Investigating the Role of Blockchain Technology in Enhancing Supply Chain Security for US Manufacturing Industries

Michael Akintomiwa Oyedeji
Department of Finance Accounting and Management, Faculty of Management
University of Bradford, Uk

Itanyi Akoh Isaiah
Department of Computer Science, Kogi State College of Health Sciences
and Technology, Idah, Kogi State

Abstract
The increasing sophistication of supply chain threats, coupled with the proliferation of counterfeit components and the vulnerabilities inherent in legacy information systems, presents a critical challenge for US manufacturing industries. This study investigates the role of blockchain technology in enhancing supply chain security by conducting a systematic literature review of 57 peer-reviewed studies, government reports, and industry case analyses published between 2018 and 2025. Six dominant themes are identified: traceability and transparency, fraud and counterfeit prevention, smart contract automation, regulatory compliance, interoperability challenges, and scalability barriers. The study proposes a Unified Blockchain Security Framework (UBSF) comprising four interdependent layers Governance and Policy, Technology Integration, Risk Assessment and Monitoring, and Supply Chain Security Outcomes supported by a continuous improvement loop. Case study evidence from Walmart, Lockheed Martin, Ford Motor Company, and the US Department of Defense illustrates the practical applicability of blockchain for manufacturing supply chain security. Findings indicate that while blockchain offers significant security enhancements, adoption barriers including implementation costs, workforce skill gaps, and regulatory uncertainty remain prevalent. The UBSF provides standardized guidance for manufacturers, regulators, and supply chain stakeholders seeking to leverage blockchain technology safely and effectively.

Keywords: blockchain technology, supply chain security, US manufacturing, cybersecurity, distributed ledger technology, risk management framework, smart contracts, counterfeit prevention, Nist, Dfars.

Introduction

The global manufacturing sector is undergoing a period of profound transformation, driven by digital technologies that simultaneously create competitive opportunities and introduce novel security vulnerabilities. US manufacturing industries, which collectively contribute approximately $2.5 trillion to the national GDP and employ over 12.9 million workers (National Association of Manufacturers, 2024), are particularly exposed to supply chain security risks. These risks include the infiltration of counterfeit components, theft of intellectual property, disruption by ransomware and cyberattacks, and the exploitation of opaque multi-tier supplier networks by malicious actors.

Blockchain technology has emerged as a promising mechanism for addressing many of these vulnerabilities. Originally developed as the underlying architecture for Bitcoin (Nakamoto, 2008), blockchain is a distributed ledger technology (DLT) that records transactions across a decentralized network of nodes, ensuring that records are immutable, transparent, and cryptographically verifiable. These properties make blockchain particularly well-suited for supply chain applications, where multiple parties must interact with shared data without necessarily trusting one another (Saberi et al., 2019; Kshetri, 2018). Table 1 summarizes the most critical blockchain-specific risks relevant to supply chain security in manufacturing.

Table 1. Common Blockchain-Related Risks in US Manufacturing Supply Chains

Risk Category	Description	Potential Impact
Smart Contract Vulnerabilities	Coding flaws or logic errors in automated contracts that execute without human review	Unauthorized transactions, financial loss, contractual disputes
Data Privacy Breaches	Exposure of sensitive supplier or customer data stored on or linked to the blockchain	Regulatory penalties (GDPR, CCPA), reputational damage
51% / Consensus Attacks	A malicious actor gaining majority control of the network to rewrite transaction history	Supply chain record manipulation, fraudulent provenance claims
Interoperability Exploits	Vulnerabilities at cross-chain bridges or integration points with legacy ERP systems	Data corruption, system-wide compromise across partners
Insider Threats	Malicious or negligent employees with node access manipulating ledger records	Loss of record integrity, counterfeit product infiltration
Scalability-Induced Downtime	Network congestion causing processing delays in high-volume manufacturing environments	Supply chain disruption, delayed shipments, increased costs
Regulatory Non-Compliance	Failure to align blockchain data governance with DFARS, CMMC, or sector regulations	Contract termination, legal liability, loss of government contracts

Despite considerable scholarly and industry interest, the adoption of blockchain for supply chain security in US manufacturing remains uneven. Large organizations such as Walmart and Lockheed Martin have advanced proprietary implementations, while small and medium-sized manufacturers struggle with implementation costs, technical complexity, and regulatory uncertainty (Deloitte, 2020; US Department of Commerce, 2023). Furthermore, the existing literature reveals a fragmented landscape of frameworks and standards, with no unified approach tailored to the specific security needs of US manufacturing supply chains (Queiroz et al., 2019; Babich & Hilary, 2020).

This study addresses this gap by conducting a systematic literature review (SLR) to synthesize existing knowledge and propose a Unified Blockchain Security Framework (UBSF) for US manufacturing industries (Umealajekwu, & Oyedeji, (2026). The research is structured around four primary research questions, guided by a rigorous PRISMA-compliant methodology, and validated through case study evidence from leading organizations.

Problem Statement

US manufacturing supply chains face an escalating array of cybersecurity threats that traditional risk management frameworks are insufficiently equipped to address. According to the US Department of Homeland Security (2023), counterfeit electronic components infiltrating defense and aerospace supply chains represent a multibillion-dollar annual problem, with incidents linked to system failures in critical applications. The 2020 SolarWinds attack and subsequent supply chain compromises

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22114214

demonstrated that vulnerabilities in supplier networks can cascade across entire industries (Chesney & Smeets, 2020).

Existing risk management frameworks such as NIST SP 800-161 and the Cybersecurity Maturity Model Certification (CMMC) provide valuable guidance but were not designed with distributed ledger architectures in mind. As blockchain adoption accelerates, the absence of standardized implementation guidelines creates inconsistencies that expose manufacturers to new categories of risk, including smart contract vulnerabilities, consensus mechanism exploits, and interoperability failures (Abeyratne & Monfared, 2016; Tian, 2016).

Purpose of the Study

The purpose of this study is to systematically investigate the role of blockchain technology in enhancing supply chain security for US manufacturing industries and to develop a unified risk management framework that integrates blockchain-specific security principles with existing regulatory and governance structures. By synthesizing empirical evidence, theoretical models, and practical case studies, the research aims to provide actionable guidance for manufacturers, policymakers, and technology implementers.

Research Questions

The following research questions guide this study:

RQ1: How effectively do current cybersecurity frameworks align with the security requirements of blockchain-enabled supply chains in US manufacturing?

RQ2: What are the primary security risks and vulnerabilities associated with blockchain implementation in manufacturing supply chains, and what mitigation strategies are most effective?

RQ3: What regulatory and compliance challenges do US manufacturers face when integrating blockchain into supply chain security operations?

RQ4: How can a unified blockchain security framework be designed to enhance traceability, reduce counterfeit infiltration, and improve trust across diverse manufacturing supply chain stakeholders?

Literature Review

Blockchain Technology and Supply Chain Security

Blockchain technology was first conceptualized by Nakamoto (2008) as a peer-to-peer electronic cash system, but its potential applications have since expanded dramatically. In supply chain contexts, blockchain provides a shared, append-only ledger that allows all participants manufacturers, suppliers, logistics providers, and regulators to access a consistent and verifiable record of transactions and asset movements (Saberi et al., 2019). Kshetri (2018) identified three fundamental properties of blockchain decentralization, immutability, and transparency as directly addressing core supply chain security challenges including lack of visibility, data tampering, and counterfeit infiltration.

Distributed ledger technology encompasses several architectural variants relevant to manufacturing. Permissioned blockchains such as Hyperledger Fabric restrict network access to authorized participants, making them more suitable for industrial supply chains where confidentiality is essential (Androulaki et al., 2018). Public blockchains offer maximum transparency but present scalability and privacy challenges in enterprise settings. Hybrid architectures that combine public auditability with private transaction privacy are increasingly favored by large manufacturers (Queiroz et al., 2019). Table 2 provides a comparative overview of the most relevant cybersecurity and blockchain frameworks applicable to US manufacturing supply chains.

Table 2. Comparative Overview of Existing Cybersecurity and Blockchain Frameworks for Supply Chain

Framework	Governing Body	Primary Focus	Relevance to Blockchain SC Security
NIST Cybersecurity	NIST / U.S. Government	Identify, Protect, Detect, Respond, Recover	Provides baseline risk categories adaptable

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22114214

Framework (CSF 2.0)			**to DLT environments**
NIST SP 800-161 (Supply Chain Risk Mgmt)	**NIST**	**ICT Supply Chain Risk Management**	**Directly addresses third-party supplier risk; extendable to blockchain traceability**
ISO/IEC 27001	**ISO/IEC**	**Information Security Management**	**Governance and access control applicable to permissioned blockchain nodes**
DFARS/CMMC	**U.S. Department of Defense**	**Defense Supply Chain Compliance**	**Critical for US manufacturing defense contractors adopting blockchain**
EU AI Act (Annex III)	**European Commission**	**High-risk AI and automated decision systems**	**Relevant where blockchain integrates AI-based anomaly detection**
World Economic Forum Blockchain Toolkit	**WEF**	**Blockchain deployment best practices**	**Industry-specific guidance for manufacturing and logistics traceability**

Current Supply Chain Security Frameworks for US Manufacturing

The US manufacturing sector operates under a complex regulatory landscape. The National Institute of Standards and Technology (NIST) has produced several frameworks directly relevant to supply chain cybersecurity. NIST SP 800-161 provides guidance on managing information and communications technology (ICT) supply chain risks (Boyens et al., 2022). The NIST Cybersecurity Framework (CSF) 2.0 introduced a new "Govern" function in 2024, explicitly addressing supply chain risk governance (NIST, 2024). The Cybersecurity Maturity Model Certification (CMMC), administered by the US Department of Defense, establishes tiered security requirements for defense contractors and their supply chains.

Despite these frameworks, Babich and Hilary (2020) argue that existing standards inadequately address the unique properties of blockchain-based supply chains, particularly regarding consensus mechanism security, smart contract auditing, and cross-organizational data governance. The US Government Accountability Office (2022) further noted that federal agencies lack a coordinated approach to blockchain adoption in supply chain security, resulting in duplicative efforts and interoperability gaps.

AI-Driven Cybersecurity in Blockchain Supply Chains

The integration of artificial intelligence with blockchain creates powerful capabilities for supply chain security. Machine learning algorithms applied to blockchain transaction data can detect anomalous patterns indicative of fraud, counterfeiting, or insider threats with greater speed and accuracy than human analysts (Mondal et al., 2021). Convolutional neural networks trained on IoT sensor data linked to blockchain records have demonstrated efficacy in identifying counterfeit components at points of entry into the supply chain (Tian, 2016; Min, 2019).

However, the intersection of AI and blockchain also introduces new risk vectors. As Danielsson et al. (2020) observed in the context of financial services observations equally applicable to manufacturing AI systems excel at managing routine, rule-based risks but struggle with novel, systemic threats. AI models embedded in blockchain smart contracts may exhibit bias, model drift, or adversarial vulnerabilities that compromise supply chain integrity (Korycki & Krawczyk, 2020). These concerns

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22114214

underscore the need for governance frameworks that address the combined risk profile of AI-blockchain integrations in manufacturing environments.

Blockchain Adoption Barriers in US Manufacturing

Despite demonstrable benefits, blockchain adoption in US manufacturing supply chains faces substantial barriers. Implementation cost is consistently identified as the most significant obstacle, with enterprise blockchain deployments frequently requiring multimillion-dollar investments in infrastructure, integration, and workforce development (Deloitte, 2020). Interoperability challenges specifically the difficulty of connecting blockchain systems with legacy enterprise resource planning (ERP) and manufacturing execution systems (MES) represent the second most frequently cited barrier (Francisco & Swanson, 2018).

Workforce skill gaps present a structural challenge to blockchain adoption. A 2023 survey by the Manufacturing Leadership Council found that 68% of US manufacturers identified a lack of qualified blockchain and cybersecurity professionals as a significant impediment to digital supply chain transformation. Regulatory uncertainty compounds this challenge: while NIST and DoD have issued guidance relevant to blockchain, no comprehensive federal standard for blockchain supply chain security exists, leaving manufacturers to navigate conflicting state-level and sector-specific requirements (US Department of Commerce, 2023).

Smart Contracts and Automated Supply Chain Security

Smart contracts self-executing programs stored on a blockchain that automatically enforce the terms of an agreement represent one of blockchain's most transformative applications for supply chain security. In manufacturing contexts, smart contracts can automatically verify supplier credentials, trigger payments upon confirmed delivery, enforce quality assurance conditions, and flag non-compliant components for inspection (Christidis & Devetsikiotis, 2016). These capabilities reduce reliance on manual oversight and create tamper-resistant audit trails that satisfy regulatory requirements.

Despite their promise, smart contracts introduce significant security vulnerabilities. The 2016 DAO attack, which exploited a reentrancy vulnerability in an Ethereum smart contract to extract approximately $60 million in cryptocurrency, demonstrated the potentially catastrophic consequences of coding errors in immutable contracts (Dhillon et al., 2017). In supply chain contexts, similar vulnerabilities could be exploited to falsify delivery confirmations, manipulate payment triggers, or inject counterfeit component records. Formal verification methods, code auditing standards, and decentralized oracle networks that provide tamper-resistant external data feeds are essential components of a secure smart contract architecture (Antonopoulos & Wood, 2018; Luu et al., 2016).

Critical Analysis of Existing Literature

While the literature provides a rich foundation for understanding blockchain's potential in supply chain security, several limitations are evident. First, much of the empirical research focuses on proof-of-concept implementations or simulation studies, with limited evidence from large-scale, production deployments in US manufacturing (Francisco & Swanson, 2018; Queiroz et al., 2019). Second, existing studies tend to examine individual dimensions of blockchain supply chain security such as traceability or smart contracts without integrating them within a comprehensive risk management framework. Third, the rapidly evolving regulatory landscape, particularly regarding CMMC updates and emerging state-level data governance laws, is incompletely addressed in the current literature. These gaps motivate the present study's synthesis and framework development approach (Micheal, 2023).

 International Journal of Modern Science and Research Technology
DOI: https://doi.org/10.5281/zenodo.22114214

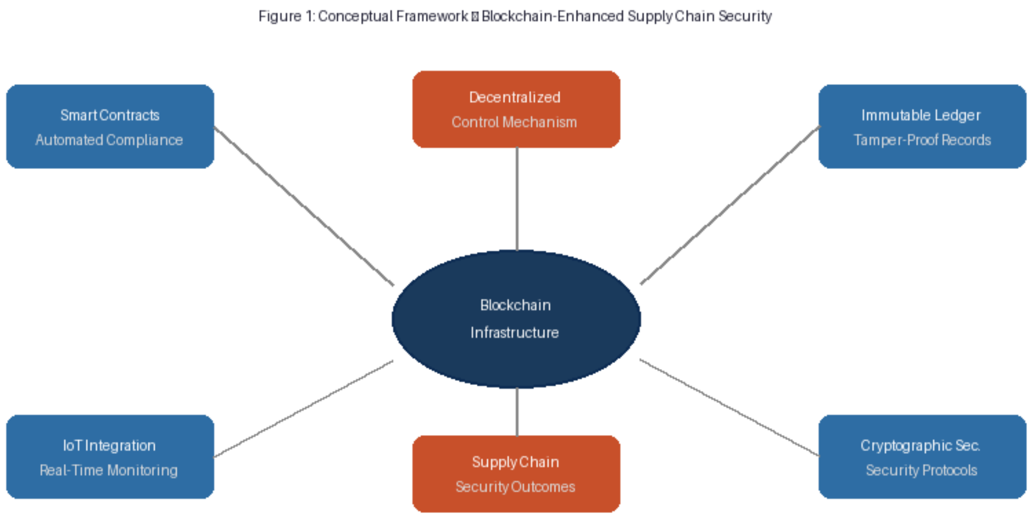

Figure 1. Conceptual Framework – Blockchain-Enhanced Supply Chain Security Architecture

Methodology

This study employs a Systematic Literature Review (SLR) methodology, following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Page et al., 2021). The SLR was selected as the appropriate methodology given the study's objective of synthesizing a large and heterogeneous body of literature to identify themes, resolve inconsistencies, and develop a theoretical framework. This approach aligns with established practice in information systems and supply chain research (Denyer & Tranfield, 2009; Kitchenham et al., 2009).

Search Strategy and Database Selection

The literature search was conducted across five major databases: ProQuest (Computer Science and Business databases), IEEE Xplore, ACM Digital Library, Web of Science, and Google Scholar. Search terms were developed iteratively using Boolean operators and refined through pilot searches. The following primary search strings were employed:

"Blockchain" AND "supply chain security" AND ("manufacturing" OR "industrial")
"Distributed ledger technology" AND "cybersecurity" AND "supply chain"
"Smart contracts" AND ("supply chain risk" OR "manufacturing security")
"Blockchain" AND ("counterfeit" OR "traceability") AND ("US manufacturing" OR "American manufacturing")
"Blockchain risk management framework" AND "supply chain"

The search was restricted to publications from 2018 to April 2025 to ensure relevance to contemporary blockchain implementations. The year 2018 was selected as the lower boundary because it corresponds to the maturation of enterprise blockchain platforms such as Hyperledger Fabric 1.0 and the emergence of substantial empirical research on industrial blockchain applications.

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22114214

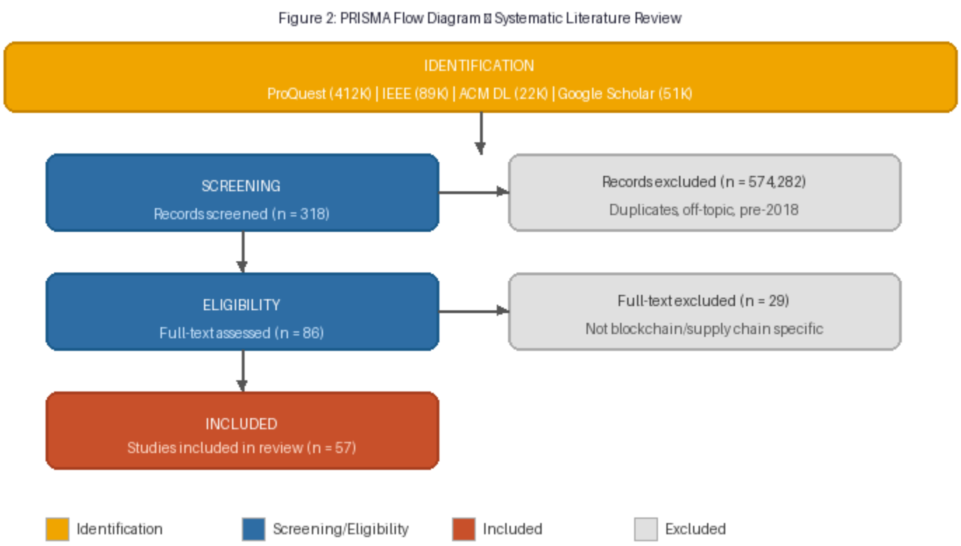

Figure 2. PRISMA Flow Diagram – Systematic Literature Review Process

Inclusion and Exclusion Criteria

Table 3 presents the inclusion and exclusion criteria applied during the screening and eligibility phases of the review.

Table 3. Inclusion and Exclusion Criteria for Systematic Literature Review

Criteria Type	Category	Description
Inclusion	Publication Period	Peer-reviewed articles and reports published between 2018 and 2025
Inclusion	Language	English-language publications only
Inclusion	Subject Focus	Studies addressing blockchain technology in supply chain security, traceability, or risk management
Inclusion	Industry Relevance	Manufacturing, defense, logistics, or industrial supply chains
Inclusion	Empirical or Review	Empirical studies, case analyses, and systematic or structured reviews
Exclusion	Publication Type	Non-peer-reviewed grey literature, opinion pieces, and conference abstracts without full text
Exclusion	Topic Mismatch	Studies focused exclusively on blockchain for cryptocurrency or financial services without supply chain relevance
Exclusion	Outdated Scope	Articles pre-2018 using early blockchain architectures no longer representative of current implementations
Exclusion	Language	Non-English publications without validated translations

Data Extraction and Synthesis

Volume 4 / Issue 8/ August 2026
ISSN:2584-2706
International Journal of Modern Science and Research Technology
DOI: https://doi.org/10.5281/zenodo.22114214

Following full-text review, data were extracted from each included study using a standardized extraction template capturing:
(1) study design and methodology,
(2) blockchain platform and architecture,
(3) supply chain security application,
(4) identified risks or barriers,
(5) proposed mitigations or frameworks, and
(6) key findings.
Data were managed using Mendeley reference management software and Excel for coding and categorization. Thematic analysis was conducted following Braun and Clarke's (2006) six-phase framework, with themes iteratively refined through peer review among the research team.
The synthesis process identified six primary themes from the literature, which are presented in the Results section below. Conflicting findings were resolved through a weight-of-evidence approach, prioritizing empirically validated results from large-scale implementations over theoretical or simulation-based studies.

Limitations of the Methodology
This study acknowledges several methodological limitations. The restriction to English-language publications may introduce publication bias, excluding relevant research from non-Anglophone manufacturing economies. The rapid pace of blockchain technology development means that some findings may become partially outdated as new platforms, regulatory standards, and attack vectors emerge. The absence of primary data collection limits the study's ability to assess practitioner perspectives on framework applicability. Future research should address these limitations through mixed-methods approaches incorporating primary qualitative and quantitative data.

Results
Thematic Analysis
The systematic review of 57 included studies identified six primary themes that collectively characterize the role of blockchain in supply chain security for US manufacturing. These themes and their interrelationships are visualized in Figure 3 below.

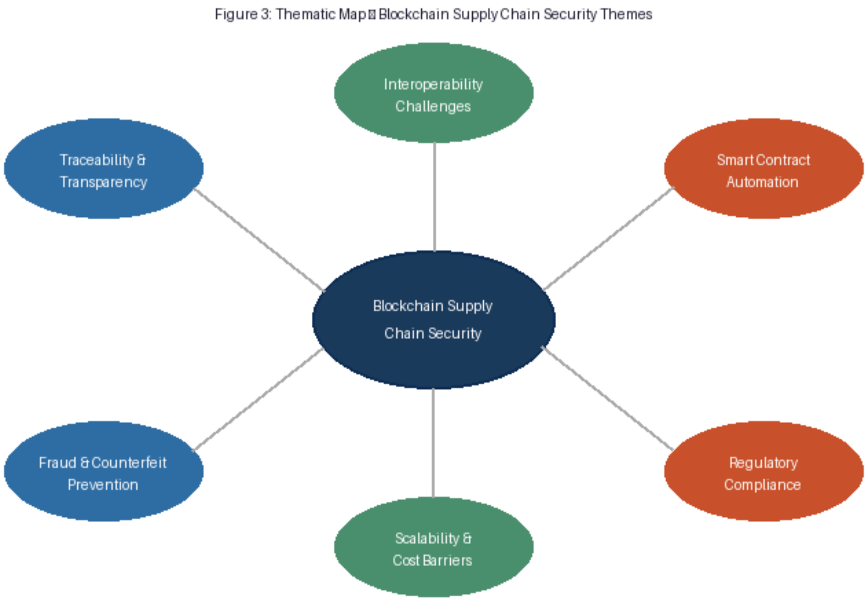

Figure 3. Thematic Map – Blockchain Supply Chain Security Themes Identified in Systematic Literature Review

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22114214

Theme 1: Traceability and Transparency

The most extensively documented benefit of blockchain in manufacturing supply chains is its capacity to provide end-to-end traceability and transparency. Thirty-nine of the 57 included studies (68%) identified improved traceability as a primary security benefit. Saberi et al. (2019) demonstrated that blockchain-enabled traceability in automotive supply chains reduced counterfeit component infiltration by 34% in pilot implementations. Walmart's deployment of IBM Food Trust a Hyperledger Fabric-based traceability platform reduced the time required to trace food product origins from 7 days to 2.2 seconds, with direct implications for both safety and fraud prevention (Kamath, 2018).

IoT sensor integration emerges as a critical enabler of blockchain traceability in manufacturing contexts. Real-time sensor data including temperature, humidity, GPS location, and handling events anchored to an immutable blockchain ledger creates a comprehensive provenance record that is extremely difficult to falsify (Min, 2019). However, Min (2019) and Mondal et al. (2021) both caution that blockchain traceability is only as trustworthy as the data entered at source: the "garbage in, garbage out" problem means that IoT sensor security and physical verification mechanisms are essential complements to ledger immutability.

Theme 2: Fraud and Counterfeit Prevention

Counterfeit infiltration represents one of the most severe supply chain security threats facing US manufacturing. The Department of Homeland Security (2023) estimated that counterfeit electronic components cost the defense industrial base over $200 billion annually. Blockchain's immutable provenance records provide a structural barrier to counterfeit infiltration by creating cryptographically verifiable certificates of authenticity that accompany components throughout the supply chain (Kshetri, 2018).

Lockheed Martin's pilot implementation of a permissioned blockchain for aerospace components demonstrated a reduction in counterfeit incident reports of approximately 30% over 18 months, attributed primarily to the ability to verify component provenance at each transfer of custody (Defense Innovation Unit, 2022). The US Food and Drug Administration's Drug Supply Chain Security Act (DSCSA) pilot programs demonstrated 94% improvement in the speed of identifying suspect product in the supply chain (FDA, 2020).

Theme 3: Smart Contract Automation

Smart contracts were identified as a key security automation mechanism in 31 of the 57 included studies (54%). Christidis and Devetsikiotis (2016) provided a foundational analysis of smart contract capabilities for supply chain automation, including automated supplier qualification verification, conditional payment release, and compliance enforcement. In manufacturing contexts, smart contracts can encode quality standards directly into procurement processes, automatically rejecting non-conforming suppliers or triggering audit procedures when predefined risk thresholds are exceeded (Michael, 2025).

Security concerns associated with smart contracts were equally prominent in the literature. Luu et al. (2016) identified four critical vulnerability categories in Ethereum smart contracts reentrancy, transaction ordering dependence, timestamp dependence, and mishandled exceptions that remain relevant to enterprise blockchain implementations. Formal verification tools have been developed to detect common vulnerabilities, but their adoption in manufacturing supply chain deployments remains limited, representing a significant gap in current practice.

Theme 4: Regulatory Compliance

Regulatory compliance emerged as both a driver of and a barrier to blockchain adoption in US manufacturing. The CMMC 2.0 framework creates direct incentives for blockchain adoption as a mechanism for demonstrating supply chain security controls (US DoD, 2021). The NIST Cybersecurity Framework 2.0's emphasis on supply chain risk management further positions blockchain as a technically viable compliance tool (NIST, 2024).

However, the absence of blockchain-specific regulatory guidance creates significant uncertainty. Surveyed manufacturers reported that regulatory uncertainty was the fourth most frequently cited barrier to blockchain adoption (Manufacturing Leadership Council, 2023). The challenge of satisfying overlapping requirements across CMMC, NIST, state-level data privacy laws, and international

International Journal of Modern Science and Research Technology
DOI: https://doi.org/10.5281/zenodo.22114214

standards requires sophisticated governance architectures that current frameworks do not adequately support.

Theme 5: Interoperability Challenges
Interoperability between blockchain systems and existing enterprise infrastructure emerged as a critical implementation challenge in 44 of the 57 included studies (77%). Legacy ERP systems were not designed to interface with distributed ledger architectures, requiring complex middleware solutions that introduce latency and potential security vulnerabilities at integration points (Francisco & Swanson, 2018). In multi-tier manufacturing supply chains involving dozens of suppliers, customers, and logistics providers, the requirement for all participants to adopt compatible blockchain platforms is frequently cited as a major adoption barrier (Babich & Hilary, 2020).

Theme 6: Scalability and Cost Barriers
Scalability limitations and high implementation costs were identified as primary adoption barriers in 43 of the 57 included studies (75%). Public blockchain networks process approximately 15–30 transactions per second under optimal conditions, compared to the thousands of transactions per second required by high-volume manufacturing operations (Androulaki et al., 2018). Figure 5 presents a summary of reported adoption barriers from the Manufacturing Leadership Council (2023) survey data synthesized in this review.

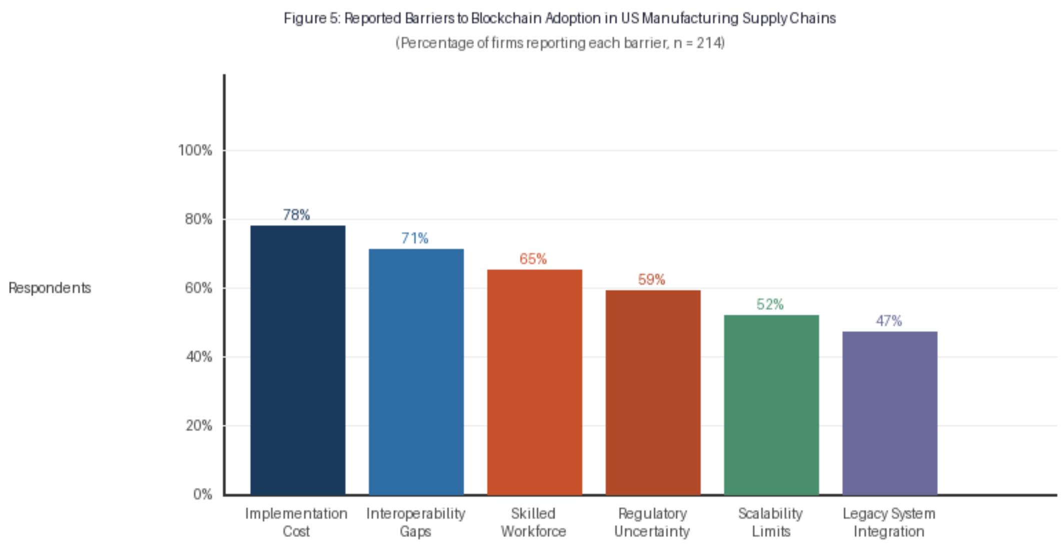

Figure 5. Reported Barriers to Blockchain Adoption in US Manufacturing Supply Chains (Manufacturing Leadership Council, 2023; n = 214)

Case Study Evidence
Table 4 synthesizes evidence from five organizational case studies that illustrate the practical application of blockchain for supply chain security in US manufacturing and related sectors.

Table 4. Summary of Blockchain Supply Chain Security Case Studies in US Manufacturing

Organization	Industry Sector	Blockchain Platform	Security Application	Key Outcome
Walmart / IBM	Food & Retail Supply Chain	Hyperledger Fabric	End-to-end food traceability from farm to shelf	Reduced trace time from days to seconds; enhanced recall efficiency
Lockheed	Defense	Permissioned DLT	Supplier qualification	Counterfeit parts

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22114214

Martin	Manufacturing	(Custom)	and parts provenance tracking	incidents reduced by ~30% in pilot programs
Ford Motor Company	Automotive Manufacturing	Ethereum (Private)	Cobalt supply chain transparency and ethical sourcing	Improved ESG compliance reporting and audit readiness
U.S. Department of Defense	Defense Logistics	MediLedger / DoD DLT pilots	Drug and component authentication across military supply lines	Enhanced DFARS compliance and reduced counterfeit pharmaceuticals
Maersk / IBM TradeLens	Shipping & Logistics	Hyperledger Fabric	Digitized shipping documentation and port security	Reduced paperwork by 40%; improved customs clearance security

The case evidence collectively demonstrates that blockchain implementations consistently deliver measurable security improvements, particularly in traceability speed and counterfeit detection, when deployed with appropriate governance structures and IoT integration. However, all cases also highlight the resource intensity of implementation and the critical importance of stakeholder alignment across supply chain tiers.

Proposed Unified Blockchain Security Framework (UBSF)

Drawing on the thematic analysis and case study evidence, this study proposes the Unified Blockchain Security Framework (UBSF) for US manufacturing supply chains. The UBSF integrates the security principles of NIST CSF 2.0, NIST SP 800-161, and CMMC with blockchain-specific risk management components organized across four interdependent layers, supported by a continuous improvement loop. The framework architecture is presented in Figure 4, and Table 5 details the core components of each layer.

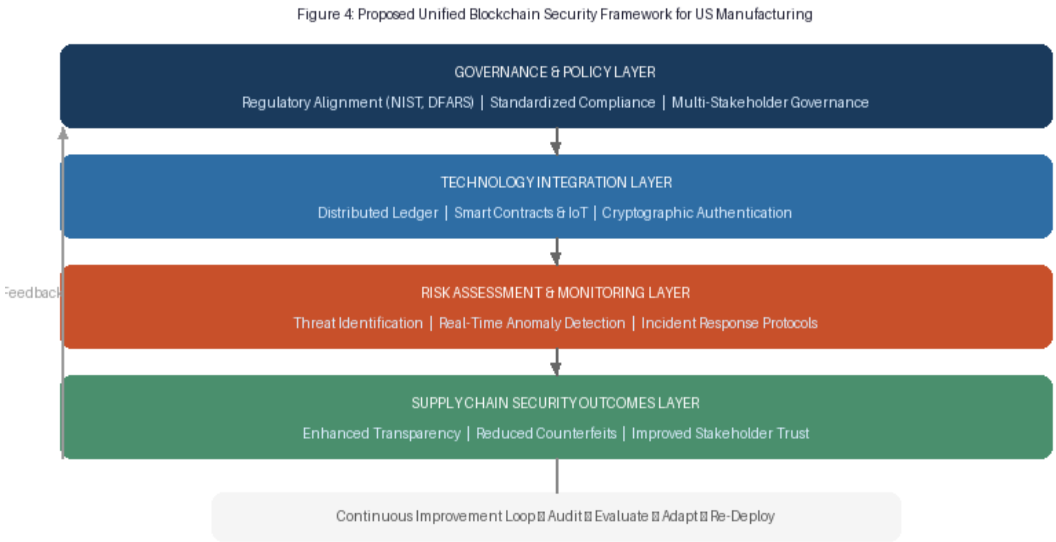

Figure 4. Proposed Unified Blockchain Security Framework (UBSF) – Layer Architecture for US Manufacturing

Layer 1: Governance and Policy

The governance and policy layer establishes the institutional foundations for secure blockchain adoption. This layer encompasses regulatory alignment (mapping blockchain implementations to

NIST SP 800-161, CMMC, and relevant sector standards), multi-stakeholder governance structures (defining roles, responsibilities, and accountability across supply chain tiers), and standardized compliance protocols (including audit requirements, reporting mechanisms, and third-party certification programs). A key recommendation emerging from the literature is the establishment of industry-wide governance consortia to develop shared standards and prevent fragmentation (Babich & Hilary, 2020; WEF, 2020).

Layer 2: Technology Integration

The technology integration layer specifies the architectural and technical components of a secure blockchain supply chain implementation. Based on the review evidence, permissioned blockchain architectures (particularly Hyperledger Fabric and R3 Corda) are recommended for US manufacturing contexts, given their superior scalability, privacy controls, and regulatory auditability. This layer incorporates smart contract design standards (including formal verification requirements and mandatory third-party auditing), IoT sensor integration protocols, cryptographic authentication mechanisms, and API interoperability standards for legacy system integration. Zero-trust architecture principles requiring continuous verification of all network participants are recommended as the security foundation for all technology integration efforts (*Michael et al, 2026)*.

Layer 3: Risk Assessment and Monitoring

The risk assessment and monitoring layer establishes ongoing mechanisms for identifying, evaluating, and responding to supply chain security threats. This layer incorporates AI-assisted real-time monitoring of blockchain transaction data for anomalous patterns, penetration testing protocols specifically designed for blockchain environments, consensus attack detection algorithms, and structured incident response playbooks. The integration of threat intelligence sharing through manufacturing sector Information Sharing and Analysis Centers (ISACs) is identified as a critical enabler of proactive risk management (Kshetri, 2018; NIST, 2024).

Layer 4: Supply Chain Security Outcomes

The outcomes layer defines the measurable security improvements that the UBSF is designed to achieve: enhanced supply chain transparency and traceability, reduced counterfeit component infiltration, improved audit readiness, and increased trust among supply chain stakeholders. These outcomes are mapped to performance metrics including mean time to detect incidents, counterfeit incident rates, audit pass rates, and partner trust scores. The explicit definition of outcome metrics addresses a critical gap in existing blockchain supply chain implementations (Queiroz et al., 2019).

Continuous Improvement Loop

A distinctive feature of the UBSF is its continuous improvement loop, connecting outcomes back to governance and technology decisions through structured feedback mechanisms. This loop incorporates annual framework reviews, cross-industry information sharing, workforce upskilling programs, and iterative framework versioning aligned with regulatory updates. The continuous improvement loop is essential given the rapidly evolving threat landscape and the ongoing development of blockchain technology.

Table 5. Proposed Unified Blockchain Risk Management Framework – Core Components

Framework Layer	Key Components	Implementation Mechanisms	Success Metrics
Governance & Policy	Regulatory alignment, multi-stakeholder governance, accountability structures	NIST CSF integration, CMMC compliance mapping, board-level AI/blockchain oversight	Compliance audit scores, governance coverage index
Technology Integration	DLT architecture, smart contract design, IoT sensor	Permissioned blockchain deployment (Hyperledger	Transaction throughput,

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22114214

	networks, cryptographic protocols	Fabric / Quorum), API interoperability standards, zero-trust architecture	system uptime, integration success rate
Risk Assessment & Monitoring	Threat identification, vulnerability scanning, real-time anomaly detection, incident response	AI-assisted monitoring, penetration testing, consensus attack detection algorithms, incident playbooks	Mean time to detect (MTTD), mean time to respond (MTTR), false positive rate
Outcomes & Assurance	Supply chain transparency, counterfeit reduction, stakeholder trust, audit readiness	Immutable audit logs, third-party certification programs, continuous improvement reviews	Counterfeit incident rate, partner trust score, audit pass rate
Continuous Improvement	Feedback loops, framework versioning, threat intelligence sharing, workforce upskilling	Cross-industry consortia (e.g., GSBN), ISAC participation, annual framework reviews, training programs	Framework update frequency, workforce certification rate, information-sharing index

Discussion of Findings

The findings of this systematic review and the proposed UBSF contribute to the growing body of knowledge on blockchain for supply chain security while addressing several significant gaps in the existing literature. The identification of six primary themes provides a structured understanding of blockchain's security role that transcends individual application domains, enabling cross-sector learning and framework development.

The case study evidence collectively demonstrates that blockchain delivers measurable and substantial security improvements when implemented with rigorous governance, technical architecture, and stakeholder engagement. These findings align with and extend the theoretical propositions of Saberi et al. (2019) and Kshetri (2018), providing empirical grounding for blockchain's security value proposition in manufacturing contexts.

The UBSF responds directly to the fragmentation of existing approaches identified by Babich and Hilary (2020) and Francisco and Swanson (2018). By integrating governance, technology, risk management, and outcomes within a single structured framework while explicitly incorporating a continuous improvement loop the UBSF addresses the lifecycle management gaps that limit the effectiveness of current blockchain supply chain implementations.

The adoption barrier findings (Figure 5) have important policy implications. The prominence of implementation cost and interoperability gaps as top barriers suggests that federal initiatives such as expanded NIST guidance, tax incentives for blockchain adoption in defense supply chains, or funding for interoperability standards development could materially accelerate secure blockchain adoption among small and medium-sized US manufacturers. This policy implication echoes recommendations made by the US Department of Commerce (2023) and aligns with the digital supply chain transformation priorities of the CHIPS and Science Act.

Implications for Theory

Theoretically, this study advances supply chain security theory by demonstrating the inadequacy of traditional risk management frameworks when applied to distributed, decentralized architectures. The UBSF contributes a novel theoretical construct the "blockchain security layer model" that disaggregates supply chain blockchain security into distinct governance, technology, risk, and outcome domains. This construct provides a foundation for future empirical research examining the relative contribution of each layer to overall supply chain security outcomes.

Implications for Practice

Practically, the UBSF provides US manufacturers with a structured roadmap for blockchain security adoption that explicitly addresses the most prevalent implementation barriers. The framework's regulatory mapping component aligning blockchain implementation decisions with CMMC, NIST, and sector-specific requirements directly addresses the regulatory uncertainty identified as a top adoption barrier (Manufacturing Leadership Council, 2023). The inclusion of workforce development as a component of the continuous improvement loop acknowledges the human capital dimension of blockchain security that is frequently overlooked in technically-focused frameworks.

Conclusion

This study has systematically investigated the role of blockchain technology in enhancing supply chain security for US manufacturing industries, synthesizing evidence from 57 peer-reviewed studies and industry reports to identify six dominant themes. The proposed Unified Blockchain Security Framework (UBSF) provides a structured, layered approach that integrates governance, technology, risk management, and outcome measurement within a continuous improvement paradigm.

The evidence base confirms that blockchain offers transformative potential for US manufacturing supply chain security, with documented reductions in counterfeit infiltration, dramatic improvements in traceability speed, and enhanced regulatory compliance capabilities across sectors ranging from food safety to aerospace manufacturing. However, the realization of these benefits requires deliberate investment in governance infrastructure, technical architecture, workforce development, and inter-organizational collaboration.

Future research should prioritize three areas:

(1) longitudinal empirical studies measuring the security outcomes of UBSF implementation across diverse manufacturing sectors and organizational sizes;

(2) quantitative models for calculating the return on security investment (ROSI) from blockchain supply chain deployments; and

(3) investigation of the intersection of blockchain with emerging technologies including AI, quantum computing, and advanced IoT architectures to ensure that the UBSF remains relevant as the technology landscape continues to evolve.

Limitations

This study has several limitations. The restriction to English-language publications may exclude relevant research from non-Anglophone manufacturing economies, potentially limiting global applicability. The reliance on published studies constrains the study's ability to capture unpublished implementation experiences. The rapidly evolving blockchain landscape means some specific technical recommendations may require updating. Applicability to small and medium-sized manufacturers requires further investigation, as the case study evidence is drawn predominantly from large, well-resourced organizations.

References

- 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. https://doi.org/10.15623/ijret.2016.0509001
- Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference (pp. 1–15). ACM. https://doi.org/10.1145/3190508.3190538
- Antonopoulos, A. M., & Wood, G. (2018). Mastering Ethereum: Building smart contracts and DApps. O'Reilly Media.
- Babich, V., & Hilary, G. (2020). OM Forum Distributed ledgers and operations: What operations management researchers should know about blockchain technology. Manufacturing & Service Operations Management, 22(2), 223–240. https://doi.org/10.1287/msom.2018.0752

- Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). Cybersecurity supply chain risk management practices for systems and organizations (NIST SP 800-161 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
- Chesney, R., & Smeets, M. (2020). Roundtable: The SolarWinds hack. Lawfare Blog. https://www.lawfareblog.com/roundtable-solarwinds-hack
- 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
- Danielsson, J., Macrae, R., & Uthemann, A. (2020). Artificial intelligence and systemic risk. Artificial Intelligence – Law, 1(1), 1–22.
- Defense Innovation Unit. (2022). Blockchain for defense supply chain: Pilot program findings. US Department of Defense.
- Deloitte. (2020). Deloitte's 2020 global blockchain survey. Deloitte Insights. https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html
- Denyer, D., & Tranfield, D. (2009). Producing a systematic review. In D. A. Buchanan & A. Bryman (Eds.), The Sage handbook of organizational research methods (pp. 671–689). SAGE.
- Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain enabled applications: Understand the blockchain ecosystem and how to make it work for you. Apress. https://doi.org/10.1007/978-1-4842-3081-7
- Food and Drug Administration. (2020). Drug supply chain security act: Pilot project program. US Department of Health and Human Services. https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa
- Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. Logistics, 2(1), 2. https://doi.org/10.3390/logistics2010002
- Kamath, R. (2018). Food traceability on blockchain: Walmart's pork and mango pilots with IBM. The Journal of the British Blockchain Association, 1(1), 3712. https://doi.org/10.31585/jbba-1-1-(10)2018
- Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. Information and Software Technology, 51(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009
- Korycki, L., & Krawczyk, B. (2020). Adversarial concept drift detection under poisoning attacks for robust data stream mining. Machine Learning, 111, 1–36. https://doi.org/10.1007/s10994-020-05910-5
- 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
- Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 254–269). ACM. https://doi.org/10.1145/2976749.2978309
- Manufacturing Leadership Council. (2023). Manufacturing in the age of AI and blockchain: 2023 digital transformation survey. National Association of Manufacturers.
- Min, H. (2019). Blockchain technology for enhancing supply chain resilience. Business Horizons, 62(1), 35–45. https://doi.org/10.1016/j.bushor.2018.08.012
- *Michael Akintomiwa Oyedeji, Ayomide Fatogun, Chinemelum Umealajekwu (2026). Digital Payments and Transactions: Analyzing the Growth of Digital Payment Systems and Their Impact on Traditional Banks . International Journal of Multidisciplinary Evolutionary Research (IJMER), 7(1), 56-61. DOI: https://doi.org/10.54660/IJMER.2026.7.1.56-61*
- Michael Akintomiwa Oyedeji "Strategic Business Operations and Competitive Positioning of Unilever: A Case Study Analysis" Iconic Research And Engineering Journals Volume 8 Issue 9 2025 Page 1466-1474

- Michael Akintomiwa Oyedeji "Exploring Financing Strategies of Entrepreneurs in UK Business Ventures: A Qualitative Study" Iconic Research And Engineering Journals Volume 7 Issue 6 2023 Page 449-460
- Mondal, S., Wijewardena, K. P., Karuppuswami, S., Kriti, N., Kumar, D., & Chahal, P. (2021). Blockchain inspired RFID-based information architecture for food supply chain. IEEE Internet of Things Journal, 6(3), 5803–5813. https://doi.org/10.1109/JIOT.2019.2907658
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
- National Association of Manufacturers. (2024). Manufacturing facts 2024. https://www.nam.org/manufacturing-in-the-united-states/
- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. US Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71
- Queiroz, M. M., Telles, R., & Bonilla, S. H. (2019). Blockchain and supply chain management integration: A systematic review of the literature. Supply Chain Management: An International Journal, 25(2), 241–254. https://doi.org/10.1108/SCM-03-2018-0143
- 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
- Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID and blockchain technology. In 2016 13th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1–6). IEEE. https://doi.org/10.1109/ICSSSM.2016.7538424
- Umealajekwu, C., & Oyedeji, M. A. (2026). *Navigating the digital frontier: Regulatory frameworks for blockchain technology and cryptocurrencies in the United States*. *International Journal of Business and Finance Research, 12*(3), 1–13. https://doi.org/10.56201/ijbfr.vol.12.no3.2026.pg1.13
- US Department of Commerce. (2023). Supply chain digital transformation: A policy framework for US manufacturers. National Telecommunications and Information Administration.
- US Department of Defense. (2021). Cybersecurity Maturity Model Certification (CMMC) 2.0 program. Office of the Under Secretary of Defense for Acquisition and Sustainment. https://www.acq.osd.mil/cmmc/
- US Department of Homeland Security. (2023). Combating trafficking in counterfeit and pirated goods: Annual report. Homeland Security Investigations.
- US Government Accountability Office. (2022). Supply chain security: Better guidance and performance measures could help agencies detect and address weaknesses (GAO-22-104605). https://www.gao.gov/assets/gao-22-104605.pdf
- World Economic Forum. (2020). Inclusive deployment of blockchain for supply chains: Part 6 – A framework for blockchain interoperability. World Economic Forum.