactions. This objective therefore combines security, interoperability, scalability, and governance requirements within a unified engineering data-management framework.

3. Literature Review

3.1 Blockchain and Data Integrity

Blockchain technology provides a distributed mechanism for recording transactions through cryptographically linked blocks. Each block contains information that is connected to previous records, creating a structure in which modification of historical information becomes detectable. Nakamoto introduced the foundational blockchain concept through a decentralized electronic cash architecture, while subsequent research expanded blockchain applications beyond financial transactions.

The security properties of blockchain are largely associated with cryptographic hashing, distributed validation, digital signatures, and consensus mechanisms. These characteristics make blockchain relevant to engineering information systems where data authenticity and historical traceability are important. However, blockchain does not automatically guarantee the correctness of information entered into the ledger. The technology primarily protects recorded information after validation, meaning that secure data acquisition and trusted input mechanisms remain essential.

3.2 Permissioned Blockchain for Engineering Collaboration

Permissioned blockchain networks are particularly appropriate for industrial and engineering environments because participants can be identified and authorized before gaining access to the ledger. Unlike open public networks, permissioned architectures can restrict participation to approved organizations and individuals. This structure can improve confidentiality, reduce unnecessary computational overhead, and support enterprise governance requirements.

Engineering collaboration often involves contractual relationships in which participants need shared visibility of selected events without exposing proprietary information. A permissioned blockchain can provide a common verification layer while allowing confidential engineering files to remain within organizational repositories. This model is especially useful for supply-chain engineering, manufacturing coordination, construction projects, infrastructure management, and maintenance ecosystems.

3.3 Smart Contracts and Engineering Workflows

Smart contracts are programmable mechanisms that execute predefined actions when specified conditions are satisfied. In engineering data management, smart contracts can automate document approvals, verification processes, quality-control procedures, equipment-service records, and data-sharing permissions. Automation can reduce manual intervention and create consistent enforcement of predefined rules.

Smart contracts can also improve accountability because contractual events and workflow decisions can be recorded as verifiable blockchain transactions. Nevertheless, smart contracts must be carefully designed because programming errors or poorly defined business rules can produce incorrect outcomes. Engineering organizations therefore require testing, governance, monitoring, and controlled upgrade mechanisms before smart contracts are deployed in operational environments.

3.4 Blockchain Integration with Engineering Information Systems

Blockchain is unlikely to replace established engineering databases, cloud repositories, product lifecycle-management systems, or enterprise information platforms completely. Instead, integration-based architectures are more practical. Blockchain can serve as a trust and verification layer while existing systems continue to manage large files and computationally intensive engineering information.

This approach is particularly important for CAD models, finite-element simulations, digital-twin datasets, sensor streams, and engineering videos because these datasets can be too large for efficient direct blockchain storage. Hash values, timestamps, ownership information, and access events can be stored on-chain while the actual files remain in encrypted off-chain repositories. Such hybrid architectures combine blockchain's integrity capabilities with the storage efficiency of conventional systems.

4. Methodology

4.1 Research Design

This study adopts a conceptual and analytical research design to examine blockchain-based approaches for secure engineering data management. The methodology focuses on identifying engineering security requirements and mapping them to blockchain mechanisms capable of addressing integrity, authentication, traceability, access control, and collaborative data exchange. Existing scholarly research and established blockchain principles were examined to identify architectural components appropriate

for engineering environments. The analysis considers both technical capabilities and operational limitations to avoid treating blockchain as a standalone solution to all engineering security problems.

The research framework evaluates blockchain from a systems perspective. Engineering data-management requirements are considered across the complete information lifecycle, including data creation, validation, storage, sharing, modification, approval, and archival. Particular attention is given to permissioned networks because engineering organizations generally require controlled participation. The methodology also considers hybrid storage architectures in which large engineering files are maintained off-chain while cryptographic references and transaction records are maintained on-chain. This approach supports both security and practical scalability.

4.2 Blockchain Security Mechanisms

The second methodological component examines the security mechanisms used by blockchain-based engineering architectures. Cryptographic hashing is considered for data-integrity verification, while digital signatures are evaluated for identity authentication and transaction accountability. Consensus mechanisms are assessed in relation to controlled engineering networks, where participants are known and network performance is more important than unrestricted decentralization.

The methodology further considers smart contracts as programmable governance mechanisms. Smart contracts can define conditions for data access, document approval, verification, and information exchange. The study evaluates how these components can work together with identity-management systems and encrypted storage. The resulting analysis provides a conceptual basis for determining which blockchain capabilities should operate directly on-chain and which functions should remain within conventional engineering information systems.

4.3 Engineering Data Management Requirements

The following key requirements were used to evaluate the suitability of blockchain-based engineering data frameworks:

- **Data integrity:** Engineering information should remain verifiable and resistant to unauthorized modification.
- **Authentication:** Every important transaction should be associated with an authenticated participant.
- **Traceability:** Data creation, modification, approval, and transfer events should be auditable.
- **Confidentiality:** Proprietary engineering information should be accessible only to authorized users.
- **Interoperability:** Blockchain systems should communicate with existing engineering and enterprise platforms.
- **Scalability:** The framework should support increasing numbers of transactions and participating organizations.
- **Availability:** Authorized engineering users should be able to access required information reliably.
- **Governance:** Network rules, participant responsibilities, and smart-contract procedures should be clearly defined.

These requirements establish the evaluation criteria for the proposed framework. They also recognize that engineering data security involves more than immutability. A technically immutable record is insufficient if the underlying information was incorrect, improperly classified, or accessed by an unauthorized party before being recorded. Therefore, blockchain is considered one component within a broader security architecture.

4.4 Framework Development

The final methodological stage develops a conceptual framework integrating blockchain with encrypted off-chain storage, identity management, engineering applications, and smart-contract governance. The architecture separates high-volume engineering information from blockchain transaction metadata. When a file is created or modified, its cryptographic hash can be generated and recorded on the blockchain together with information regarding the responsible participant and transaction time.

Subsequent verification can compare the current file hash with the blockchain-recorded reference. Any discrepancy can indicate that the file has changed since the original transaction. Smart contracts can additionally control authorization procedures and trigger workflow actions when predefined conditions are satisfied. The framework therefore establishes a multi-layered architecture in which blockchain provides trust and traceability while conventional systems provide efficient storage and engineering functionality.

5. Analysis

5.1 Blockchain Architecture for Engineering Data Security

A secure engineering data-management framework should combine several complementary layers rather than depend solely on the blockchain ledger. At the application layer, engineers interact with CAD, simulation, manufacturing, maintenance, project-management, and asset-management systems. An integration layer transfers relevant transaction information to the blockchain. The blockchain layer records hashes, timestamps, identities, permissions, and workflow events. An encrypted off-chain layer stores large engineering files.

This architecture enables organizations to preserve the efficiency of existing engineering systems while adding a distributed verification mechanism. For example, when an engineering drawing is approved, the system can calculate its hash and record the hash with the approval event. The complete drawing remains in secure storage. If the drawing is later altered, the new hash will differ from the blockchain record, providing evidence that the file has changed.

Table 1: Core Blockchain Components for Secure Engineering Data Management

Component	Primary Function	Engineering Security Contribution
Distributed Ledger	Records verified transactions	Improves transparency and auditability
Cryptographic Hashing	Generates unique data fingerprints	Detects unauthorized modifications
Digital Signatures	Authenticates participants	Strengthens accountability
Smart Contracts	Automates predefined rules	Controls approvals and access workflows
Permissioned Network	Restricts participation	Protects organizational confidentiality
Off-Chain Storage	Stores large engineering files	Improves scalability and storage efficiency

Component	Primary Function	Engineering Security Contribution
Identity Management	Manages user credentials	Supports controlled access
Audit Layer	Tracks engineering events	Improves provenance and compliance

Interpretation: The table demonstrates that blockchain should be implemented as a combination of complementary mechanisms rather than as a single security technology. Distributed ledgers provide transaction transparency, while hashing protects data integrity and digital signatures establish participant accountability. Permissioned networks are particularly suitable for engineering environments because sensitive information can be exchanged among verified organizations. Off-chain storage addresses the practical limitations associated with storing large engineering datasets directly on a blockchain. Together, these components create a layered security architecture capable of supporting engineering data throughout its lifecycle.

5.2 Applications Across the Engineering Lifecycle

Blockchain-based engineering data management can support multiple stages of the engineering lifecycle. During design, blockchain can document design versions, approval events, and contributor identities. During manufacturing, production parameters, inspection records, and quality-control events can be linked to verified transactions. During operation and maintenance, equipment service histories and component replacements can be recorded in a tamper-evident manner.

The technology is also relevant to engineering supply chains. Components may pass through manufacturers, suppliers, logistics providers, inspectors, and operators. A shared blockchain infrastructure can record important events across organizational boundaries while maintaining an auditable chain of responsibility. This capability can help identify where discrepancies occurred and support more reliable verification of engineering components and documentation.

5.3 Security and Operational Performance

The security benefits of blockchain must be considered alongside operational performance. Blockchain introduces additional processing requirements because transactions must be validated and distributed across participating nodes. Permissioned consensus mechanisms can reduce this overhead compared with public proof-of-work systems, making them more appropriate for enterprise engineering environments.

Table 2: Evaluation of Blockchain-Based Engineering Data Management

Evaluation Dimension	Conventional Centralized Systems	Blockchain-Based Framework
Data Integrity	Depends strongly on administrators	Cryptographically verifiable
Traceability	Often system-dependent	Distributed transaction history
Accountability	Based on access logs	Linked to authenticated transactions

Evaluation Dimension	Conventional Centralized Systems	Blockchain-Based Framework
Collaboration	Requires trusted central repository	Shared verification environment
Confidentiality	Centralized access controls	Permissioned and encrypted access
Scalability	Generally high for databases	Requires architectural optimization
Large File Management	Efficient	Better through off-chain storage
Auditability	Depends on logging configuration	Strong transaction provenance
Governance	Centralized	Shared or consortium-based
Legacy Integration	Usually established	Requires integration mechanisms

Interpretation: The comparison indicates that blockchain provides substantial advantages in integrity, traceability, accountability, and collaborative verification. However, conventional databases can remain more efficient for high-volume data storage and rapid transaction processing. Consequently, a hybrid architecture is more appropriate than complete replacement of existing systems. Blockchain should primarily provide a trusted verification and audit layer, while engineering databases and cloud repositories continue to handle large datasets. This approach balances security improvements with scalability, performance, and organizational practicality.

6. Discussion

6.1 Improving Trust in Engineering Information

Blockchain can significantly strengthen trust in engineering information by providing verifiable records of data-related transactions. In complex engineering projects, stakeholders may have different levels of organizational trust and may use independent information systems. A shared ledger can reduce uncertainty by allowing authorized participants to verify the history of important engineering events. This capability is particularly valuable for design approvals, quality records, manufacturing documentation, and maintenance histories.

The concept of immutable provenance can also improve accountability. When transactions are associated with authenticated participants and timestamps, organizations can determine when a particular engineering event occurred and which authorized participant initiated it. This can strengthen quality management, auditing, and dispute resolution. However, blockchain cannot independently verify whether information entered into the system is factually correct. Reliable input validation therefore remains essential.

6.2 Blockchain for Collaborative Engineering

Modern engineering increasingly involves geographically distributed teams and interconnected supply chains. Collaboration requires secure information exchange without excessive dependence on

centralized intermediaries. Permissioned blockchain networks can provide a shared environment in which participating organizations validate relevant transactions while retaining control over confidential engineering information.

The combination of smart contracts and blockchain can further improve collaborative workflows. Approval requirements, quality checks, delivery conditions, and documentation rules can be encoded into automated processes. This can reduce administrative delays and create consistent workflow execution. Nevertheless, organizational governance must accompany technical automation because engineering responsibilities and contractual relationships cannot always be represented adequately through simple computational rules.

6.3 Integration with Emerging Engineering Technologies

Blockchain can complement emerging engineering technologies such as digital twins, IoT, artificial intelligence, cloud computing, and advanced manufacturing. IoT devices can generate operational records that are cryptographically referenced through blockchain, while digital twins can use trusted provenance information to improve confidence in asset histories. Artificial intelligence systems can also benefit from reliable data lineage because model outputs depend heavily on the quality and origin of training and operational datasets.

The integration of these technologies should nevertheless be carefully designed. Continuous sensor streams can generate enormous transaction volumes that are unsuitable for direct blockchain storage. Instead, aggregated records, event hashes, or selected verification points can be recorded on-chain. This approach preserves blockchain's integrity benefits while limiting computational and storage overhead.

7. Challenges

One major challenge is scalability. Engineering environments can generate extremely large volumes of information through sensors, simulations, manufacturing systems, and digital models. Recording every data point directly on a blockchain would create substantial storage and processing requirements. Hybrid architectures involving off-chain storage, data aggregation, and selective transaction recording are therefore necessary. Engineering organizations must carefully determine which information requires immutable ledger verification and which information can remain within conventional databases.

Another challenge involves privacy and confidentiality. Engineering information frequently contains proprietary designs, manufacturing processes, technical specifications, and commercially sensitive data. Although permissioned blockchain systems restrict network membership, information recorded on a shared ledger may still create confidentiality concerns. Appropriate encryption, access controls, selective disclosure mechanisms, and data-classification policies are therefore required. Organizations must ensure that blockchain transparency does not unintentionally expose sensitive engineering information.

Interoperability also remains a significant concern. Engineering organizations use diverse CAD platforms, product lifecycle-management systems, enterprise applications, cloud services, IoT platforms, and manufacturing technologies. Blockchain systems must communicate with these heterogeneous environments without creating additional data silos. Standardized interfaces, APIs, common data models, and middleware can support integration, but developing these mechanisms may require considerable technical and organizational investment.

Governance represents another important challenge. A consortium blockchain requires agreement regarding participant admission, transaction validation, data ownership, smart-contract updates, dispute resolution, and system maintenance. Different organizations may have conflicting priorities regarding control and responsibility. Without clear governance policies, blockchain adoption can become technically functional but organizationally ineffective.

8. Future Research

Future research should investigate scalable blockchain architectures specifically designed for engineering data workloads. Conventional blockchain approaches may not efficiently support continuous sensor data, large digital models, and high-frequency manufacturing events. Research can explore lightweight consensus mechanisms, hierarchical ledgers, sidechains, layer-two architectures, and event-based recording strategies. These approaches could reduce computational overhead while maintaining verifiable data provenance. Experimental benchmarking using realistic engineering datasets would also help determine transaction capacity, latency, storage requirements, and energy consumption under different deployment configurations.

Another important direction involves integrating blockchain with artificial intelligence and digital twins. Future engineering platforms could use blockchain to verify the provenance of datasets used by AI systems and digital-twin environments. Research should investigate how trusted data histories can improve model reliability, reproducibility, and accountability. Blockchain-enabled digital twins could maintain verifiable records of asset configuration, maintenance events, and operational changes. Such integration may provide a stronger foundation for intelligent engineering systems in which automated decisions depend on trustworthy lifecycle information.

Future studies should also examine interoperability and standardized engineering data governance. Blockchain adoption will remain limited if systems cannot communicate effectively with established engineering platforms. Research can therefore focus on common data schemas, interoperable APIs, decentralized identity frameworks, and standardized smart-contract interfaces. Multi-organization pilot projects involving manufacturers, suppliers, engineering consultants, and asset operators would provide valuable evidence regarding practical adoption. Longitudinal studies could further examine economic benefits, cybersecurity performance, organizational acceptance, and governance effectiveness over extended operational periods.

9. Limitations

This study is conceptual and does not include experimental deployment of the proposed blockchain framework in a live engineering environment. Consequently, the analysis does not provide direct measurements of transaction latency, computational overhead, implementation cost, or long-term system performance. The proposed architecture is derived from established blockchain mechanisms and engineering data-management requirements rather than from a controlled industrial experiment.

A second limitation concerns the diversity of engineering environments. Requirements differ substantially between manufacturing, civil infrastructure, aerospace, energy, automotive, and process engineering organizations. A framework that performs effectively in one sector may require significant modification in another. Future empirical research should therefore validate the framework across multiple engineering domains and organizational structures.

The study also recognizes that blockchain security depends on surrounding technologies and governance processes. Blockchain can provide tamper-evident transaction records, but it cannot

guarantee that incorrect information was not entered initially. Likewise, compromised user credentials, insecure APIs, defective smart contracts, and poorly governed access policies can undermine overall system security. Therefore, blockchain should be evaluated as one component of a broader engineering cybersecurity architecture.

10. Conclusion

Blockchain-based frameworks provide a promising approach for improving the security, integrity, traceability, and accountability of engineering data. The increasing dependence of engineering organizations on digital information has created a need for mechanisms capable of maintaining trustworthy records across complex organizational and technological environments. Blockchain addresses several of these requirements through distributed ledgers, cryptographic hashing, digital signatures, permissioned participation, and smart contracts. These capabilities can strengthen confidence in engineering records and improve visibility across the data lifecycle.

The analysis demonstrates that blockchain is particularly valuable in collaborative engineering environments where multiple stakeholders must exchange information while maintaining accountability. Applications can extend across design management, manufacturing, quality assurance, supply-chain coordination, asset management, and maintenance. However, direct storage of large engineering datasets on blockchain networks is generally impractical. A hybrid architecture combining blockchain-based verification with encrypted off-chain storage offers a more realistic solution. This approach allows engineering organizations to retain existing databases and cloud repositories while introducing a distributed trust layer.

Overall, blockchain should not be viewed as a universal replacement for conventional engineering information systems. Its greatest value lies in strengthening the trust, provenance, and verification capabilities of existing infrastructures. Future implementation should therefore focus on scalable permissioned architectures, interoperability, privacy protection, identity management, smart-contract governance, and integration with digital engineering technologies. With appropriate architectural design and organizational governance, blockchain-based frameworks can contribute to more secure, transparent, and accountable engineering data ecosystems.

References

1. Huang, S., Wang, G., Yan, Y., & Fang, X. (2020). Blockchain-based data management for digital twin of product. *Journal of Manufacturing Systems*, 54, 361–371. <https://doi.org/10.1016/j.jmsy.2020.01.009>
2. Wei, Q., Li, B., Chang, W., Jia, Z., Shen, Z., & Shao, Z. (2022). A survey of blockchain data management systems. *ACM Transactions on Embedded Computing Systems*, 21(3), Article 1. <https://doi.org/10.1145/3502741>
3. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. <https://doi.org/10.1016/j.tele.2018.11.006>
4. Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Management: An International Journal*, 24(1), 62–84. <https://doi.org/10.1108/SCM-03-2018-0148>

5. Pournader, M., Shi, Y., Seuring, S., & Koh, S. C. L. (2020). Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *International Journal of Production Research*, 58(7), 2063–2081. <https://doi.org/10.1080/00207543.2019.1650976>
6. Dutta, P., Choi, T.-M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E: Logistics and Transportation Review*, 142, Article 102067. <https://doi.org/10.1016/j.tre.2020.102067>
7. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117–2135. <https://doi.org/10.1080/00207543.2018.1533261>
8. Kshetri, N. (2017). Can blockchain strengthen the Internet of Things? *IT Professional*, 19(4), 68–72. <https://doi.org/10.1109/MITP.2017.3051335>
9. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
10. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data* (pp. 557–564). IEEE. <https://doi.org/10.1109/BigDataCongress.2017.85>
11. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview (NIST Interagency/Internal Report 8202). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8202>
12. Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications*. Springer. <https://doi.org/10.1007/978-3-030-03035-3>
13. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>
14. Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 4182–4191). <https://doi.org/10.24251/HICSS.2017.506>
15. Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Management: An International Journal*, 23(6), 545–559. <https://doi.org/10.1108/SCM-01-2018-0029>
16. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59, 183–187. <https://doi.org/10.1007/s12599-017-0467-3>
17. Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain technology in business and information systems research. *Business & Information Systems Engineering*, 59, 381–384. <https://doi.org/10.1007/s12599-017-0505-1>
18. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. <https://doi.org/10.1016/j.tele.2018.11.006>
19. Blockchain-based digital twins: Research trends, issues, and future challenges. (2022). *ACM Computing Surveys*. <https://doi.org/10.1145/3517189>