Journal of Innovation & Knowledge 10 (2025) 100744

Contents lists available at ScienceDirect

Journal of Innovation & Knowledge

journal homepage: www.elsevier.com/locate/jik

An innovative supply chain solution for information management in cyber resilience: Blockchain technology

Ava Hajian [a], Saba Rezaeinejad [b], Kiarash Rayman [c,*], Sajad Khorsandroo [d]

[a] Department Business Information Systems and Analytics, Willie A. Deese College of Business and Economics, North Carolina A&T State University, NC 27411, USA
[b] Department of Supply Chain Management, G. Brint Ryan College of Business, University of North Texas, Denton, TX 76203, USA
[c] Department of Marketing and Supply Chain Management, Willie A. Deese College of Business and Economics, North Carolina A&T State University, NC 27411, USA
[d] Department of Computer Science, College of Engineering, North Carolina A&T State University, NC 27411, USA

ARTICLE INFO

JEL code:
O00

Keywords:
Transparency
Sales and operations planning
Blockchain
Cyber resilience
Experiment

ABSTRACT

Blockchain is an innovative solution for many supply chain (SC) issues. This study presents empirical and theoretical evidence to address the following research question: *How can blockchain impact the information flow in SCs to enhance cyber resilience*? The practice-based view provides theoretical support for the presented model. This study presents a conceptual model that includes hypothesized relationships. Empirical data are collected via a vignette-based, between-subject experimental design study. Blockchain-based SCs can improve sales and operations planning (S&OP) by allowing firms to align plans and processes to achieve cyber resilience during cyber disruptions. This study offers empirical evidence that blockchain contributes to transparency by giving SC decision makers access to high-quality data during cyber disruptions, which can lead to improved cyber resilience performance. The contribution of this study is twofold. First, this research explains the impact of blockchain on the information flow of the SC to create cyber resilience through two mediating variables: transparency and S&OP. Second, this study provides empirical evidence, including a detailed experimental methodology, to explore the role of blockchain in SC information management, particularly in enhancing transparency and cyber resilience.

Introduction

Blockchain technology represents an innovative solution for information systems by introducing a decentralized and secure framework for data management, which can result in the transformation of traditional practices in transparency and cyber resilience (Aslam et al., 2021). The blockchain distributed ledger system ensures that all transactions and data entries are immutable, verifiable, and accessible to authorized stakeholders, which improves trust and accountability across networks (Sizan et al., 2025). In the context of transparency, blockchain reduces information silos and enables real-time data sharing, thereby empowering organizations to track processes and materials with unprecedented clarity (Cao et al., 2022). For cyber resilience, blockchain's cryptographic algorithms and decentralized architecture significantly mitigate the risks of data breaches and cyberattacks, as no single point of failure exists (Zkik et al., 2024). Organizations can revolutionize their information systems by integrating blockchain, which can result in innovation management and the creation of resilient frameworks for handling complex challenges in the digital era.

In information systems, transparency has become a significant concern in supply chains (SCs) due to growing societal awareness. Transparency concerns require innovative solutions and efficient knowledge management. SC transparency involves open sharing of information regarding both internal and external factors, such as the origin of raw materials and working conditions for employees, among all members of the SC. In societal concerns, the forced labor issue can be mitigated in SC through transparency. Moreover, transparency can contribute to firm performance such as resilience and efficiency (Montecchi et al., 2021). SC transparency can be a risk management strategy to improve resilience by providing high-quality information for decision makers. However, owing to the sensitivity of supply information, focal firms are reluctant to share their business information (e.g., product development, daily profit, and production cost), which is a barrier in achieving transparency objectives in SCs (Montecchi et al.,

* Corresponding author.
E-mail addresses: ahajian@ncat.edu (A. Hajian), Saba.Rezaeinejad@unt.edu (S. Rezaeinejad), krayman@ncat.edu, kiarash.rayman@outlook.com (K. Rayman), skhorsandroo@ncat.edu (S. Khorsandroo).

https://doi.org/10.1016/j.jik.2025.100744
Received 7 November 2024; Accepted 27 May 2025
Available online 3 June 2025

2021).

Past empirical works have explored antecedents and outcomes of transparency, for example, SC analytics (Zhu et al., 2018) and SC structure (Zhu et al., 2018). However, previous studies have underestimated the role of emerging technologies in enabling SC transparency, particularly when cyberattacks occur (Zelbst et al., 2020). Disasters and disruptions have accelerated SC digitalization, consequently making companies more vulnerable to cyberattacks. More empirical research is needed to elucidate the impact of emerging technologies, such as blockchain, on transparency and their consequences for enhancing cyber risk management. Blockchain is an innovative practice that firms can employ to improve SC capabilities and performance (Bromiley & Rau, 2014). Blockchain can contribute to knowledge management. Therefore, the current study addresses the following research question: *How can blockchain impact the information flow in SCs to enhance cyber resilience*? Through a review of related literature, we address the research question by presenting a research model that includes hypothesized relationships. The practice-based view (PBV) provides theoretical support for the presented model (Bromiley & Rau, 2014). Empirical data are collected via a vignette-based between-subject experimental design study. Findings reveal that blockchain technology is an innovative solution to improve cyber resilience through two new mediators.

The contribution of this study is twofold. First, this study explains the impact of blockchain as an innovative solution on the information flow of the SC and knowledge management to create cyber resilience. In response to Industry 4.0, which aims to combine disruptive technologies with smart operations and SC management (SCM), we examined its impacts on information flow through transparency and sales and operations planning (S&OP); these two capabilities can considerably impact performance (Goh & Eldridge, 2019; Jonsson et al., 2021). This study builds upon previous research by introducing two mediating factors that explain how blockchain can influence SC resilience through improved information flow. Second, this study provides empirical evidence, including a detailed experimental methodology, to explore the role of blockchain in SC information management, particularly in enhancing transparency and cyber resilience (Ghadge et al., 2020).

Literature review

We used ProQuest and Google Scholar databases to find recent empirical studies related to the research question based on the keywords "transparency," "visibility," "blockchain," and "resilience."

Blockchain

As an innovative SC solution, blockchain is the main contributor to zero-trust cybersecurity and knowledge management, which can improve cyber resilience. A blockchain consists of blocks of data that chronologically record transaction withina secure and trustworthy environment, which is safeguarded by cryptographic techniques (Sizan et al., 2025). The blockchain enables financial transactions between SC members while serving as an inventory system and registry for recording, tracing, monitoring, and transacting assets (Sadeghi et al., 2023). Blockchain-based systems offer a high level of security in distributed data in knowledge management by which SC decision makers can be improved. Several studies review past blockchain works on operations and SC management, for example, Shukla et al. (2024) and Sizan et al. (2025).

Previous research has examined the positive effects of blockchain on improving logistics operations (Aslam et al., 2024) and SCM practices (Aslam et al., 2021) to enhance operational performance and efficiency. Blockchain adoption positively impacts SC visibility and sustainable organizational performance (Sun et al., 2022). Furthermore, blockchain improves credit reporting and enterprise credit information sharing in SC finance with the help of new consensus mechanisms (Zheng et al., 2022). Previous research has identified The influence of blockchain in disaster management and SC resilience. For example, Javadpour et al. (2023) proposed a disaster framework including blockchain and Internet of things (IoT), which was tested with simulation models. Past studies have focused on the potential of blockchain to improve SC performance. However, more empirical research is needed to explain how blockchain can impact complex SC activities such as S&OP and transparency (Jonsson et al., 2021), which is addressed in the current study.

Sales and operations planning (S&OP)

S&OP is an integrated process to align demand, supply, and financial planning, which is in a company's master planning (Goh & Eldridge, 2019). S&OP is developed from manufacturing resource planning (MRP) as a replacement for aggregate production planning (Singhal & Singhal, 2007). S&OP supports executive-integrated decision-making (Pereira et al., 2020) to balance the total demand with company resources. S&OP integrates tactical decisions across functions and SCs, ultimately aligning daily operations with a long-term strategy for effective planning. For more details, we refer interested readers to previous works that review S&OP in operations and SCM such as Pereira et al. (2020).

Previous studies have examined the role of S&OP in three main categories: antecedents, design, and implementation (Kreuter et al., 2022). For example, Laari et al. (2023) investigated the effects of redundancy and monitoring strategies on the procurement ability to balance demand and supply in S&OP, in which co-management of procurement was influential. Swaim et al. (2016) focused on antecedents of S&OP, including integration, organizational priorities, standardized processes, and engagement. Moreover, Goh and Eldridge (2019) examined the impact of coordinating mechanisms of S&OP (e.g., procedure and schedule) on SC performance. However, incorporating information technologies, for example, blockchain, into S&OP needs more research, particularly when cyber resilience is a business focus.

Supply chain transparency

SC transparency refers to sharing high-quality specific business data in an SC relationship (Wang et al., 2023). SC information flow management comprises concepts of information sharing, visibility, transparency, and traceability. These concepts have been used interchangeably in previous studies (Montecchi et al., 2021). We distinguished these concepts using three main categories: quality, type, and relationship. Information sharing refers to sharing a low quality of general business data in a business-to-business (B2B) relationship, for example, logistics costs and tax data between suppliers and buyers (Sahin & Robinson Jr., 2005). Visibility refers to sharing high-quality specific business data in a B2B relationship, for example, suppliers' location and materials data between suppliers and buyers (Williams et al., 2013). Previous research provides a relatively comprehensive review of visibility types, which can clarify the differences between these concepts (Swink et al., 2024). Transparency refers to sharing a high quality of specific business data in an SC relationship, for example, suppliers' location, itemized costs, and materials data between suppliers, manufacturers, buyers, retailers, and customers (Wan et al., 2023). Traceability refers to sharing a medium quality of general organizational data in a public relationship, for example, sharing suppliers' countries, employees' demographic information, and benefits data with the public (Skilton & Robinson, 2009). Traceability is sometimes called external transparency in operations and SCM.

A well-established SC relationship can share a high quality of information, thus resulting in transparency (Sunny et al., 2020). Transparency positively impacts subsystems' monitoring, which can improve SC performance (Sunny et al., 2020). The availability and accessibility of business data between SC members considerably impact the change capability by which SCs can address disruptions (Feizabadi et al., 2019). Zhu et al. (2018) provided empirical evidence for the positive effect of

SC analytics on transparency in SCs. Zelbst et al. (2020) explored the relationship between transparency and technologies such as radio frequency identification, industrial IoT, and blockchain in technology-based practices. Moreover, Wang et al. (2023) explored the relationship between transparency and suppliers' provision of trade credit, in which two moderating effects were considered: market share and corporate social responsibility.

Multiple reviews of transparency have been conducted to contribute to future studies (Montecchi et al., 2021) such as blockchain-based SCs (Sunny et al., 2020). However, few empirical studies consider the role of transparency in blockchain-based SCs, for example, Zelbst et al. (2020), mainly when cyber resilience is a focus for improvement.

Supply chain cyber resilience

SC resilience involves finding an appropriate match between an SC's risk exposure and the corresponding readiness level to handle those risks (2024). SC risk is the uncertainties and potential disruptions in managing the flows from suppliers to customers, and arises from various factors such as natural disasters, supplier bankruptcy, transportation delays, and information security breaches. The resilience concept focuses on how well the SC performs against risk. Christopher and Peck (2004) considered a risk as a system's capacity to restore an original state or adapt to a more favorable state after being disrupted. Similarly, SC cyber resilience focuses on cyberspace as the SC's capacity to recover from the consequences of cyberattacks and data breaches (O. Khan & Estay, 2015). Resilience focuses on product flows, while cyber resilience includes information flow and cyberspace. For more comprehensive information, we refer interested readers to review papers on blockchain in cyber resilient SCs (e.g., Shukla et al. (2024)). However, more empirical research on supply chain cyber resilience (SCCR) is needed, particularly when the role of technologies such as blockchain is a focus.

Theoretical lens: practice-based view

Previous research papers have applied the PBV to explain the effects of copyable practices on performance improvement. Humanitarian SC agility and resilience are considered imitable and easily transferred practices, ultimately influencing humanitarian SC performance (Dubey et al., 2022). Khan et al. (2023) applied PBV to explain the effects of sustainable SC practices on a company's environmental, social, and economic performances. Similarly, generative artificial intelligence usage has been examined as a practice that contributes to sustainable SC performance (Li et al., 2024). In the same vein, Liu et al. (2023) adopt the theoretical lens of PBV and demonstrate that circular manufacturing practices contribute to financial and environmental performances in manufacturing companies. Digital transformation practices offer operational performance improvement, such as workforce productivity, physical asset efficiency, and working capital efficiency in manufacturing firms (Tian et al., 2023). Likewise, digital SC practices improve operational performance through SC viability as an intermediate outcome (Yu et al., 2024).

Theoretical lens and hypothesis development

The PBV explains a phenomenon in which replicable activities or practices are frequently accessible to the public and can be adopted by various firms (Bromiley & Rau, 2014). In the context of PBV theory, company performance differences are connected to the activities or routines the company carries out (Bromiley & Rau, 2016). The PBV emerged from the resource-based view (RBV). However, the RBV explains a firm's competitive advantage through specific resources that are not imitable, while the PBV focuses on copyable practices influencing firms' performance (Barney, 1991). While the RBV emphasizes the importance of tangible and intangible resources as sources of competitive advantage, how these resources are applied, transformed, or leveraged in day-to-day organizational practices is not sufficiently addressed (Bromiley & Rau, 2016). In RBV, resources are rare and not copyable. By contrast, the PBV focuses on the role of organizational practices, routines, and processes as the mechanisms through which practices are effectively utilized and capabilities are developed (Bromiley & Rau, 2014). Blockchain technology is a copyable practice, which can be implemented by any organization.

Blockchain technology is an information-based practice, a copyable method by other firms to improve SC performance such as resilience management. Blockchain-based information systems can positively affect cyber resilience by improving capabilities in SCM networks. According to the PBV, capability, for example, transparency and S&OP, refers to an organization's capacity to accomplish a task. Capabilities arise from the interplay of practices, including established procedures (Bromiley & Rau, 2014). The impact of practice on performance may flow through mediating variables (Bromiley & Rau, 2016). Therefore, our proposed research model explains how blockchain as a practice can contribute to transparency and S&OP capabilities to improve SC cyber resilience as performance.

Blockchain and S&OP

Blockchain can impact S&OP components: demand forecasting, operations planning, and financial planning (Pereira et al., 2020). Blockchain can provide immutable and distributed data blocks that ensure real-time information flow for demand prediction and operational decisions in S&OP (Sunny et al., 2020). Distributed databases in blockchain-based SC help SC members to collaborate on operational planning (Cao et al., 2022). In addition, incorporating smart contracts within blockchain enhances financial transactions in S&OP processes. Blockchain can contribute to S&OP in terms of data accuracy and smart contracts. S&OP relies on accurate data for forecasting demand and planning production. Blockchain's capability to provide real-time, unalterable data significantly reduces the risks of errors, which can result in reliable planning processes. For example, Walmart practices blockchain to track the movement of goods from suppliers to distribution centers in real time, which ensures that S&OP teams have up-to-date information.

De Beers, which is the world's largest diamond producer, implemented a blockchain-based platform that provides a tamper-proof and permanent record of every diamond's journey from mine to retail (Bambysheva & Castillo, 2024). This creates high trust among stakeholders, thus reducing disputes and streamlining operations. Blockchain facilitates S&OP processes by providing a platform for transparent information sharing, enhancing coordination, and aligning goals across the SC. Developed by Maersk and IBM, TradeLens is a blockchain-enabled shipping solution that allows all parties involved in the SC to access real-time shipping data (Paris, 2019). For S&OP, this means that companies can adjust their sales and production plans based on the latest information about shipping delays and customs clearance times.

Smart contracts automate routine transactions and enforce compliance with agreed-upon terms, thereby reducing lead times and operational bottlenecks. In S&OP, this means more efficient order fulfillment, procurement processes, and compliance management, thus allowing for smoother operations and more accurate planning. In the food and beverage industry, companies such as Nestlé have experimented with blockchain to automate payments and agreements with suppliers through smart contracts (Nash, 2018). Accordingly, we formulate the following hypothesis:

H1. Blockchain-based supply chains are positively associated with sales and operations planning (S&OP).

Blockchain and supply chain transparency

SC structure can positively contribute to transparency. Blockchain attributes (e.g., traceability, immutability, distributed database, and private blockchain) can contribute to SC transparency. A total of three categories of transparency are identified: history (e.g., tracking and tracing), operations (e.g., collaborative planning in logistics), and strategy (e.g., cooperative innovation) transparency. Blockchain traceability enables transparency through tracing and tracking (Sunny et al., 2020). The immutable and distributed characters of blockchain can help achieve operations transparency and collaborative SC planning among participants (Sunny et al., 2020). Similarly, strategy transparency can be improved with private blockchains protecting sensitive business information.

Owing to the immutability of the blockchain, any transaction recorded on it remains unalterable and permanent, which contributes to maintaining a clear historical record of past information actions (Shukla et al., 2024). Blockchain's traceability is employed across various sectors to monitor products, raw materials, and operations, for example, manufacturing SCs.

Blockchain's immutable distributed database can help increase operations transparency. Operations transparency involves sharing information between SC parties, thereby enabling them to coordinate and synchronize their activities. In a blockchain-based SC, activities by any network member are visible and must be authenticated by all other participants, which can result in transparency throughout the entire network. The origin of every action remains evident and permanent across the SC network, ultimately ensuring transparent operations.

A private blockchain network comprises familiar partners who share mutual trust, which can contribute to strategy transparency and can positively impact such transparency between close members of the SC network. Previous empirical research has investigated the influence of blockchain on SC transparency; for example, Zelbst et al. (2020) presented the contribution of technological solutions, including blockchain, to advancing SC transparency. Accordingly, we formulate the following hypothesis:

H2. Blockchain-based supply chains are positively associated with supply chain transparency.

S&OP and supply chain cyber resilience

Previous empirical works have suggested that S&OP can contribute to risk management (Dittfeld et al., 2021). Moreover, S&OP can make a plan to mitigate risks in the dynamic business environment (Tavares Thomé et al., 2012).

S&OP can contribute to cyber resilience in terms of anticipation, maintenance (resistance), and recovery. Cyber resilience can be improved by threat detection, which is built on S&OP prediction capability. S&OP can develop cyber maintenance in which SCs can quickly adopt changes (Jonsson et al., 2021). During the recovery stage, S&OP can quickly provide financial and operational plans for scenarios.

S&OP processes necessitate a comprehensive overview of the SC, that is, visibility. The BMW automotive company uses its S&OP process to map out its entire SC network. This visibility is essential to identifying cyber vulnerabilities. By clearly understanding the entire SC, organizations can implement targeted cybersecurity measures where they are most needed, thereby enhancing overall cyber resilience. S&OP involves close coordination between various organizational departments and external partners (suppliers, logistics providers) (Kazmi & Ahmed, 2022). This collaborative approach fosters a culture of information sharing and joint problem-solving. Regarding cyber resilience, such collaboration ensures that cybersecurity measures are integrated into every aspect of the SC, from the initial design of products and services to the delivery to customers. Furthermore, it enables a rapid, coordinated response to cyber incidents, consequently minimizing their impact.

A key goal of S&OP is to create a flexible and responsive SC that can quickly adapt to changes in demand, supply, and other external conditions (Dittfeld et al., 2021). An SC that can quickly adjust its operations in the face of a cyberattack (such as rerouting shipments if a logistics provider's systems are compromised) is less likely to experience significant disruptions. Flexibility in operations and planning allows for contingency strategies that are vital for cyber resilience. S&OP relies on data for forecasting, planning, and decision-making (Kreuter et al., 2022). The same data can be analyzed to predict and identify potential cyber threats, such as unusual activity patterns that could indicate a breach or an attack in progress. By leveraging data analytics within S&OP, companies can enhance their ability to detect and respond to cyber threats more effectively. Blockchain is a practice that can impact firms' capacity, for example, S&OP, which results in performance improvement such as cyber resilience. Therefore, we formulate the following hypotheses:

H3. Sales and operation planning (S&OP) is positively associated with supply chain cyber resilience.

H3a. Blockchain-based supply chains improve sales and operations planning (S&OP), which results in creating a mediation pathway of cyber resilience.

Supply chain transparency and supply chain cyber resilience

Essential steps to evaluate cyber risk include understanding the origins of products, identifying suppliers, and tracking movements, which can be provided by transparency. Transparency includes historical, operational, and strategic information, which can impact SC performance, such as cyber-resilience (Montecchi et al., 2021). Technological practices, for example, blockchain, can offer a transparent historical data record through which cyber vulnerabilities can be identified. Operational and strategical transparency can quickly provide understandable information for SC decision makers to maintain businesses (Rejeb et al., 2021).

Using transparency, SC learn against cyberattacks by retrieving prior data. Leveraging prior learning to identify cyber threats quickly can significantly enhance the probability of preventing damage (Gani et al., 2022). In transparency, operational information can prepare SCs for quick change. Transparency can mitigate disruptions and increase resilience by providing useful information for decision makers (Montecchi et al., 2021). The exchange of strategic information increases trust among SC partners (Modgil et al., 2021). Operational SC transparency contributes to swift trust, which can create resilience. Strategy transparency can facilitate strategic recovery plans for possible cyberattacks.

According to the PBV theory, capabilities arise from practices and lead to the ability to accomplish tasks (Bromiley & Rau, 2014). Consistent information sharing through blockchain enables SC transparency, potentially achieving cyber-resilience. Previous empirical research has suggested that visibility practices can improve SC performance (Swift et al., 2019; Swink et al., 2024). Information transparency considerably impacts resilience by providing the required information during cyber disruptions. Thus, we formulate the following hypotheses:

H4. Supply chain transparency is positively associated with supply chain cyber-resilience.

H4a. Blockchain-based supply chains improve transparency, which results in creating a mediation pathway of cyber-resilience.

Methodology

We employ a vignette-based design to run experiments for collecting data from individuals to test the conceptual model illustrated in Fig. 1. Possible demand effects are addressed using a between-subject design in

Fig. 1. Research model.

experiments. In a within-subject design, participants may discern the purpose of the study by comparing conditions. This awareness can lead them to alter their responses based on what they think the researcher expects (demand characteristics). In addition to demand effects, the between-subject design measures items in such a way that they are not influenced by prior exposure to other conditions, which protects the integrity and objectivity of the results. Moreover, the between-subject design duration is shorter than a within-subject design, which increases the quality of data by less cognitive load. In a within-subject design, participants are exposed to multiple conditions, which can lead to carryover effects, such as learning, fatigue, or order effects. These effects may influence how participants respond to subsequent conditions, thereby introducing bias. To address the complexities inherent in examining the impact of blockchain technology on SC performance, we employ a between-subject experimental design, which is explained in the following subsections. Regression analysis is used to provide statistical evidence to test the hypotheses. Common method bias is checked along with the reliability and validity of the measurement model.

Data and sample

The sample includes individuals with work experience in technology, operations, and SCM. Owing to its diverse population (500,000 participants), we recruited participants using the Amazon M-Turk platform, which is used by operations and SC journals. Using a pre-screened pool technique (Ried et al., 2021), we created our sample to include participants with operations and SC job experience familiar with Industry 4.0. From an initial sample size of 200, after excluding incomplete surveys and those that failed attention tests, the final sample consists of 150 participants, including 68 women. Individuals are an average of 34.9 years old with a standard deviation of 9.1. The sample contains 144 college degree holders and six without college degrees. The demographic information shows a diverse selection.

Experimental design

The experimental design follows a vignette-based design, which includes three main phases: scenarios, manipulated variables, and measurements. In the first phase, participants reviewed consent letters and picked a hypothetical name to be prepared for scenario-based activities. Participants were given a company explanation and a description of the SC manager role. Participants were asked to focus on the company and SC manager. Then, participants were presented with a cyber incident for the company for them to review. The first phase ends with controlling participant focus. Note that hypothetical scenarios are as follows.

> *The hypothetical company is described as follows: Imagine a hypothetical scenario where a Supply Chain Manager is employed at ABC—Company. ABC—Company operates ten plants situated in different states across the USA. Established two decades ago, ABC—Company has successfully supplied a diverse range of products. With a robust and well-organized supply chain (SC), ABC—Company has achieved a stable position in its respective market.*
>
> *The hypothetical supply chain's role is described as follows: The Supply Chain Manager is responsible for managing risks within the SC. The responsibility includes safeguarding against cyberattacks and minimizing their impact to ensure a prompt return to normal operations. By employing risk management strategies, the Supply Chain Manager can prevent and mitigate potential disruptions caused by cyber threats, thus ensuring the smooth functioning of the SC.*
>
> *The hypothetical SC incident is described as follows: In a hypothetical scenario, on a business day, a sudden alert from the IT department shocks the company, cyberattacks and data breaches have struck, causing an estimated cost of $1 million. The gravity of the situation propels the company into action, carefully exploring various business continuity plans while considering the far-reaching consequences on the environment, economy, and society.*

In the second phase, we manipulated the independent variable into two scenarios: non-blockchain and blockchain-based SCs. We randomly assigned two manipulated levels to 150 participants to have 75 individuals for each treatment. The manipulated scenarios are as follows.

> *The first level is described as follows: A traditional approach is employed in the firm SC without utilizing recent technologies such as blockchain. The SC process involves multiple stakeholders, including suppliers, manufacturers, distributors, and retailers. Communication between these parties relies on conventional methods such as emails, phone calls, and physical documentation. While this approach has been functional, it suffers from challenges such as data silos and limited quick tracking data from source of materials to the end of the SC. Data are stored in a centralized database system. SC members need a financial third party to conduct financial transactions as these cannot occur immediately within the system.*
>
> *The second level is described as follows: A modern approach is employed in this firm SC, utilizing recent technologies such as blockchain technology. The SC process involves multiple stakeholders, including suppliers, manufacturers, distributors, and retailers. Communication between stakeholders is streamlined in a distributed network, thus reducing data silos and enhancing traceability. With real-time updates, the movement of materials from the source to the end of the SC becomes quick and efficient. SC members do not need a financial third party to conduct financial transactions as these can occur immediately within the system.*

The third phase of the experiment includes measuring outcomes. A seven-point Likert scale ranging from 1 (highly disagree) to 7 (highly agree) measures variables.

Variables

The independent variable has two levels: non-blockchain-based and blockchain-based SCs. The mediator variables are transparency and S&OP. The dependent variable is the SC cyber resilience. Items are presented in Table 1. Business type and company size are used to evaluate the effects of control variables on outcomes.

Table 1
Measurements and factor loadings.

Variables	Items	λ	e
Supply chain transparency (SCT) (Kumar et al., 2021)	SCT01: Supply chain members have information about the origin of raw materials or services.	0.945	0.107
	SCT02: Supply chain members have information about the ingredients and parts used in products and services.	0.995	0.011
	SCT03: Supply chain members have information about operations and processes.	0.950	0.098
	SCT04: Supply chain members have information about the location of other supply chain members.	0.904	0.183
Sales and operations planning (S&OP) adapted from Goh and Eldridge (2019)	SOP01: Supply chain data are collected for demand and sales planning.	0.996	0.008
	SOP02: Supply operations planning is clear and matched with the predicted demand.	0.968	0.063
	SOP03: Financial decisions are aligned with the supply that matches the demand.	0.958	0.082
	SOP04: Executive decision-making is based on an integrated planning process that aligns demand, supply, and financial planning.	0.955	0.087
Supply chain cyber resilience (SCCR) adapted from Sadeghi R. et al. (2024):	SCCR01: "We can identify potential cyber disruptions for avoidance."	0.985	0.029
	SCCR02: "We can cope with changes brought by cyber disruptions."	0.980	0.040
	SCCR03: "We can maintain control over structure and function during cyber disruptions."	0.961	0.076
	SCCR04: "We can provide a quick response to cyber disruptions."	0.918	0.157

Results

This section provides the assumptions tests and robustness checks of the measurement model including hypotheses testing.

Bias consideration

The social desirability bias was examined by deliberately hiding the research objective, including indirect questioning techniques, while anonymity and confidentiality were met (Ried et al., 2021). M-Turk in participant recruitment provided monetary incentives for completing surveys and maintained confidentiality throughout the recruitment procedure. As a result, concerns regarding non-response bias were addressed. We employed two marker-variable tests to address common method bias (CMB). Social desirability is the marker variable, which is not related to the research model (Sadeghi R. et al., 2024). In the first CMB check, no difference was noted between bivariate and partial correlations, while the marker variable exhibited no correlation with the variables (correlation $\langle$ 0.03 with p-value $\rangle$ 0.6); therefore, the CMB concern is mitigated. In the second CMB check, we used a chi-square test (χ^2), and the null hypothesis was upheld both for the models inclusive and exclusive of the marker variable ($(\Delta\chi 2)\Delta df$, p-value $>$ 0.05); therefore, CMB's concern is mitigated.

Reliability and validity

The robustness of item reliability is confirmed by composite reliability (CR) coefficients exceeding 0.95 (Kline, 2023, p. 287). We employed confirmatory factor analysis to address the validity of the measurement model (see Table 2). The fifth item of cyber resilience was dropped due to low loadings. The χ^2 was insignificant, which supports the good fit of the measurement model (χ^2/df=66.25/51, p-value=0.07). Values for factor loadings (λ) surpass 0.7. Moreover, the convergent validity is not questioned because the average variance extracted (AVE) values are greater than 0.5 (Kline, 2023, p. 239). The discriminant validity test is supported by the values of $\sqrt{\text{AVE}}$, which are greater than the inter-construct correlations (φ). In addition, we consider other fit indices (usually used for the conditions in which χ^2 is significant), which are within recommended ranges, for example, RMSEA = 0.04 and CFI = 0.99 > 0.90 (Hahs-Vaughn, 2016, p. 452). Therefore, the measurement validity is not a concern.

Manipulation test

The manipulation test is an important step in the validity of the experimental design to confirm that the independent variable, the two levels of non-blockchain- and blockchain-based SCs, was perceived by participants as intended. The manipulation test was implemented immediately following the scenario presentation in the second phase of the experiment. Participants were asked a set of targeted questions designed to assess their understanding of the features highlighted in their assigned scenario. For instance, participants were asked to rate their agreement with statements such as, "Data are stored in a centralized database system" or "Supply chain members do not need a financial third party to conduct financial transactions." These items were measured using a seven-point Likert scale to capture the degree of clarity and differentiation perceived by participants. Manipulation test confirmed the study's validity by demonstrating that participants consistently identified the key characteristics of their assigned scenario (p-value $<$ 0.001).

Hypotheses testing

The regression assumptions are met. Shapiro-Wilk test results (p-value = 0.11) support the normality assumption; the Breusch-Pagan test results (11.5, $df = 7$, and p-value = 0.11) pass the homoscedasticity; and the variance inflation factors (VIF) values do not exhibit multicollinearity. The data used in this study satisfies the assumptions of regression, including normality, linearity, and multicollinearity thresholds. Regression techniques are well-suited for datasets where these assumptions are held, which provide robust and interpretable parameter estimates. Another technique is the partial least squares (PLS) method, which is often used when these assumptions are violated or when the data are highly collinear, which was not the case here. Moreover, to present more details about the mediation analysis steps, we provide four statistical models using regression analysis. The effects of control variables on the outcomes were insignificant, including regressing the dependent variable on them (p-value >0.6). We present four regression

Table 2
Validity, reliability, and construct correlations.

Constructs	SOP	SCT	SCCR	$\sqrt{\text{AVE}}$	AVE	CR (Ω)
Sales and operations planning (S&OP)	–	–	–	0.969	0.938	0.984
Supply chain transparency (SCT)	0.536	–	–	0.948	0.899	0.974
Supply chain cyber resilience (SCCR)	0.555	0.576	–	0.962	0.926	0.98

AVE: Average variance extracted; CR: Composite reliability.

models in Table 3 to provide more statistical details of testing hypotheses, including confidence intervals.

Model-1 shows the significant effect of blockchain on the SC performance to identify and avoid cyberattacks by showing cyber resilience ($t = 7.9$, error $= 0.203$, and $p < 0.001$, adjusted R square $= 0.28$). Model-2 and Model-3, moreover, reveal that blockchain positively impacts S&OP (H1: $t = 9.4$, error $= 0.20$, and $p < 0.001$, adjusted R-squared $= 0.4$) and SC transparency (H2: $t = 10$, error $= 0.18$, and $p < 0.001$, adjusted R-squared $= 0.44$), respectively. Model-4 provides statistical support to create SCCR by SC transparency (H3: $t = 3.6$, error $= 0.08$, and $p < 0.001$, adjusted R square $= 0.43$) and S&OP (H4: $t = 3.3$, error $= 0.07$, and $p < 0.001$, adjusted R-squared $= 0.43$). Moreover, using the Lavaan within the R programming language, the regression analysis is compared with the structural equation modeling (SEM). The regression outcomes were consistent with the SEM results, which are reported in Table 4.

We perform the mediation analysis using the fourth Hayes Process framework with 5000 bootstrap samples to explain the direct and indirect impacts. Supportive findings for the mediation relationships are presented in Table 5; the mediating roles of S&OP and SC transparency, H3a and H4a, indirect effects, are significant, thus supporting a full mediation relationship. By contrast, the direct effects of blockchain on SCCR are insignificant.

Table 3
Regression analysis of 150 responses.

	Model-1	Model-2	Model-3	Model-4
(Intercept)	1.480*	1.265*	1.697**	0.611
	$t = 2.446$	$t = 2.031$	$t = 3.160$	$t = 1.067$
	se = 0.605	se = 0.623	se = 0.537	se = 0.572
	[0.284, 2.676]	[0.034, 2.496]	[0.636, 2.759]	[−0.520, 1.742]
Sales and operations planning (S&OP)	–	–	–	0.257***
	–	–	–	$t = 3.397$
	–	–	–	se = 0.076
	–	–	–	[0.107, 0.406]
Supply chain transparency (SCT)	–	–	–	0.321***
	–	–	–	$t = 3.665$
	–	–	–	se = 0.088
	–	–	–	[0.148, 0.494]
Blockchain	1.606***	1.985***	1.913***	0.482+
	$t = 7.904$	$t = 9.492$	$t = 10.606$	$t = 1.781$
	se = 0.203	se = 0.209	se = 0.180	se = 0.271
	[1.204, 2.007]	[1.572, 2.399]	[1.556, 2.269]	[−0.053, 1.018]
Goods production companies	−0.217	−0.421	0.229	−0.183
	$t = -0.407$	$t = -0.766$	$t = 0.482$	$t = -0.375$
	se = 0.534	se = 0.550	se = 0.474	se = 0.487
	[−1.272, 0.838]	[−1.507, 0.666]	[−0.708, 1.165]	[−1.146, 0.780]
Services companies	−0.056	−0.212	0.134	−0.044
	$t = -0.105$	$t = -0.388$	$t = 0.285$	$t = -0.092$
	se = 0.532	se = 0.547	se = 0.472	se = 0.484
	[−1.107, 0.995]	[−1.294, 0.870]	[−0.799, 1.067]	[−1.001, 0.912]
Trade and commerce companies	−0.110	−0.603	0.164	−0.007
	$t = -0.183$	$t = -0.980$	$t = 0.309$	$t = -0.014$
	se = 0.598	se = 0.616	se = 0.531	se = 0.546
	[−1.291, 1.072]	[−1.820, 0.613]	[−0.885, 1.213]	[−1.087, 1.072]
Company size	0.003	0.142	−0.109	0.002
	$t = 0.023$	$t = 1.066$	$t = -0.950$	$t = 0.013$
	se = 0.129	se = 0.133	se = 0.115	se = 0.119
	[−0.253, 0.259]	[−0.121, 0.406]	[−0.336, 0.118]	[−0.233, 0.236]
Dependent variable	SCCR[1]	SOP	SCT	SCCR
R^2	0.308	0.401	0.447	0.436
Adj. R^2	0.284	0.381	0.428	0.408

1: Supply chain cyber resilience (SCCR); + $p < 0.1$.
* $p < 0.05$.
** $p < 0.01$.
*** $p < 0.001$.

Table 4
Comparison of the regression analysis with structural equation modeling (SEM).

Relationships	SEM/ Regression	p-values
Blockchain → Sales and operations planning (S&OP)	1.907/1.985	< 0.001
Blockchain → Supply chain transparency (SCT)	2.039/1.913	< 0.001
Blockchain → Supply chain cyber resilience (SCCR)	0.518/0.482	= 0.075
Supply chain transparency (SCT)→ Supply chain cyber resilience (SCCR)	0.306/0.321	= 0.001
Sales and operations planning (S&OP)→ Supply chain cyber resilience (SCCR)	0.268/0.257	< 0.001

Discussion and conclusion

This study proposed a conceptual model to address the research question. Findings suggest that blockchain contributes to information flow improvement in SCM to improve performance.

Previous works have emphasized the considerable impact of new technologies on the S&OP (Swaim et al., 2016). The results demonstrate the significant contribution of blockchain to S&OP through its utilization of immutability, distributed databases, and smart contracts, H1. Our empirical evidence supports the positive effect of blockchain practice on the transparency in SCs, H2. However, contrasting perspectives exist regarding the benefits of transparency and SOP in previous studies. For instance, previous research emphasizes the potential adverse impacts of transparency on organizational performance, including increased audit fees (Ye et al., 2018). Furthermore, Babu et al., 2023 observed that SOPs can hinder the efficiency of production processes and the standardization of products as they necessitate frequent updates. Nevertheless, the current study demonstrated that the extent of access to business data shared among SC members can significantly improve SC abilities (e.g., S&OP) to effectively manage and adapt to disruptions (Feizabadi et al., 2019). Past studies have established that S&OP can improve SC performance regarding risk management (Dittfeld et al., 2021). By doing so, the results of the current study revealed that blockchain-based SCs can improve S&OP by allowing firms to align plans and processes to achieve cyber-resilience during disruptions, H3 and H3a. We extend the existing literature to investigate the unexploited potential of transparency in enhancing cyber resilience. Our findings indicate that transparency is a fundamental capability by which SC decision makers gain access to high-quality data during cyber disruptions. This transparency can lead to improved performance in cyber resilience, H4, and H4a.

Table 5
Indirect and direct effects of 5000 bootstrap samples.

Effects	Effect	Error	LLCI	ULCI
Direct Effect				
Blockchain → SCCR	0.48	0.27	−0.05	1.01
Indirect Effects				
Blockchain → SCT → SCCR	0.42	0.13	0.16	0.68
Blockchain → SOP → SCCR	0.35	0.10	0.14	0.56
Total	0.77	0.15	0.47	1.07

Lower limit confidence interval (CI), Upper limit CI,.
Supply chain transparency (SCT), Sales and operations planning (S&OP),.
Supply chain cyber resilience (SCCR).

Theoretical implications

The theoretical implications of this study are twofold. First, this study highlights blockchain as a significant explanatory variable for improving SC flows, such as cash and information flow, to improve cyber resilience in risk management. As a disruptive practice, blockchain can change existing SC relationships. As demonstrated in the current study, transparency enabled by blockchain has a considerable impact on SC performance in terms of cyber risk mitigation. These findings offer valuable insights for developing theories incorporating blockchain-based transparency as a practical component of risk management strategies. Second, this study suggests that S&OP is a significant enabler of cyber resilience. Future research has the potential to enhance the understanding of this suggested relationship by investigating the conditions under which the impact of S&OP is either decreased or increased. S&OP can enhance coordination and interaction in the SC while integrating the different plans during disruptions (e.g., cyberattacks).

Managerial implications

Built on empirical evidence and theoretical support, this study offers three managerial implications. First, managers can employ blockchain-based information management for their SCs. In a blockchain-based SC, decision makers have access to high-quality data that is immune against cyberattacks, which contrasts with traditional systems. SC data are more secure and immune in a blockchain-based system, which can improve cyber resilience. A global average cyberattack costs 4.4 million dollars, but this expense can be avoided in a blockchain-based SC. Second, managers can strategically implement transparency as a fundamental component of their risk management approach. In a transparent SC, pertinent information, data, and decision-making processes are visible to stakeholders. Transparency can serve as a proactive tool for early risk detection and assessment. Transparency facilitates understanding of SC risk and empowers stakeholders to share insights and suggestions for risk avoidance or mitigation. Transparency as a risk management strategy can improve stakeholder relationships by creating trust and credibility. Industry summits have highlighted the role of SC transparency in creating resilience. Third, managers can improve SCM using blockchain-based S&OP, ultimately resulting in higher customer satisfaction, lower lead time, efficient budget management, and better demand forecasting (Goh & Eldridge, 2019). Our findings indicate that S&OP can improve companies' ability to identify and mitigate disruptions (e.g., cyberattacks and data breaches) (Jonsson et al., 2021). For instance, companies such as IBM, Microsoft, and SAP employ blockchain-based SCs to streamline transparent financial and inventory transactions.

Limitations and future research

Findings presented herein are limited to cross-sectional data, which can be addressed in future research by collecting longitudinal data. Moreover, future research can improve data quality by collecting in-person data rather than the virtual option used in the current study. This study employed the PBV to provide theoretical support. Future research can employ other theoretical frameworks, such as organizational information processing theory. Future research can explore potential mediating variables to provide more explanations regarding how blockchain can contribute to transparency and SCCR. Moreover, future research can consider the role of absorptive capacity as a moderator to explain when a blockchain-based SC can backfire. The relationships between transparency and cyber resilience can be explored by considering the role of power and SC complexity in times of cyberattacks. Finally, other emerging technologies, such as the metaverse, can be considered in cyber resilience. More empirical studies are needed to explain the role of Industry 4.0, including blockchain and metaverse, in SCM, particularly in risk management and sustainable development. Future research could explore the potential sustainability implications of blockchain within SCs. Blockchain's ability to enhance transparency and traceability could play a pivotal role in advancing sustainable practices, such as reducing waste, optimizing resource usage, and ensuring ethical sourcing. Investigating how blockchain integrates with sustainability goals would provide valuable insights into its broader impact on SCM and contribute to the growing body of knowledge on technology-driven sustainability initiatives.

Availability of data

The data is available from the corresponding author upon reasonable request.

CRediT authorship contribution statement

Ava Hajian: Writing – review & editing, Writing – original draft. **Saba Rezaeinejad:** Writing – review & editing, Writing – original draft. **Kiarash Rayman:** Writing – review & editing, Writing – original draft. **Sajad Khorsandroo:** Writing – review & editing, Software.

Acknowledgment

This work is partially supported by NSF grants 2113945 and 2200538 at NC A&T State University. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agency.

References

Aslam, J., Lai, K., Kim, Y. B., & Treiblmaier, H. (2024). The implications of blockchain for logistics operations and sustainability. *Journal of Innovation & Knowledge, 9*(4), Article 100611. https://doi.org/10.1016/j.jik.2024.100611

Aslam, J., Saleem, A., Khan, N. T., & Kim, Y. B. (2021). Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry. *Journal of Innovation & Knowledge, 6*(2), 124–134. https://doi.org/10.1016/j.jik.2021.01.002

Bambysheva, N., & Castillo, M. (2024). *Forbes blockchain 50 2023*. Forbes. https://www.forbes.com/sites/ninabambysheva/2023/02/07/forbes-blockchain-50-2023/.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Bromiley, P., & Rau, D. (2014). Towards a practice-based view of strategy: Research Prospectives. *Strategic Management Journal, 35*(8), 1249–1256. https://doi.org/10.1002/smj.2238

Bromiley, P., & Rau, D. (2016). Operations management and the resource based view: Another view. *Journal of Operations Management, 41*(1), 95–106. https://doi.org/10.1016/j.jom.2015.11.003

Cao, S., Foth, M., Powell, W., Miller, T., & Li, M. (2022). A blockchain-based multisignature approach for supply chain governance: A use case from the Australian beef industry. *Blockchain: Research and Applications, 3*(4), Article 100091. https://doi.org/10.1016/j.bcra.2022.100091

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The International Journal of Logistics Management, 15*(2), 1–14. https://doi.org/10.1108/09574090410700275

Dittfeld, H., Scholten, K., & Van Donk, D. P. (2021). Proactively and reactively managing risks through sales & operations planning. *International Journal of Physical Distribution & Logistics Management, 51*(6), 566–584. https://doi.org/10.1108/IJPDLM-07-2019-0215

Dubey, R., Bryde, D. J., Dwivedi, Y. K., Graham, G., & Foropon, C. (2022). Impact of artificial intelligence-driven big data analytics culture on agility and resilience in humanitarian supply chain: A practice-based view. *International Journal of Production Economics, 250*, Article 108618. https://doi.org/10.1016/j.ijpe.2022.108618

Feizabadi, J., Maloni, M., & Gligor, D. (2019). Benchmarking the triple-A supply chain: Orchestrating agility, adaptability, and alignment. *Benchmarking: An International Journal, 26*(1), 271–295. https://doi.org/10.1108/BIJ-03-2018-0059

Gani, A. B. D., Fernando, Y., Lan, S., Lim, M. K., & Tseng, M.-L. (2022). Interplay between cyber supply chain risk management practices and cyber security performance. *Industrial Management & Data Systems, 123*(3), 843–861. https://doi.org/10.1108/IMDS-05-2022-0313

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management, 25*(2), 223–240. https://doi.org/10.1108/SCM-10-2018-0357

Goh, S. H., & Eldridge, S. (2019). Sales and operations planning: The effect of coordination mechanisms on supply chain performance. *International Journal of Production Economics, 214*, 80–94. https://doi.org/10.1016/j.ijpe.2019.03.027

Hahs-Vaughn, D. L. (2016). *Applied multivariate statistical concepts*. Routledge.

Javadpour, A., AliPour, F. S., Sangaiah, A. K., Zhang, W., Ja'far, F., & Singh, A. (2023). An IoE blockchain-based network knowledge management model for resilient disaster frameworks. *Journal of Innovation & Knowledge, 8*(3), Article 100400. https://doi.org/10.1016/j.jik.2023.100400

Jonsson, P., Kaipia, R., & Barratt, M. (2021). Guest editorial: The future of S&OP: Dynamic complexity, ecosystems and resilience. *International Journal of Physical Distribution & Logistics Management, 51*(6), 553–565. https://doi.org/10.1108/IJPDLM-07-2021-452

Kazmi, S. W., & Ahmed, W. (2022). Understanding dynamic distribution capabilities to enhance supply chain performance: A dynamic capability view. *Benchmarking, 29*(9), 2822–2841. https://doi.org/10.1108/BIJ-03-2021-0135

Khan, O., & Estay, D. A. S. (2015). Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review, 5*(4), 6–12. https://doi.org/10.22215/timreview/885

Khan, S. A. R., Tabish, M., & Zhang, Y. (2023). Embracement of industry 4.0 and sustainable supply chain practices under the shadow of practice-based view theory: Ensuring environmental sustainability in corporate sector. *Journal of Cleaner Production, 398*, Article 136609. https://doi.org/10.1016/j.jclepro.2023.136609

Kline, R. B. (2023). *Principles and practice of structural equation modeling*. Guilford Press.

Kreuter, T., Scavarda, L. F., Thomé, A. M. T., Hellingrath, B., & Seeling, M. X. (2022). Empirical and theoretical perspectives in sales and operations planning. *Review of Managerial Science, 16*(2), 319–354. https://doi.org/10.1007/s11846-021-00455-y

Kumar, S., Murphy, M., Talwar, S., Kaur, P., & Dhir, A. (2021). What drives brand love and purchase intentions toward the local food distribution system? A study of social media-based REKO (fair consumption) groups. *Journal of Retailing and Consumer Services, 60*, Article 102444. https://doi.org/10.1016/j.jretconser.2021.102444

Laari, S., Lorentz, H., Jonsson, P., & Lindau, R. (2023). Procurement's role in resolving demand–supply imbalances: An information processing theory perspective. *International Journal of Operations & Production Management, 43*(13), 68–100. https://doi.org/10.1108/IJOPM-06-2022-0382

Li, L., Zhu, W., Chen, L., & Liu, Y. (2024). Generative AI usage and sustainable supply chain performance: A practice-based view. *Transportation Research Part E: Logistics and Transportation Review, 192*, Article 103761. https://doi.org/10.1016/j.tre.2024.103761

Liu, Y., Farooque, M., Lee, C.-H., Gong, Y., & Zhang, A. (2023). Antecedents of circular manufacturing and its effect on environmental and financial performance: A practice-based view. *International Journal of Production Economics, 260*, Article 108866. https://doi.org/10.1016/j.ijpe.2023.108866

Mahesh Babu, P., Seadon, J., & Moore, D. (2023). Cognitive biases that influence Lean implementation and practices in a multicultural environment. *International Journal of Lean Six Sigma, 14*(7), 1655–1714. https://doi.org/10.1108/IJLSS-10-2022-0218

Modgil, S., Singh, R. K., & Hannibal, C. (2021). Artificial intelligence for supply chain resilience: Learning from Covid-19. *The International Journal of Logistics Management, 33*(4), 1246–1268. https://doi.org/10.1108/IJLM-02-2021-0094

Montecchi, M., Plangger, K., & West, D. C. (2021). Supply chain transparency: A bibliometric review and research agenda. *International Journal of Production Economics, 238*, Article 108152. https://doi.org/10.1016/j.ijpe.2021.108152

Nash, K. S. (2018). Farm to cradle: Nestlé experiments with tracking gerber baby food on the blockchain. *Wall Street Journal*. https://www.wsj.com/articles/farm-to-cradle-nestle-experiments-with-tracking-gerber-baby-food-on-the-blockchain-1533121929.

Paris, C. (2019). Big ocean cargo carriers join blockchain initiative. *Wall Street Journal*. https://www.wsj.com/articles/big-ocean-cargo-carriers-join-blockchain-initiative-11559044800.

Pereira, D. F., Oliveira, J. F., & Carravilla, M. A. (2020). Tactical sales and operations planning: A holistic framework and a literature review of decision-making models. *International Journal of Production Economics, 228*, Article 107695. https://doi.org/10.1016/j.ijpe.2020.107695

Rejeb, A., Keogh, J. G., Simske, S. J., Stafford, T., & Treiblmaier, H. (2021). Potentials of blockchain technologies for supply chain collaboration: A conceptual framework. *The International Journal of Logistics Management, 32*(3), 973–994. https://doi.org/10.1108/IJLM-02-2020-0098

Ried, L., Eckerd, S., Kaufmann, L., & Carter, C. (2021). Spillover effects of information leakages in buyer–supplier–supplier triads. *Journal of Operations Management, 67*(3), 280–306. https://doi.org/10.1002/joom.1116

Sadeghi, R., Hajian, A., & Rabiee, M. (2023). Blockchain and machine learning framework for financial performance in pharmaceutical supply chains. *Advancement in business analytics tools for higher financial performance* (pp. 112–128). IGI Global. https://doi.org/10.4018/978-1-6684-8386-2.ch006

Sadeghi, R., Ojha, D., K., Kaur, P., Mahto, R. V., & Dhir, A. (2024). Explainable artificial intelligence and agile decision-making in supply chain cyber resilience. *Decision Support Systems, 180*, Article 114194. https://doi.org/10.1016/j.dss.2024.114194

Sahin, F., & Robinson, E. P., Jr. (2005). Information sharing and coordination in make-to-order supply chains. *Journal of Operations Management, 23*(6), 579–598. https://doi.org/10.1016/j.jom.2004.08.007

Shukla, A., Jirli, P., Mishra, A., & Singh, A. K. (2024). An overview of blockchain research and future agenda: Insights from structural topic modeling. *Journal of Innovation & Knowledge, 9*(4), Article 100605. https://doi.org/10.1016/j.jik.2024.100605

Singhal, J., & Singhal, K. (2007). Holt, Modigliani, Muth, and Simon's work and its role in the renaissance and evolution of operations management. *Journal of Operations Management, 25*(2), 300–309. https://doi.org/10.1016/j.jom.2006.06.003

Sizan, N. S., Dey, D., Layek, M. A., Uddin, M. A., & Huh, E.-N. (2025). Evaluating blockchain platforms for IoT applications in industry 5.0: A comprehensive review. *Blockchain: Research and Applications*. , Article 100276. https://doi.org/10.1016/j.bcra.2025.100276

Skilton, P. F., & Robinson, J. L. (2009). Traceability and normal accident theory: How does supply network complexity influence the traceability of adverse events? *Journal of Supply Chain Management, 45*(3), 40–53. https://doi.org/10.1111/j.1745-493X.2009.03170.x

Sun, Y., Shahzad, M., & Razzaq, A. (2022). Sustainable organizational performance through blockchain technology adoption and knowledge management in China. *Journal of Innovation & Knowledge, 7*(4), Article 100247. https://doi.org/10.1016/j.jik.2022.100247

Sunny, J., Undralla, N., & Madhusudanan Pillai, V. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. *Computers & Industrial Engineering, 150*, Article 106895. https://doi.org/10.1016/j.cie.2020.106895

Swaim, J. A., Maloni, M., Bower, P., & Mello, J. (2016). Antecedents to effective sales and operations planning. *Industrial Management & Data Systems, 116*(6), 1279–1294. https://doi.org/10.1108/IMDS-11-2015-0461

Swift, C., Guide, V. D. R., Jr, & Muthulingam, S. (2019). Does supply chain visibility affect operating performance? Evidence from conflict minerals disclosures. *Journal of Operations Management, 65*(5), 406–429. https://doi.org/10.1002/joom.1021

Swink, M., Sant'Ana Gallo, I., Defee, C., & da Silva, A. L. (2024). Supply chain visibility types and contextual characteristics: A literature-based synthesis. *Journal of Business Logistics, 45*(1), Article e12366. https://doi.org/10.1111/jbl.12366

Tavares Thomé, A. M., Scavarda, L. F., Fernandez, N. S., & Scavarda, A. J. (2012). Sales and operations planning: A research synthesis. *International Journal of Production Economics, 138*(1), 1–13. https://doi.org/10.1016/j.ijpe.2011.11.027

Tian, M., Chen, Y., Tian, G., Huang, W., & Hu, C. (2023). The role of digital transformation practices in the operations improvement in manufacturing firms: A practice-based view. *International Journal of Production Economics, 262*, Article 108929. https://doi.org/10.1016/j.ijpe.2023.108929

Wan, X., Jha, A. K., Kazantsev, N., & Boh, W. F. (2023). Online-to-offline platforms: Examining the effects of demand-side usage on supply-side decisions. *Information & Management, 60*(2), Article 103757. https://doi.org/10.1016/j.im.2023.103757

Wang, Y., Liu, B., Chan, H. K., & Zhang, T. (2023). Who pays buyers for not disclosing supplier lists? Unlocking the relationship between supply chain transparency and trade credit. *Journal of Business Research, 155*, Article 113404. https://doi.org/10.1016/j.jbusres.2022.113404

Williams, B. D., Roh, J., Tokar, T., & Swink, M. (2013). Leveraging supply chain visibility for responsiveness: The moderating role of internal integration. *Journal of Operations Management, 31*(7–8), 543–554. https://doi.org/10.1016/j.jom.2013.09.003

Ye, Q., Gao, J., & Zheng, W. (2018). Accounting standards, earnings transparency and audit fees: Convergence with IFRS in China. *Australian Accounting Review, 28*(4), 525–537. https://doi.org/10.1111/auar.12226

Yu, W., Chavez, R., Liu, Q., & Cadden, T. (2024). Examining the effects of digital supply chain practices on supply chain viability and operational performance: A practice-based view. *IEEE Transactions on Engineering Management, 71*, 10413–10426. https://doi.org/10.1109/TEM.2023.3294670. IEEE Transactions on Engineering Management.

Zelbst, P. J., Green, K. W., Sower, V. E., & Bond, P. L. (2020). The impact of RFID, IIoT, and Blockchain technologies on supply chain transparency. *Journal of Manufacturing Technology Management, 31*(3), 441–457. https://doi.org/10.1108/JMTM-03-2019-0118

Zheng, K., Zheng, L. J., Gauthier, J., Zhou, L., Xu, Y., Behl, A., & Zhang, J. Z. (2022). Blockchain technology for enterprise credit information sharing in supply chain finance. *Journal of Innovation & Knowledge, 7*(4), Article 100256. https://doi.org/10.1016/j.jik.2022.100256

Zhu, S., Song, J., Hazen, B. T., Kang, L., & Cegielski, C. (2018). How supply chain analytics enables operational supply chain transparency: An organizational information processing theory perspective. *International Journal of Physical Distribution & Logistics Management, 48*(1), 47–68. https://doi.org/10.1108/IJPDLM-11-2017-0341

Zkik, K., Belhadi, A., Kamble, S., Venkatesh, M., Oudani, M., & Sebbar, A. (2024). Cyber resilience framework for online retail using explainable deep learning approaches and blockchain-based consensus protocol. *Decision Support Systems, 182*, Article 114253. https://doi.org/10.1016/j.dss.2024.114253