Asian Management and Business Review, Volume 5 Issue 2, 2025: 297-312

The interplay of blockchain technology, user-centric orientation, and cybersecurity measures in supply chains of manufacturing enterprises

Baraka Israel

Department of Procurement & Supplies Management, College of Business Education, Mbeya Campus, Tanzania

Article History
Received : 2025-01-23
Revised : 2025-03-07
Accepted : 2025-03-08
Published : 2025-07-28

Keywords:
Blockchain technology; cybersecurity; user-centric orientation; supply chain; manufacturing enterprises.

***Corresponding author:**
isbara03@gmail.com

DOI:
10.20885/AMBR.vol5.iss2.art4

Abstract

As supply chains become increasingly digitalized, cybersecurity (CBS) threats escalate, necessitating the adoption of innovative technologies such as blockchain technology (BLT) to enhance security. The purpose of this study is to examine the effect of blockchain technology (BLT) on cybersecurity (CBS) measures within the supply chains of manufacturing enterprises, considering the moderating role of user-centric orientation (UCO). The study is grounded in the Diffusion of Innovation (DOI) theory and adopts a cross-sectional quantitative research design, using a questionnaire survey to collect data from 206 supply chain partners of manufacturing enterprises in Dar es Salaam, Tanzania. Hayes' PROCESS macro is employed to test model hypotheses. The study results exhibit a significant positive direct effect of both BLT and UCO on CBS. Furthermore, UCO positively moderates the relationship between BLT and CBS. For manufacturing enterprises and supply chain partners seeking to implement BLT to enhance CBS, the study highlights the importance of incorporating UCO into the design and implementation of security protocols, ensuring that users are educated and actively involved in CBS practices. This research contributes to the growing body of literature on BLT and CBS by exploring the under-researched moderating role of UCO. It extends the application of DOI theory to the intersection of BLT and CBS in manufacturing supply chains, offering a novel perspective on how user engagement can optimise the security benefits of emerging technologies.

Introduction

The rapidly evolving business environment has brought significant changes, with digital technologies such as artificial intelligence (AI), cloud computing, blockchain, and the Internet of Things (IoT) emerging as critical components of modern supply chain management (SCM). Integrating these digital technologies into SCM has become crucial for companies aiming to enhance operational efficiency, competitiveness, and resilience (Hong & Hales, 2024; Calle et al., 2019). However, as technological advancements progress, supply chains (SCs) face increasing challenges, primarily due to the growing digitalisation of operations and the integration of complex networks involving suppliers, manufacturers, and partners. One major challenge is the heightened vulnerability to cyberattacks, such as ransomware, data breaches, and hacking, which can disrupt material flow, expose sensitive information, and compromise manufacturing and distribution processes (Gani et al., 2023; Renaud & Ophoff, 2021). Moreover, global SCs often involve multiple third-party vendors, increasing the risk of cyber threats due to inconsistent compliance with cybersecurity regulations. The lack of standardised cybersecurity protocols across different nodes in SCs further complicates this issue, as varying levels of security practices create weak links (Friday et al., 2024; Renaud & Ophoff, 2021).

E ISSN 2775-202X

These vulnerabilities in SCs can lead to significant consequences, including data breaches, financial losses, compromised data integrity, and erosion of stakeholder trust. Evidence of this, a global information security analysis reveals that 66% of businesses experience significant customer information leakage, while 56% report the disclosure of sensitive corporate data (Kaspersky, 2021). These challenges highlight the need for robust cybersecurity strategies and resilient operational frameworks to ensure business continuity and mitigate risks in an increasingly digital and interconnected SC landscape. This study delves into the interaction effect of blockchain technology and user-centric orientation on cybersecurity measures in the SCs of manufacturing enterprises, framed within the diffusion of innovation (DOI) theory. In this context, the SC of manufacturing enterprises refers to the systems and processes involved in producing and distributing goods, operating within complex networks of suppliers, manufacturers, distributors, retailers, and customers (Rehman et al., 2023; Israel, 2022). These enterprises play a significant role in regional and global SCs by converting raw materials into finished goods through various methods and operational systems, contributing approximately 50% to 60% of the goods produced (Lelo & Israel, 2024). However, as these enterprises increasingly rely on digitalised SCM to ensure the efficient flow of raw materials, components, and finished products, they also face heightened risks related to cybersecurity (Hong & Hales, 2024; Chaduvula et al., 2018).

Essentially, digitalisation exposes SCs to vulnerabilities such as data breaches, hacking, and cyberattacks (Rauniyar et al., 2023; Nicoletti & Appolloni, 2024), making it essential to address these risks through innovative and user-centred cybersecurity strategies. In response, studies have highlighted blockchain technology, characterised by its decentralized and immutable ledger, as having the potential to enhance transparency, resilience, traceability, and security within the SCs of manufacturing enterprises (Rauniyar et al., 2023; Raj et al., 2024). This technology facilitates more efficient transactions and strengthens trust among SC stakeholders, ultimately leading to improved operational efficiency and risk management (Gohil & Thakker, 2021). Besides, blockchain technology offers a streamlined approach by connecting various SC stakeholders through real-time data exchange, automation, and collaborative platforms. Amidst the evolution of blockchain, a user-centric orientation has emerged as a crucial determinant of the successful integration of this technology within SCs (Alyami et al., 2024; Aliu et al., 2024). A user-centric approach prioritises the needs and preferences of end-users, enabling SC partners to design and implement digital security measures that are responsive, agile, and tailored to meet user demands. Integrating user-centric orientation with blockchain technology can significantly enhance the user experience, foster collaboration, and facilitate more informed security decision-making across SC operations (Kont, 2024; Morganelli, 2021). Thus, successfully integrating blockchain technology requires a deep understanding of user needs alongside a robust cybersecurity framework to mitigate the risks associated with digital transactions.

As manufacturing enterprises navigate the complex digital transformation landscape, understanding the interaction effect of blockchain technology and user-centric orientation on cybersecurity becomes essential for safeguarding SC resilience and sustainability. According to the DOI theory (Rogers, 2003), adopting innovation can occur at varying rates, influenced by factors such as perceived advantage, compatibility with existing systems, complexity, trialability, and observability. For manufacturing enterprises, the adoption of blockchain technology represents not just a technological shift but a comprehensive transformation that requires alignment with user expectations and adherence to stringent cybersecurity protocols. Existing studies reveal a notable gap in understanding the interplay between blockchain technology, user-centric orientation, and cybersecurity measures within the SCs of manufacturing enterprises, especially in developing countries. Most available research focuses on blockchain's operational benefits (Kumar et al., 2024; Renaud & Ophoff, 2021) and challenges (Rauniyar et al., 2023; Raj et al., 2024), primarily in foreign and developed countries (Kawaguchi, 2019; Topcu et al., 2024). Furthermore, studies have overlooked how a user-centric orientation can strengthen the unique properties of blockchain technology, such as immutability and decentralization, in realizing comprehensive cybersecurity frameworks. Against this backdrop, this study introduces a novel perspective by examining the interaction effect of blockchain technology on cybersecurity in the SCs of Tanzania's

manufacturing enterprises, a developing country, with user-centric orientations serving as a moderating factor. Three central research objectives guide the study:
RQ1. Does blockchain technology have a significant direct effect on cybersecurity measures?
RQ2. Do user-centric orientations have a significant direct effect on cybersecurity measures?
RQ3. How do user-centric orientations moderate the relationship between blockchain technology and cybersecurity measures?

The study contributes to both academic and practical knowledge in several ways. Academically, it expands the understanding of blockchain's role in cybersecurity beyond operational efficiency, offering insights into how it can mitigate cyber risks in the SCs of manufacturing enterprises. The research also contributes to the literature on user-centric design by highlighting its moderating influence on the success of blockchain-based security measures. Practically, the study provides actionable insights for SC managers and cybersecurity professionals in the manufacturing sector, helping them design more effective, user-aligned blockchain solutions to safeguard against cyber threats. In addition, the study lays the groundwork for future studies to explore the role of human factors in implementing advanced cybersecurity technologies.

Literature Review and Hypotheses Development

Diffusion of Innovation (DOI) Theory

The DOI theory offers a foundational framework for understanding how, why, and at what rate new ideas and technologies spread within and across organisations. Initially introduced by Tarde in 1903 and later popularized by Rogers in 1962, the theory posits that adopting innovations is influenced by several key factors. These include the perceived attributes of the innovation (such as relative advantage, compatibility, complexity, trialability, and observability), the communication channels through which information flows, the social systems involved, and the roles of change agents (Tarde, 1903; Rogers, 1962). In this study, DOI theory provides valuable insights into how UCO influences the adoption of BLT and CBS measures in SCs of manufacturing enterprises. Essentially, the perceived advantages of BLT, such as enhanced transparency and security, align with the key propositions of DOI theory, as these attributes can drive user acceptance and engagement. UCO, which emphasises tailoring processes and systems to meet the specific needs of end-users, enhances the perceived compatibility of blockchain solutions (Kont, 2024; Lyon, 2024). By addressing user needs, companies can mitigate concerns related to complexity and trialability, thus fostering an environment conducive to the adoption of BLT and CBS measures. It is theorised that the perceived security benefits of blockchain can significantly influence users' willingness to engage with this technology. Drawing on DOI theory, this study explores how BLT and UCO interact to shape the effectiveness of CBS measures in SCs of manufacturing enterprises.

Blockchain Technology and Cybersecurity Measures

As SCs become more digitised and complex, ensuring the security and authenticity of shared information is critical. BLT has the potential to significantly enhance CBS measures within SCs by providing a decentralised, tamper-proof ledger for data sharing (Kawaguchi, 2019; Bayramova et al., 2021). BLT's cryptographic features and distributed ledger system make it nearly impossible for unauthorised entities to alter or corrupt data, strengthening the CBS posture of organizations and SCs. Empirical studies by Dutta et al. (2020) and Ray et al. (2024) suggest that BLT enables real-time tracking and auditing of SC transactions, reducing the risks of fraud, data breaches, and cyberattacks. Moreover, BLT automates compliance and security protocols by leveraging smart contracts, safeguarding sensitive information. From the theoretical perspective of the DOI theory (Rogers, 1962, 2003), BLT is viewed as an innovative technology that offers relative advantages over traditional, centralized systems for information sharing in SCs. Early adopters of BLT may gain a competitive edge in CBS by detecting and preventing cyber threats more effectively than firms relying on older technologies. As more firms recognize these benefits and adopt BLT, the technology will gradually spread across SCs, facilitating broader improvements in CBS practices.

Aligned with the DOI theory, it can be opined that the gradual diffusion of BLT is driven by its perceived usefulness, ease of integration, and ability to address critical CBS challenges in increasingly interconnected global SCs (Kawaguchi, 2019; Chang et al., 2022).
H_1: BLT positively influences CBS measures.

User-Centric Orientation and Cybersecurity Measures

User-centric orientation (UCO) focuses on tailoring systems and processes to meet the specific needs and preferences of end-users in the design and implementation of security-based measures and interfaces along SCs (Grobler et al., 2021). Studies in this context reveal that companies that align with user behaviours and preferences, and actively seek feedback during the planning and execution of information security practices, are more likely to strengthen their CBS measures (Chaduvula et al., 2018; Agarwal et al., 2022). Besides, fostering greater awareness through training and capacity-building programs ensures stakeholders across the company's SCs comply with CBS measures and become proactive in addressing potential vulnerabilities. This alignment is critical in SCs, where the secure exchange of information heavily depends on user interaction within the network. Supported by the DOI theory (Rogers, 2003), UCO can drive the adoption of innovative CBS measures within SCs. According to the DOI theory, innovative CBS measures are more likely to be adopted when perceived as user-friendly, advantageous, and compatible with existing systems. By focusing on users' needs, UCO makes CBS measures more approachable and relevant, leading to more robust practices as users become more engaged and better equipped with risk mitigation strategies (Morganelli, 2021; Agarwal et al., 2022). Therefore, UCO facilitates the diffusion of CBS measures and strengthens the SC's overall security posture by fostering a culture of active user participation.
H_2: UCO positively influences CBS measures.

The Moderation Role of User-Centric Orientation

Literature regards user-centric orientation (UCO) as a potent enabler of adopting digital technologies such as BLT and CBS measures (Preuveneers et al., 2017; Yadav & Singh, 2020; Nabben, 2021). As organisations adopt BLT to enhance their CBS frameworks, the effectiveness of this implementation, however, can be significantly influenced by how well they align their systems and processes with the needs and preferences of end-users. A strong UCO ensures that the design and application of blockchain solutions incorporate user feedback and prioritise usability, thereby enhancing user engagement and trust in the technology (Sang & Hexmoor, 2021; Preuveneers et al., 2017). According to the diffusion of innovation theory, adopting new technologies, such as BLT, often depends on the perceived ease of use and the extent to which users believe the innovation meets their needs. When firms prioritise a user-centric approach, equipping users with the necessary skills and knowledge while highlighting the benefits of innovative security protocols, they not only facilitate smoother adoption of blockchain solutions but also enhance the overall effectiveness of CBS measures (Al-Farsi et al., 2021; Zhuang et al., 2020). This dynamic suggests that companies with a high level of UCO are more likely to achieve improved outcomes in their CBS efforts when integrated with BLT.
H_3: UCO moderates the relationship between BLT and CBS measures.

Conceptual Framework

The conceptual framework for this study hypothesises that BLT has a positive effect on CBS measures. Blockchain, characterised by its decentralised and transparent nature, enhances security by providing immutable transaction records within the SCs of manufacturing enterprises where data integrity is paramount. However, this relationship is moderated by the level of UCO in the design and implementation of BLT and CBS measures. It is proposed that a higher UCO amplifies the positive effect of BLT on CBS, as enterprises with strong customer-focused strategies are more likely to implement comprehensive security measures to ensure customer trust and data protection. Conversely, lower levels of UCO might weaken this effect, as enterprises that are less focused on

user needs may not fully leverage blockchain's security-enhancing capabilities. Figure 1 illustrates this conceptual framework, where the direct relationship between BLT and CBS measures is moderated by UCO, creating an interaction effect that influences the overall CBS outcomes in manufacturing SCs.

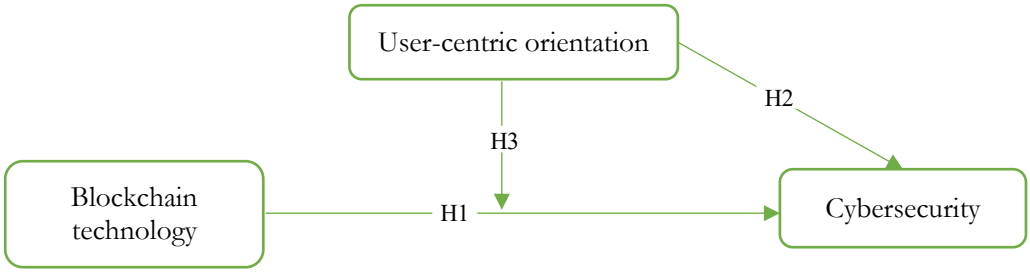


Figure 1. Proposed Conceptual Model
Source(s): Figure by the author

Research Methods

Research Design and Study Area

A cross-sectional quantitative research design was employed to achieve the study's objectives. This design is well-suited for facilitating the statistical testing of hypotheses and assessing causal relationships among variables at a specific time using numerical data (Creswell & Creswell, 2018; Saunders et al., 2019). Similarly, cross-sectional quantitative data were collected for this study from a representative sample across the SCs of large manufacturing enterprises in Dar es Salaam to test the proposed model hypotheses of the interaction effect of BLT and UCO on CBS measures. The selection of Dar es Salaam as the study area was based on two key reasons. First, Dar es Salaam is Tanzania's commercial capital and a central industrial hub, hosting 92 (50.3%) of the country's large manufacturing enterprises (United Nations, 2020). Second, the region has experienced significant growth in ICT infrastructure and the digital economy, increasing integration of digital technologies such as BLT across various sectors, including manufacturing. These factors make Dar es Salaam an ideal location to investigate the interplay of BLT, UCO, and CBS.

Sampling

All 92 large manufacturing enterprises operating in the Dar es Salaam region (United Nations, 2020), along with their SC partners, represented the target population of this study. Specifically, the study focused on the SCs of manufacturing in electrical and electronics, beverages, pharmaceuticals, rubber and plastics, food, machinery, chemicals, and textiles. At each node of these manufacturing SCs, individuals holding managerial positions with relevant knowledge, experience, and orientation in BLT and CBS were selected to participate in the survey as the unit of enquiry. These participants included company managers, potential suppliers, distributors, retailers, and customers. Including this diverse group was essential to ensure an adequate sample, drawing on the unique roles these individuals play as key players in the SCs of manufacturing enterprises (Lelo & Israel, 2024; Rehman et al., 2023). A snowball sampling technique was employed since no sampling frame was available regarding a database of enterprises' and individuals' use of BLT. This approach asked study participants to identify and refer other potential BLT users within their network. Experts involved in a pre-test survey were asked to identify potential BLT users, serving as the starting point for selecting participants in the extensive survey. This approach resulted in an initial sample size of 278 study participants.

Data Collection

This study used a questionnaire survey as the primary data collection method. In essence, 278 study participants were invited to respond to structured questionnaires containing closed-ended

questions related to BLT, UCO, and CBS measures. Questionnaires were distributed to the participants via email between May and July 2024. Of the 278 questionnaires distributed, 229 were returned, 23 were incomplete and thus excluded from the analysis. Consequently, 206 complete responses, representing a response rate of 74.10%, were included in the final analysis. This response rate provided sufficient data for conducting confirmatory factor analysis (CFA) and structural equation modelling (SEM), both of which require a minimum sample size of 200 cases (Hair et al., 2020). Table 1 illustrates the sample characteristics of the study's participants, categorising them based on their sex, academic qualification, work position or role in SC, experience, and industries. The rationale for choosing the questionnaire method was its ability to quickly gather responses from a large sample while minimising bias and administrative costs (Saunders et al., 2019).

Table 1. Overview of Sample Characteristics

Attributes	Category	Frequency (n = 206)	Percent (%)
Sex respondents	Female	88	42.72
	Male	118	57.28
Academic qualification	First degree	74	35.92
	Postgraduate	132	64.08
Years of work experience	3 – 5 years	59	28.64
	6 – 8 years	65	31.55
	9 – 11 years	43	20.87
	12 years and above	39	18.93
Work position or role in SC	Suppliers	41	19.90
	Company managers	47	22.82
	Distributors	59	28.64
	Retailers	36	17.48
	Customers	23	11.17
Types of industry	Electrical and electronics	26	12.62
	Food and beverages	31	15.05
	Pharmaceuticals	33	16.02
	Textiles	39	18.93
	Machinery	21	10.19
	Chemicals	28	13.59
	Rubber and plastics	28	13.59

Source(s): Table by the author

Measures

The questionnaire items used in this study were drawn from prior research. A five-item scale adopted from Rehman et al. (2023) and Maroufkhani et al. (2020) was used to measure the implementation level and perceived benefits of BLT in manufacturing enterprises. To assess user awareness and engagement in blockchain-integrated cybersecurity measures, UCO, a six-item scale was adapted from Friday et al. (2024) and Igbinovia and Ishola (2023). Finally, the CBS construct was measured using a four-item scale adopted from Sindhuja (2014) and Gani et al. (2023), which evaluated cybersecurity practices, risks, and mitigation strategies in SCs of manufacturing enterprises. Table 2 presents the measurement items used in this study. A 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) was used to assess respondents' perceptions and practices for each measurement item. To ensure face and content validity, 16 experts in supply chain and digital technologies were invited to assess the appropriateness of the operationalized items for each construct. Their comments and suggestions were appropriately incorporated into the questionnaire. In addition, a pilot survey involving 56 randomly selected respondents from manufacturing enterprises was conducted to test the reliability of the questionnaire before the final survey. Cronbach's alpha was used to assess the reliability of the constructs, with all constructs demonstrating values above the recommended threshold of 0.70, confirming the questionnaire's appropriateness and reliability (Hair et al., 2020).

Table 2. Measurement Items

Constructs and Items	Sources
Blockchain technology (BLT)	
Blt1. Firm's SC uses BLT to share information among our supply chain partners	Rehman et al. (2023), Maroufkhani et al. (2020)
Blt2. Firm's SC uses BLT to enhance privacy	
Blt3. Firm's SC uses BLT to improve its audit ability	
Blt4. Firm's SC uses BLT to increase operational efficiency	
Blt5. Firm's SC uses BLT to enhance transparency and traceability	
User-centric orientation (UCO)	
Uco1. Firm's SC prioritizes user needs when designing both BLT and cybersecurity interfaces	Friday et al. (2024), Igbinovia & Ishola (2023).
Uco2. Firm's SC involves all users in the design and adoption of BLT and cybersecurity systems	
Uco3. Firm's SC seeks feedback from users on how to improve BLT and cybersecurity systems	
Uco4. The BLT and CBS interfaces and tools are designed in a user-friendly manner	
Uco5. Firm's SC provides adequate training and support services for BLT and cybersecurity	
Uco6. Users are aware of their responsibilities for the security of SC flows	
Cybersecurity (CBS)	
Cbs1. Firm's SC partners have enforced proper physical controls over SC flows	Sindhuja (2014), Gani et al. (2023).
Cbs2. Firm's SC partners have enforced proper access controls over SC flows	
Cbs3. Firm's SC has clear policies and procedures in place to ensure the secure flow of SC	
Cbs4. Firm's SC partners keep each other informed of the threats that may affect the other party	

Source(s): Table by the author

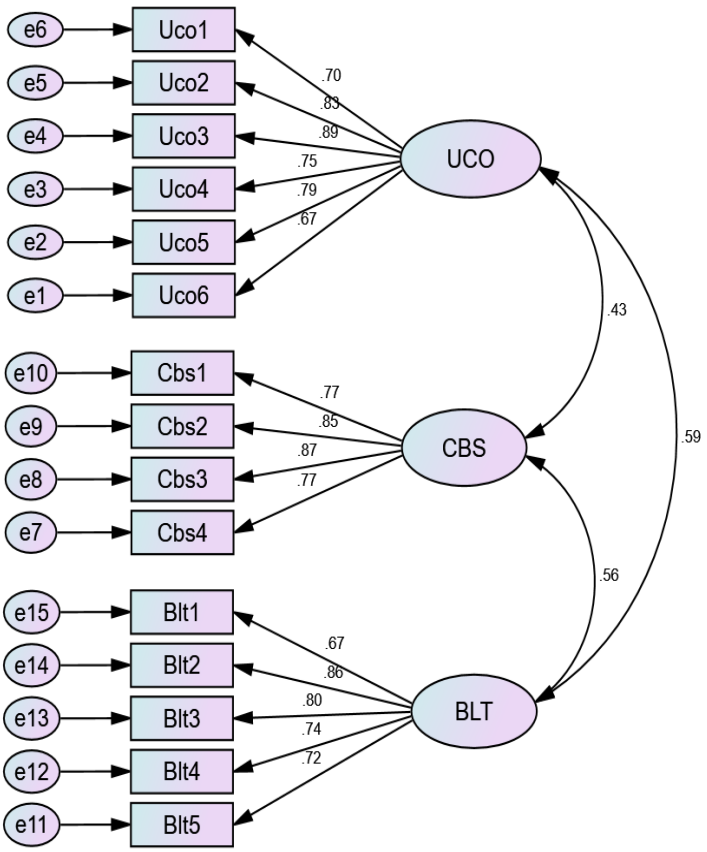
Data Analysis

The quantitative data collected in this study were subjected to CFA using AMOS 23.0 to assess the reliability and validity of the latent variables. CFA is an appropriate tool for testing the measurement model's validity and reliability, ensuring that the observed variables accurately measure the latent constructs (Fan et al., 2016). It helps confirm whether the items used in the survey or data collection instrument adequately represent the latent variables. Hayes' PROCESS macro (model 1) was employed with 5,000 bootstrap samples at a 95% confidence interval to test the proposed model hypotheses regarding the interaction effect of BLT and UCO on CBS. Hayes' PROCESS macro is a robust tool for analysing conditional, mediating, and interaction effects using bootstrapping confidence intervals (Hayes, 2022), making it suitable for the data analysis techniques used in this study.

Results and Discussion

Measurement Model

Figure 2 and Table 3 present the results of the CFA used to assess the measurement model's validity and reliability. The CFA results indicated a good fit of the measurement model to the data, with a Chi-square (χ^2) value of 258.653, $p < 0.000$, degrees of freedom (df) = 89, and a χ^2/df ratio of 2.899. Other model fit indices, as shown in Figure 2, including the Adjusted Goodness of Fit Index (AGFI), Root Mean Square Error of Approximation (RMSEA), Standardized Root Mean Square Residual (SRMR), Goodness of Fit Index (GFI), Root Mean Residual (RMR), Tucker–Lewis Index (TLI), Incremental Fit Index (IFI), Normed Fit Index (NFI), Comparative Fit Index (CFI), and Probability of Close Fit (Pclose), all exhibits marginally acceptable fit statistics that exceed commonly accepted thresholds. These values further confirm that the hypothesised model was tenable and fit the data well.



Note(s): GFI = 0.913, AGFI = 0.856, RMSEA = 0.038, RMR = 0.052, SRMR = 0.044, CFI = 0.942, NFI = 0.907, IFI =0.934, TLI = 0.924 Pclose = 0.067.

Figure 2. Measurement Model
Source(s): Figure by the author.

Table 3. Measurement Model Estimates

Constructs and Items	λ	α	CR	AVE
Blockchain technology (BLT)		0.823	0.872	0.579
Blt1.	0.673			
Blt2.	0.858			
Blt3.	0.804			
Blt4.	0.740			
Blt5.	0.715			
User-centric orientation (UCO)		0.798	0.901	0.606
Uco1.	0.700			
Uco2.	0.835			
Uco3.	0.894			
Uco4.	0.755			
Uco5.	0.789			
Uco6.	0.675			
Cybersecurity (CBS)		0.818	0.890	0.670
Cbs1.	0.773			
Cbs2.	0.850			
Cbs3.	0.872			
Cbs4.	0.774			

Source(s): Table by the author

Table 3 further presents the results of CFA concerning validity and reliability assessment of the measurement model, evaluated using standardized factor loadings (λ), Cronbach's alpha (α), composite reliability (CR), and average variance extracted (AVE). In this case, Cronbach's alpha

and composite reliability values for each research construct exceeded 0.7, indicating good scale reliability (Nawi et al., 2020). In addition, the results demonstrate good convergent validity, with factor loadings for each measurement indicator and the AVE values of all constructs surpassing the recommended threshold of 0.5 (Hair et al., 2020). In Table 4, the results confirm the adequacy of the model's discriminant validity, as the square root of AVE for all constructs was greater than the correlations between each construct and other constructs in the model (Fornell & Larcker, 1981).

Descriptive Statistics and Correlation Analysis

Analysis was performed for descriptive statistics (mean and standard deviation [SD]) and inter-construct correlations (see Table 4). The results indicate a moderate level of CBS measures in the surveyed SCs of manufacturing enterprises (mean score = 3.258, SD = 1.651). UCO has a mean of 3.915 and an SD of 1.587, suggesting a slightly higher user awareness and engagement with digitally enabled security measures and protocols. A mean score of 3.364 and an SD of 1.903 reflect a moderate level of BLT adoption in the SCs of manufacturing enterprises. Moreover, all the correlation coefficients between the study constructs are positively significant, with BLT exhibiting the highest correlation with UCO ($r = 0.588$, $p < 0.01$). These perfect correlations between study variables suggest that the interaction between BLT and UCO enhances CBS. Moreover, as none of the intercorrelation coefficients exceed the critical threshold of 0.70, the analysis indicates no presence of multicollinearity in the dataset (Pallant, 2020).

Table 4. Descriptive Statistics and Pairwise Correlations

	Mean	SD	MSV	ASV	CBS	UCO	BLT
CBS	3.258	1.651	0.316	0.251	*0.818*		
UCO	3.915	1.587	0.346	0.266	0.432**	*0.778*	
BLT	3.364	1.903	0.346	0.331	0.562**	0.588**	*0.761*

Note(s): italicised values denote √AVE > correlation between constructs, ** Correlation is significant at 0.01, CBS = Cybersecurity; UCO = User-centric orientation; BLT = Blockchain technology.
Source(s): Table by the author

Structural Model and Hypotheses Testing

Table 4 presents the results of the Hayes PROCESS macro, which was used to test the direct and interaction effects of the proposed model hypotheses (Figure 1). The model demonstrates strong predictive power, with an R^2 value of 0.462, F-statistic of 2271.257, and $p < 0.001$. This implies that the focal predictor variable (BLT) and the moderator variable (UCO) together account for 46.2% of the variance in the outcome variable (CBS). In addition, the model shows an R^2 change value of 0.021, F-statistic of 4.614, and $p < 0.05$, suggesting that the interaction term (BLT*UCO) increases the variance in the outcome variable and the model's predictive power by 2.1%. The direct relationship analysis reveals that BLT has a significant positive effect on CBS ($\beta = 0.049$, $p < 0.01$), thus supporting hypothesis H1. Similarly, the second hypothesis (H2), which examined the relationship between UCO and CBS, was also supported, as the effect was positive and statistically significant ($\beta = 0.243$, $p < 0.001$). Lastly, the results indicate a significant positive moderation effect of UCO on the relationship between BLT and CBS, with the interaction term (UCO*BLT) showing a coefficient value of $\beta = 0.057$, $p < 0.05$, and confidence intervals that do not include zero (LLCI = 0.003, ULCI = 0.071). Table 5 further shows the effect of BLT on CBS at varying levels of UCO, based on different standard deviation (SD) values. At a low level of UCO, SD –0.789, the effect of BLT is insignificant compared to a significant positive effect at a high level of UCO (SD = 0.789). These results provide support for hypothesis H3. All three of the study's proposed hypotheses were supported, exhibiting significant positive direct relationships and interaction effects between the variables.

Table 5. Regression Results on the Relationships between Study Variables

Variables	Coefficient	Std. error	T-value	P-value	LLCI	ULCI
Constant	2.523	0.010	355.258	0.000	2.504	2.543
BLT → CBS	0.049	0.018	2.708	0.007	0.013	0.085
UCO → CBS	0.243	0.013	71.241	0.000	0.217	0.269
BLT*UCO → CBS	0.057	0.017	2.148	0.033	0.003	0.071
R^2	0.462					
F(sig.)	2271.257			0.000		
R^2 change	0.021					
F(sig.) change	4.614			0.033		
Conditional effects of the focal predictor (BLT) at values of the moderator (UCO)						
Low (-0.789)	0.020	0.025	0.816	0.415	-0.029	0.069
Mean (0.000)	0.049	0.018	2.708	0.007	0.013	0.085
High (0.789)	0.078	0.020	3.850	0.001	0.038	0.118

Note. CBS = Cybersecurity; UCO = User-centric orientation; BLT = Blockchain technology.
Source(s): Table by the author

Discussion

This study investigated how BLT can serve as a precursor to CBS in the SCs of manufacturing enterprises, with the moderating role of UCO. As hypothesized, the findings revealed that BLT has a significant positive direct effect on enhancing CBS. This result aligns with previous empirical studies (Abdelwahed et al., 2024; Gohil & Thakker, 2021) and the theoretical proposition of DOI theory (Rogers, 1962), which suggests that the integration and implementation of blockchain in firms' SCs can significantly improve CBS measures. The possible explanation for this is that BLT provides decentralized and immutable ledger characteristics, which are highly effective in enhancing transparency, preventing cyberattacks, data breaches, and unauthorized data access, thereby reducing vulnerabilities in firms' SCs (Suri et al., 2024; Roy, 2024). Blockchain's ability to offer enhanced data protection, decentralized storage, and immutability makes it a superior tool for securing a firm's SC information and transactions (Singh et al., 2023; Topcu et al., 2024; Kumar et al., 2024). These perceived benefits align with the DOI theory's concept of relative advantage, positioning blockchain as a more effective cybersecurity solution than traditional measures. According to the DOI theory, these advantages will likely accelerate the adoption of blockchain in manufacturing firms, as SC partners recognize it as a more effective solution for preventing cyber threats.

More importantly, the results showed that UCO has a significant positive direct effect on CBS. Consistent with DOI theory, the findings suggest that placing users (such as employees, customers, distributors, and suppliers) at the centre of security design and decision-making leads to stronger and more effective CBS practices. Similar to the empirical findings of Lyon (2024) and Kont (2024), UCO, which focuses on understanding user needs, behaviours, and experiences in intuitive design and implementation, makes CBS protocols more responsive and robust. When CBS systems are designed with user-friendly dashboards or intuitive transaction processes, stakeholders are more likely to understand and trust the technology, leading to increased adoption and enhanced security. Similarly, Renaud and Ophoff (2021) and Alyami et al. (2024) highlighted the significant role of training and awareness in nurturing CBS measures. When users are educated about recognizing potential threats (e.g., phishing attacks) and understand their role in safeguarding their organization's data, the overall CBS posture of the supply chain is strengthened. From a DOI theoretical perspective, UCO is a compatibility approach and communication channel, ensuring that CBS measures align with existing workflows, user needs and values, cultural practices, and the technological infrastructure.

Lastly, this study takes an important step by revealing a significant positive moderating effect of UCO on the relationship between BLT and CBS. Supported by the slope plotting (Figure 3) and the results of conditional effects (Table 5), it is evident that the effect of BLT on CBS is significantly stronger at higher levels of UCO and is insignificant at low levels of UCO. Based on

DOI theory (Rogers, 2003), these findings emphasize the importance of focusing on user needs, experiences, and preferences, complemented by training and awareness initiatives to strengthen the effectiveness of both BLT implementation and CBS measures in supply chains. BLT is often complex, requiring technical expertise and a user-friendly interface. Consistent with prior literature (Aliu et al., 2024; Hashimy et al., 2023), this study establishes that a user-centric approach can simplify user interfaces, tailor features to meet specific user needs, and provide better training or support, ensuring that users are proactive in securing data. While BLT inherently offers security through a decentralized immutable ledger (Abdelwahed et al., 2024), the UCO approach reinforces it by engaging users in understanding and applying security practices (Alyami et al., 2024). Aligned with the DOI theory, it can be argued that UCO facilitates the customisation of CBS measures to address user-specific needs, thereby enhancing the overall effectiveness of blockchain-based security solutions.

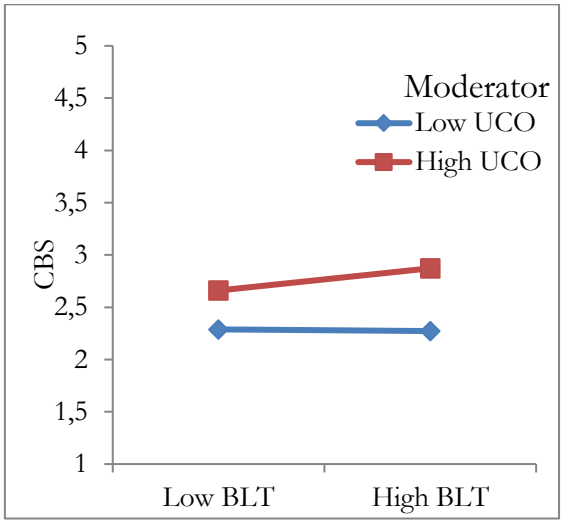


Figure 3. The Slope Plotting for Moderation Effects of UCO on BLT and CBS
Source(s): Figure by the author

Conclusion

The present study used the DOI theory as a theoretical framework to examine the moderating role of UCO in the relationship between blockchain BLT and CBS within the SCs of manufacturing enterprises. A key finding of this research is that the integration of BLT and UCO forms a critical trifecta for enhancing CBS in manufacturing SCs. Both BLT and UCO demonstrated a significant positive direct effect on CBS, with UCO further strengthening the positive impact of BLT on CBS. Thus, the study considers BLT and UCO indispensable for safeguarding sensitive SC data from cyber threats. BLT, in particular, provides secure and immutable data transactions, mitigating risks associated with fraud and inefficiencies, while fostering trust and collaboration among SC participants. On the other hand, UCO ensures that BLT aligns with the needs and expectations of stakeholders, leading to improved trust and commitment to information security. In summary, the integration of BLT and UCO represents a transformative step toward enhancing transparency, efficiency, trust, integrity, and data protection, all of which are key drivers of CBS. Through the lens of DOI theory, this study reveals that manufacturing enterprises are more likely to adopt BLT when they perceive its relative advantage in fostering transparency and traceability, especially when it is user-centred and addresses critical CBS concerns. As such, enterprises that align BLT with users' needs and tackle adoption barriers stand to gain a competitive edge, promoting more resilient, secure, and responsive SCs.

Contribution and Theoretical Implications

Empirically, the study makes significant contributions to the literature in the field of SCM, providing novel insights into how BLT and UCO jointly influence CBS in SCs, which have often

been studied separately but rarely in conjunction within the SCs of manufacturing enterprises. It delves deeper by examining the moderating effect of UCO on the relationship between BLT and CBS, offering a fresh perspective on how cyber risks can be mitigated in decentralized SC networks. Theoretically, the study advances the application of DOI theory in SCM literature by demonstrating how BLT adoption can be driven by both users' needs and security concerns, thus providing valuable implications for technology diffusion models in the manufacturing context. In this study, blockchain is revealed as a security-innovation-based technology that enhances traceability, transparency, trust, and the security of SC information. However, the diffusion of BLT and CBS measures highly depends on user-centric environments. Drawing on the compatibility and trialability aspects of DOI theory and study findings, it can be suggested that when BLT addresses the specific needs of SC users (both internal, like employees, and external, like customers and suppliers), it is more likely to be adopted rapidly, thereby strengthening the effect of BLT on CBS measures. Essentially, UCO reduces the perceived complexity of blockchain systems by providing intuitive interfaces and solutions aligned with user preferences, thus facilitating its adoption and enhancing security measures. This interplay offers a multidisciplinary perspective by linking BLT with human-centred approaches and cyber protection in the context of manufacturing enterprises, particularly in the era of Industry 5.0.

Managerial Implications

The study provides several managerial implications for how enterprise managers, support organisations, and policymakers can leverage BLT and UCO to enhance data security within the SCs of manufacturing enterprises. Given the significant direct effect of BLT on CBS, the study recommends that managers strengthen CBS protocols to protect sensitive SC data from external threats. This can be achieved by implementing multi-factor authentication and encryption-based access controls, which safeguard critical information, ensure data integrity and confidentiality, and minimize vulnerabilities that could lead to SC disruptions. Furthermore, the study suggests that managers should design and implement customized blockchain and cybersecurity solutions, focusing on the specific needs of both internal end-users and external stakeholders. This is essential to ensure these technologies enhance security and streamline processes, reducing the friction of their adoption and use. Considering the complex nature of BLT and CBS systems, the study recommends that managers, support organizations, and policymakers invest in continuous training and skill development programs. These programs would equip employees and stakeholders within manufacturing SCs with the technical expertise needed to manage and adopt BLT and security protocols effectively. Additionally, fostering a collaborative environment that encourages seamless data sharing and cybersecurity measures among SC participants, such as suppliers, manufacturers, and logistics providers, can further enhance the system. This collaborative approach helps reduce inefficiencies, facilitates shared experiences, and promotes effective adoption of BLT, UCO, and CBS protocols.

Study Limitations and Future Directions

The study has some limitations that can be exploited in further research. Firstly, the study focuses primarily on manufacturing enterprises, which may limit the generalizability of its findings to other sectors, such as retail or service industries, where SC dynamics, technology adoption, and security measures may differ significantly. In light of this, future research could extend beyond manufacturing to explore how BLT and UCO impact CBS in SCs of other sectors such as healthcare, retail, or financial services. Secondly, the study is geographically confined to the Dar es Salaam region of Tanzania, limiting the scope of blockchain adoption, UCO, and CBS practices to a specific region. This may not reflect global variations in SC practices. Consequently, conducting comparative studies across different regions and countries could offer a broader perspective on how BLT and UCO influence CBS effectiveness in SCs on a global scale. Thirdly, the study's findings are based on the current state of BLT and user needs, which could quickly become outdated as technology and CBS threats evolve. This limits the study's ability to predict future vulnerabilities and how they will be affected by blockchain-enabled SCs and UCO. Conducting

longitudinal studies would offer valuable insights into the long-term effects of integrating BLT, UCO, and CBS in SCs, allowing for a better understanding of evolving risks and benefits. In addition, exploring the potential role of artificial intelligence (AI) in enhancing the effectiveness of BLT and CBS in supply chain management presents another promising avenue for future research.

References

Abdelwahed, N. A. A., Al Doghan, M. A., Saraih, U. N., & Soomro, B. A. (2024). The predictive robustness of organizational and technological enablers towards blockchain technology adoption and financial performance. *Kybernetes*. https://doi.org/10.1108/K-09-2023-1655

Agarwal, U., Rishiwal, V., Tanwar, S., Chaudhary, R., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Blockchain technology for secure supply chain management: a comprehensive review. *IEEE Access, 10*, 85493-85517. https://doi.org/10.1109/ACCESS.2022.3194319

Aliu, J., Oke, A. E., Akinwumi, I. I., Abdulazeez Kanya, R., & Uyi Ehiosun, L. (2024). Scrutinizing the level of awareness and adoption of distributed ledger technology in the Nigerian construction industry. *Technological Sustainability*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/TECHS-01-2024-0003

Al-Farsi, S., Rathore, M. M., & Bakiras, S. (2021). Security of blockchain-based supply chain management systems: challenges and opportunities. *Applied Sciences, 11*(12), 5585. https://doi.org/10.3390/app11125585

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2024). Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives. *Information and Computer Security, 32*(1), 53-73. https://doi.org/10.1108/ICS-08-2022-0133

Bayramova, A., Edwards, D. J., & Roberts, C. (2021). The role of blockchain technology in augmenting supply chain resilience to cybercrime. *Buildings, 11*(7), 283. https://doi.org/10.3390/buildings11070283

Calle, G., DiCaprio, A., Stassen, M., & Manzer, A. (2019). Can blockchain futureproof supply chains? a Brexit case study. In Choi, J. J., & Ozkan, B. (Eds.), *Disruptive Innovation in Business and Finance in the Digital World* (International Financial Review Vol. 20, pp. 101-122). Leeds: Emerald Publishing Limited. https://doi.org/10.1108/S1569-376720190000020013

Chaduvula, S. C., Dachowicz, A., Atallah, M. J., & Panchal, J. H. (2018). Security in cyber-enabled design and manufacturing: a survey. *Journal of Computing and Information Science in Engineering, 18*(4), 040802. https://doi.org/10.1115/1.4040341

Chang, A., El-Rayes, N., & Shi, J. (2022). Blockchain technology for supply chain management: a comprehensive review. *FinTech, 1*(2), 191-205. https://doi.org/10.3390/fintech1020015

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 5th ed.* Los Angeles: Sage Publications, Inc.

Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: applications, challenges and research opportunities. *Transportation Research Part E, 142*, 102067. https://doi.org/10.1016/j.tre.2020.102067

Fan, Y., Chen, J., Shirkey, G., John, R., Wu, S. R., Park, H., & Shao, C. (2016). Applications of structural equation modelling (SEM) in ecological studies: an updated review. *Ecological Processes, 5*(1), 1–12. https://doi.org/10.1186/s13717-016-0063-3

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. https://doi.org/10.1177/002224378101800104

Friday, D., Melnyk, S. A., Altman, M., Harrison, N., & Ryan, S. (2024). An inductive analysis of collaborative cybersecurity management capabilities, relational antecedents and supply chain cybersecurity parameters. *International Journal of Physical Distribution & Logistics Management, 54*(5), 476-500. https://doi.org/10.1108/IJPDLM-01-2023-0034

Gani, A. B. D., Fernando, Y., Lan, S., Lim, M. K., & Tseng, M. -L. (2023). 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

Gohil, D., & Thakker, S. V. (2021). Blockchain-integrated technologies for solving supply chain challenges. *Modern Supply Chain Research and Applications, 3*(2), 78-97. https://doi.org/10.1108/MSCRA-10-2020-0028

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: redefining human centric cyber security. *Frontiers in Big Data, 4*, 583723. https://doi.org/10.3389/fdata.2021.583723

Hair, J. F., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of Business Research, 109*, 101–110. https://doi.org/10.1016/j.jbusres.2019.11.069

Hayes, A. F. (2022). *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach, 3rd ed.* New York: The Guilford Press.

Hashimy, L., Jain, G., & Grifell-Tatjé, E. (2023). Determinants of blockchain adoption as decentralized business model by Spanish firms – an innovation theory perspective. *Industrial Management & Data Systems, 123*(1), 204-228. https://doi.org/10.1108/IMDS-01-2022-0030

Hong, L. and Hales, D.N. (2024). How blockchain manages supply chain risks: evidence from Indian manufacturing companies. *The International Journal of Logistics Management, 35*(5), 1604-1627. https://doi.org/10.1108/IJLM-05-2023-0178

Igbinovia, M. O., & Ishola, B. C. (2023). Cyber security in university libraries and implication for library and information science education in Nigeria. *Digital Library Perspectives, 39*(3), 248-266. https://doi.org/10.1108/DLP-11-2022-0089

Israel, B. (2022). Enhancing customer retention in manufacturing SMEs through supply chain innovative practices. *Management Dynamics in the Knowledge Economy, 10*(3), 272-286.

Kaspersky (2021). *Kaspersky Security Bulletin Statistics*. Moscow: Kaspersky.

Kawaguchi, N. (2019). Application of blockchain to supply chain: flexible blockchain technology. *Procedia Computer Science, 164*, 143-148. https://doi.org/10.1016/j.procs.2019.12.166

Kont, K. -R. (2024). Management of cyber risks in the library: analysis of information security awareness of Estonian library employees. *Library Management, 45*(1/2), 118-140. https://doi.org/10.1108/LM-07-2023-0058

Kumar, J., Rani, G., Rani, M., & Rani, V. (2024). Blockchain technology adoption and its impact on SME performance: insights for entrepreneurs and policymakers. *Journal of Enterprising Communities: People and Places in the Global Economy*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JEC-02-2024-0034

Lelo, J. M., & Israel, B. (2024). Supply chain innovative practices and customer satisfaction: insights from manufacturing SMEs. *Management Dynamics in the Knowledge Economy, 12*(1), 54-69.

Lyon, G. (2024). Informational inequality: the role of resources and attributes in information security awareness. *Information and Computer Security, 32*(2), 197-217. https://doi.org/10.1108/ICS-04-2023-0063

Morganelli, C. R. (2021). *Exploring User-Centric Innovation in the Design of Information Security Awareness Programs in Health Care: A Case Study*. Doctoral Dissertation, Capella University, Minneapolis.

Nabben, K. (2021). Blockchain security as "people security": applying sociotechnical security to blockchain technology. *Frontiers in Computer Science, 2*, 599406. https://doi.org/10.3389/fcomp.2020.599406

Nawi, F. A., Tambi, M. A., Samat, M. F., & Mustapha, W. M. (2020). A review on the internal consistency of a scale: the empirical example of the influence of human capital investment on Malcom Baldridge quality principles in TVET institutions. *Asian People Journal, 3*(1), 19-29. https://doi.org/10.37231/apj.2020.3.1.121

Nicoletti, B., & Appolloni, A. (2024). Digital transformation in ecosystems: integrated operations model and its application to fifth-party logistics operators. *Journal of Global Operations and Strategic Sourcing*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JGOSS-04-2023-0024

Pallant, J. (2020). *SPSS Survival Manual: A Step-by-step Guide to Data Analysis using IBM SPSS (7th ed.)*. London: Routledge.

Preuveneers, D., Joosen, W., & Ilie-Zudor, E. (2017). Trustworthy data-driven networked production for customer-centric plants. *Industrial Management & Data Systems, 117*(10), 2305-2324. https://doi.org/10.1108/IMDS-10-2016-0419

Ray, R. K., Chowdhury, F. R., & Hasan, M. R. (2024). Blockchain applications in retail cybersecurity: enhancing supply chain integrity, secure transactions, and data protection. *Journal of Business and Management Studies, 6*(1), 206-214. https://doi.org/10.32996/jbms.2024.6.1.13

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People, 1*(1), 24-46. https://doi.org/10.1108/OCJ-03-2021-0004

Roy, S. (2024). Blockchain Technology in the Global Supply Chain: A Theoretical Overview and Security Issues. In Bhattacharyya, R., & Mazumdar, D. (Eds.), *Contemporary Issues in International Trade* (pp. 195-208). Leeds: Emerald Publishing Limited. https://doi.org/10.1108/978-1-83797-320-020241012

Sang, L., & Hexmoor, H. (2021). Information-centric blockchain technology for the smart grid. *International Journal of Network Security & Its Applications, 13*(3), 27-42. https://doi.org/10.5121/ijnsa.2021.13303

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students, 8th ed.* Harlow: Pearson Education Limited.

Singh, S., Singh, S., & Kajla, T. (2023). Checking the Effectiveness of Blockchain Application in Fraud Detection with A Systematic Literature Review Approach. In Grima, S., Sood, K., & Özen, E. (Eds.), *Contemporary Studies of Risks in Emerging Technology, Part B (Emerald Studies in Finance, Insurance, and Risk Management)* (pp. 57-86). Leeds: Emerald Publishing Limited. https://doi.org/10.1108/978-1-80455-566-820231003

Sindhuja, P. N. (2014). Impact of information security initiatives on supply chain performance. *Information and Computer Security, 22*(5), 450-473. https://doi.org/10.1108/IMCS-05-2013-0035

Raj, R., Singh, A., Kumar, V., & Verma, P. (2024). Challenges in adopting blockchain technology in supply chain management: a too farfetched idea? *International Journal of Quality & Reliability Management, 41*(8), 2146-2180. https://doi.org/10.1108/IJQRM-12-2022-0366

Rehman, S. U., Usman, M., Fernando, Y., Kamarudin, D., & Waheed, A. (2023). Improving manufacturing supply chain performance: nexus of industrial Internet of Things, blockchain technology and innovativeness. *Journal of Science and Technology Policy Management*, Vol. ahead-of print No. ahead-of-print. https://doi.org/10.1108/JSTPM-12-2021-0191

Rogers, E. (2003). *Diffusion of Innovations, fifth edition*. New York: Free Press.

Rogers, E. (1962). *Diffusion of Innovations*. New York: The Free Press.

Rauniyar, K., Wu, X., Gupta, S., Modgil, S., & Lopes de Sousa Jabbour, A. B. (2023). Risk management of supply chains in the digital transformation era: contribution and challenges of blockchain technology. *Industrial Management & Data Systems, 123*(1), 253-277. https://doi.org/10.1108/IMDS-04-2021-0235

Suri, A., Sharma, Y., Jindal, L., & Sijariya, R. (2024). Blockchain for data protection and cyber fraud reduction: systematic literature review and technology adoption dynamics among gen Y and Z. *International Journal of Quality & Reliability Management, 41*(80), 2181-2198. https://doi.org/10.1108/IJQRM-03-2023-0094

Tarde, G. (1903). *The Laws of Imitation*. Peter Smith by permission of Henry Holt & Company. Clouchester, Massachusetts.

Topcu, Y. E., Can, İ. E., & Özçınar, A. (2024). Blockchain technology in foreign trade management: which blockchain alternative is more suitable? *Digital Policy, Regulation and Governance, 26*(2), 121-134. https://doi.org/10.1108/DPRG-05-2023-0064

United Nations (2020). *Tanzanian Industrial SMEs Cluster Mapping Report*. Climate Technology Centre and Network. Nairobi, Kenya.

Yadav, S., & Singh, S. P. (2020). Blockchain critical success factors for sustainable supply chain. *Resources, Conservation and Recycling, 152*, 104505. https://doi.org/10.1016/j.resconrec.2019.104505

Zhuang, P., Zamir, T., & Liang, H. (2020). Blockchain for cybersecurity in smart grid: a comprehensive survey. *IEEE Transactions on Industrial Informatics, 17*(1), 3-19. https://doi.org/10.1109/TII.2020.2998479