International Journal of Business Strategy and Financial Markets
Vol. 1 No. 1 (2025): Volume 1, Issue 1
ISSN:
DOI:
Journal homepage: https://iaglobalpub.org/index.php/IJBSFM
Research article

Evaluation of the management of supply chain cybersecurity risks via the application of innovative technologies – The case of Walmart China Blockchain Traceability Platform

Wei Huang[1]*

[1] School of Information Management and Engineering, Shanghai University of International Business and Economics, Shanghai, China

**Corresponding author: Wei Huang, email: Josephh0617@hotmail.com*

Abstract

This study investigates the application of blockchain technology in managing cybersecurity risks within food retail supply chains, focusing on Walmart China's Blockchain Traceability Platform (WCBTP). The aim of the research is to explore potential cybersecurity threats, evaluate the impacts of such threats on supply chain operations and corporate reputation, assess the effectiveness of blockchain technology in mitigating these risks, and propose recommendations for future applications of blockchain technology within the food retail supply chain sector. Using a qualitative research design, the study adopted a case study approach and gathered data through surveys conducted with 20 participants involved in the implementation and management of the WCBTP. The collected data were analysed using thematic analysis to categorize the key themes and insights related to the research objectives. The findings revealed several key cybersecurity risks within Walmart's supply chain, including unauthorized access, data breaches, and system vulnerabilities. The impacts of these threats on supply chain operations included operational disruption, threat to data integrity, and potential financial implications. The study also found that the application of blockchain technology within the WCBTP has been instrumental in managing these risks, with participants noting the benefits of features such as encryption, decentralization, and immutability. Despite the challenges associated with the technical complexity of blockchain and integration issues, several key factors were identified that contributed to the successful implementation of the WCBTP system. These included technical expertise, regular security assessments, stakeholder commitment and effective communication. The study concludes with recommendations for future applications of blockchain technology within food retail supply chains, emphasizing the importance of continuous learning and adaptation, robust security measures, rigorous testing and evaluation, and stakeholder involvement. The research contributes to the growing body of literature on the intersection of supply chain management, cybersecurity, and blockchain technology, providing valuable insights for both academics and practitioners.

Received: June 23, 2025. **Revised:** August 26, 2025. **Editorial decision**: September 3, 2025. **Accepted**: September 9, 2025

Keywords: blockchain technology; cybersecurity risks; food retail supply chain; Walmart China; traceability platform; supply chain management; data integrity; decentralization

1. Introduction

Supply chain cybersecurity risks have become a critical issue in recent years as organizations are increasingly relying on technology to manage their supply chains. According to Perwej et al (2021), cyber-attacks can lead to data breaches, intellectual property theft, and disruption of business operations, resulting in significant financial losses and reputational damage. To mitigate these risks, organizations are actively exploring innovative technologies such as blockchain to secure their supply chains, as it is found to be commonly employed across supply chain and financial applications as shown in figure 1 (World Economic Forum, 2022). As one of the largest supermarket retailers in the world with operations in over 27 countries, Walmart has been at the forefront of using blockchain to secure its supply chain (Forbes, 2019). In late 2018, Walmart began developing a blockchain based system to track food products from suppliers to its stores, which reduced the time it took to trace the origin of food products from several days to just seconds (Tan et al, 2018). In a pilot project with PwC China and blockchain based supply chain management platform VeChain (VET), the Walmart China Blockchain Traceability Platform (WCBTP) was developed and launched in 2019, allowing supply chain actors and customers to access detailed information of the origin of products by scanning QR codes printed on its product packaging, addressing "long term pain points in fresh food logistics, product information transparency, visibility and cybersecurity" (Hang, 2020).

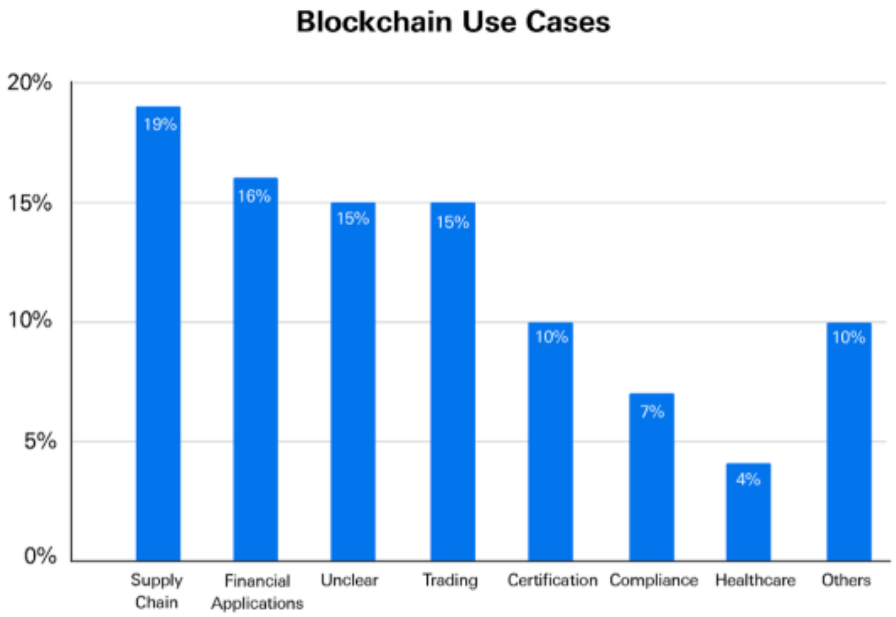

Figure 1: Most common blockchain use cases (World Economic Forum, 2022)

According to Xu et al (2020), the WCBTP represents a notable initiative in supply chain management by using blockchain technology to enhance traceability, transparency and efficiency, marking significant progress in advancing supply chain security and transparency in the retail industry. The WCBTP employs a blockchain decentralized ledger system to trace the origins, processing, and distribution of products, providing a seamless and robust means to verify data at every point in the supply chain. The fact that each transaction on the blockchain is immutable and timestamped means that the platform is highly resistant to data tampering and fraud (Qian et al, 2020). By the end of 2020, Walmart China had reportedly incorporated 23 product lines into the WCBTP and anticipated the platform to track and trace approximately 50% of its packed fresh meat sales, 40% of its vegetables, and 12.5% of its seafood by the end of 2021 (Walmart, 2021). This level of product tracking and data transparency not only enhances consumer confidence but also deters ill-intentioned actors who could exploit traditional supply chains' opacity (Hassija et al, 2020).

In terms of cybersecurity, the distributed nature of the blockchain network means there's no single point of failure, whereby in the event of one node being compromised in a blockchain network, the rest of the system remains secure, overcoming the limitations of traditional centralised supply chain systems and greatly reduces the potential for catastrophic data breaches (Etemadi et al, 2021). Additionally, since blockchain uses cryptographic principles for data protection, it ensures that transaction data is secure, confidential and integral (Xi et al, 2022). The case study of Walmart's WCBTP system presents a unique opportunity to explore the effectiveness of blockchain in managing supply chain cybersecurity risks. The application of innovative technologies to address the increasing vulnerability against cybersecurity risks in supply chain has become a major trend due to major high-profile scandals in recent years (Hached, 2021), including Marriott's data leak in 2020 due to compromised third party apps, SolarWind's supply chain cyberattack in 2020 and JBS Food's ransomware attack in 2021 which had caused global supply chain disruptions. A large number of supply chain cybersecurity scandals highlight the growing importance of managing cybersecurity risks in the supply chain and the need for innovative technologies such as blockchain to secure supply chain operations (Hached, 2021).

1.1 Research problem/ rationale

This research aims to address the problem related to increasing cybersecurity risks in supply chain management and explore the effectiveness of blockchain technology in mitigating these risks, using Walmart's WCBTP system as a case study. The problem of cybersecurity risks in supply chain management has become critical in recent years, as organizations are increasingly relying on technology to manage their supply chains (Hached, 2021). The traditional supply chain management systems lack the ability to provide end-to-end visibility and transparency in the supply chain, which makes it difficult to trace and identify the source of the cyber-attack (Perwej

et al, 2021). To mitigate these risks, organizations are exploring innovative technologies such as blockchain to secure their supply chains. Blockchain provides a decentralized, transparent, and tamper-proof platform that enables secure data exchange and transaction processing, ensuring that each transaction is verified by all participants in the network, eliminating the need for intermediaries and reducing the risk of cyber-attacks (Xi et al, 2022).

However, there is a lack of empirical evidence in recent literature on the effectiveness of blockchain in managing supply chain cybersecurity risks especially with emergence of the nascent blockchain technologies (Etemadi et al, 2021). Existing studies have mainly focused on the technical aspects of blockchain, such as its scalability and interoperability, and have neglected its impact on cybersecurity risks when applied towards the supply chain management of agriculture-food industries (Bhat et al, 2021). This rationale behind this research is to fill this gap in the literature by exploring the effectiveness of blockchain in managing supply chain cybersecurity risks via the case study of Walmart's WCBTP system. By addressing this research problem, the study contributes to the development of knowledge on supply chain cybersecurity risks and blockchain technology. Additionally, the justification for this study lies in the critical need to address the increasing supply chain cybersecurity risks faced by organizations, as well as the growing importance of blockchain technology as a solution to these risks.

While there have been studies on the application of blockchain technology in supply chain management (Cole et al, 2019; Gurtu & Johny, 2019), there is a lack of research on the effectiveness of blockchain in managing cybersecurity risks in food/ retail supply chains (Bhat et al, 2021). The research findings will provide valuable insights to organizations in different industries, policymakers and researchers, evaluating the effectiveness of blockchain in mitigating supply chain cybersecurity risks and make informed decisions regarding its implementation. Overall, this research will contribute to the improvement of supply chain security and resilience, which is essential for the sustainability of businesses and the global economy.

1.2 Research aims and objectives

The main aim of this research project is to investigate the effectiveness of blockchain application in managing supply chain cybersecurity risks, using the case study of Walmart's WCBTP system. The project seeks to explore how blockchain technology can enhance the security and resilience of supply chains, by providing a tamper-proof and decentralized system for tracking and verifying the movement of goods and information. The study will also seek to identify the specific cybersecurity risks that are prevalent in modern supply chains and how blockchain can be used to address these risks. By achieving these aims, the research project will contribute to the growing body of knowledge on supply chain management and cybersecurity, and provide insights that can inform the development of best practices for securing supply chains in the face of cyber threats. To achieve this aim, the research will focus on four specific objectives:

1. To investigate and categorise potential cybersecurity threats in food retail supply chains through integrating a broad review of academic literature and an in-depth investigation of the Walmart case study.
2. To critically evaluate the impacts of cybersecurity risks on supply chain operations and corporate reputation, exploring the repercussions of these threats on the functioning of supply chain operations in a holistic manner.
3. To examine the efficiency of blockchain technology applications in mitigating cybersecurity risks within Walmart's supply chain, evaluating the practical effectiveness of using blockchain as a tool to enhance supply chain security.
4. To propose recommendations and strategies for organisations aiming to integrate or apply blockchain technologies to manage cybersecurity threats in their supply chains, drawing upon potential implementation challenges and corresponding mitigation strategies.

1.3 Research question

How can the application of blockchain technologies help Walmart overcome cybersecurity risks across its supply chain activities?

1.3.1 Research sub-questions

1. What cybersecurity risks and threats does Walmart's supply chain encounter?
2. What are the effects of cybersecurity risks on the supply chain operations and corporate reputation of Walmart?
3. How do Walmart's supply chain department employees perceive the effectiveness of the blockchain-based system in managing cybersecurity risks?
4. What challenges did Walmart face during the implementation of the blockchain technology in their supply chain management, and what strategies were employed to surmount these challenges?
5. What are the key factors influencing the adoption and successful implementation of blockchain technology in supply chains, and how can these factors be leveraged to bolster supply chain cybersecurity management?

1.4 Research significance

As the dependence on technology in supply chain management grows, organizations are increasingly exposed to risks such as data breaches, intellectual property theft, and disruption of business operations. In light of the research objectives, this study aims to provide a comprehensive understanding of the benefits and challenges associated with adopting blockchain technology for managing supply chain cybersecurity risks. This will enable organizations to make informed decisions regarding the implementation of this technology. The study's impact on Walmart is twofold. Firstly, by evaluating the effectiveness of Walmart's blockchain-integrated supply chain, the research will offer insights into the company's effectiveness in safeguarding its supply chain from cybersecurity threats. Secondly, the research findings may hold implications for the broader supermarket industry. As a pioneer in supply chain management practices, Walmart's adoption of blockchain technology could serve as a benchmark for other retailers. Moreover, the study contributes to the existing body of knowledge by addressing the literature gap on the effectiveness of blockchain technology in mitigating supply chain cybersecurity risks. While previous studies have explored the application of blockchain in supply chain management, research focusing on its effectiveness in managing cybersecurity risks remains scarce. This study will delve into the practical effectiveness and challenges of adopting blockchain technology for managing supply chain cybersecurity risks, enriching the academic literature on the subject.

1.5 Alignment to MSc Programme

The proposed research aligns with the core principles of the University of Warwick's MSc Supply Chain Management degree, focusing on risk management, supply chain optimization, and the use of innovative technologies like blockchain. This study offers invaluable insights into effective management of supply chain cybersecurity risks, important knowledge for any future supply chain professional. Moreover, the research will provide practical experience in critical thinking, problem-solving, and data analysis, contributing to the development of essential research skills. Finally, the emphasis on innovative technologies as a means to achieve sustainable supply chains reflects the University of Warwick's commitment to sustainability and responsible business practices.

1.6 Structure of study

This study begins with the introduction (Chapter 1), providing an overview of the study, including the background, rationale, aims, objectives, and research questions. It also delineates the significance of the study to both academia and industry. Following the introduction, a thorough exploration of existing academic and industry literature on the topic is presented in the literature review (Chapter 2). This chapter grounds the study in existing knowledge, identifying gaps and opportunities for further exploration. The third chapter outlines the methodology adopted in this study, detailing the research design, data collection, and analysis methods used. The results and

findings (Chapter 4) subsequently presents the data gathered, followed by an in-depth discussion (Chapter 5) interpreting these results in the context of the research objectives and existing literature. The study concludes with the final chapter, providing the conclusion and limitations of the study. This chapter synthesizes the research findings, offers insights into the implications of the study, and discusses any limitations encountered during the research process.

2. Literature review

This chapter presents a thorough review of the literature surrounding cyber supply chain risk management (C-SCRM), cybersecurity threats in supply chains, and the role of blockchain technology. Section 2.1 unpacks the concept of C-SCRM, consolidating key definitions and theories from extant literature. Following this, Section 2.2 provides an in-depth analysis of cybersecurity threats in supply chains, exploring their causes and potential impacts on supply chain operations and organizational reputation. Section 2.3 discusses the defining characteristics of blockchain, exploring its potential applications within the realm of C-SCRM from empirical studies. The final section of this chapter encapsulates key insights drawn from the literature review, identifies existing knowledge gaps, and presents the theoretical framework that underpins the subsequent research. The structured approach taken in this chapter aims to establish a robust knowledge foundation for an informed analysis of the Walmart China Blockchain Traceability Platform (WCBTP).

2.1 Cyber supply chain risk management (C-SCRM) definition

The management of cybersecurity risks within supply chains has been the focus of burgeoning research attention in recent years, as reflected by the emerging concept of cyber supply chain risk management (C-SCRM) in academic literature (Ghadge et al 2020). According to Boyson (2014), C-SCRM is a dynamic phenomenon resulting from the fusion of cybersecurity, enterprise risk management and supply chain management, representing a multifaceted construct that encapsulates the fusion of diverse approaches, methodologies and practices across these disciplines. Furthermore, Creazza et al. (2022) suggests that this hybrid discipline focuses on the development and implementation of strategies, emphasising on programmatic activities geared towards the assessment and mitigation of risks across the end-to-end processes inherent within the supply chains for IT networks, hardware, and software systems in the digital transformation era. Since the turn of the 21st century, increasing research attention has been dedicated on conceptualizing the definitions and practices of C-SCRM (Harrington et al. 2018; Boyson, 2014; Windelberg, 2016), Moreover, Boyson's (2014) conceptualization of C-SCRM to include the representative practices of enterprise risk management, supply chain management and cybersecurity as shown in figure 2 below remains a widely accepted definition amongst academicians (Cheung et al. 2021; Ghadge et al. 2020).

Discipline	Representative practices
1. Enterprise Risk Management	**Executive risk group**, composed of chief risk officer and members of board of directors and strategic business units, created to set objectives and guide enterprise risk management program development Probablistic methods of analysis (such as Monte Carlo simulations) employed to assess the likelihood and severity of impact of enterprise risks Ongoing audit methodologies used to track the timeliness and effectiveness of risk mitigation activities
2. Supply Chain Management	**Corporate supply chain group**, composed of chief supply chain officer and unit directors for demand planning, sourcing, manufacturing, and distribution, set supply chain-wide policies for demand/supply balancing and ensure process integration across units and with extended enterprise partners Use of sophisticated supply chain mapping/network design tools to ensure maximum efficiency in the establishment of production and distribution points worldwide Use of enterprise resource planning (ERP) systems to fuse disparate planning and production data into a unified, real-time database Use of radio-frequency identification (RFID), digital locks, and other tracking technologies to assure end-to-end visibility of high-value goods in transit
3. Cybersecurity	**IT security group**, composed of a chief information security officer and technical representatives of operating units, sets security policy and assures compliance with key practices Compliance areas include Federal Information Processing Standards (FIPS) certification of cryptographic features Bolster IT network "perimeter defenses" through enhanced intrusion-detection systems Common criteria standards for security of systems, products, and services Build or buy better IT threat-analysis capabilities Screen software code or hardware from offshore prior to domestic integration Increase sourcing from pre-certified "trusted" vendors of IT hardware and software

Figure 2: Representative practices of C-SCRM (Boyson, 2014, p2)

The National Institute of Standards and Technology (NIST, 2016) defines C-SCRM as the process of identifying, assessing and mitigating the risks associated with the distributed and interconnected nature of IT products and service supply chains. This definition emphasizes the ongoing nature of C-SCRM and the need to manage the entire lifecycle of IT products and services, including hardware, software and information assurance (Jaikaran, 2018). Alternatively, Baldwin's (2022) cross-sectional survey of key C-SCRM practices recognized under the NISTIR 8276 recognizes that many practitioners define C-SCRM as a systematic process for managing exposure to cybersecurity risks throughout the supply chain, highlighting the importance of reducing the likelihood of supply chain compromise by improving an organization's ability to detect, respond and recover from disruptions. The academic definitions of C-SCRM are criticized by Boyens et al. (2020) to offer limited representation of its dynamic nature, challenging for the need to recognize its inevitable state of constant evolution due to continuous technological advancements, changing threat actors, strategies and shifts in regulatory landscapes to maintain an effective supply chain. Nonetheless, Boyson's (2014) multifaceted approach to conceptualise C-SCRM practices offer a thorough understanding of its practices and hence would serve the knowledge foundation for this study, despite apparent room for improvement for further refinement that can fully encompass its complexity, scope and constantly evolving nature according to Topping et al. (2021).

2.1.1 Theoretical background of C-SCRM

The theoretical underpinnings of C-SCRM draws upon multiple frameworks, theories and academic concepts, reflecting an interdisciplinary approach that incorporates the complexities associated with effectively managing cyber risks in supply chains (Nygard & Katsikas, 2022). Several academic theories underpin the concept of C-SCRM, lending credence to the multi-

disciplinary approach it entails. According to Gani et al (2022) the contingency theory posits that the effectiveness of C-SCRM practices hinges on the specific contexts and conditions they are applied within, emphasizing the customization of such practices to suit each organization's unique characteristics. Alternatively, Fan & Stevenson (2018) applied the resource-based view (RBV) theory to explore the competitive advantage needs of C-SCRM, drawing upon the theoretical foundation of RBV that suggests the leverage of unique firm resources and capabilities to pursue operational gains. According to Fan & Stevenson (2018), the RBV theory underscores the importance of developing valuable resources such as cybersecurity expertise, technology, and processes to effectively manage cyber supply chain risks.

Moreover, Hampton et al (2021) applied the theoretical foundations of the risk management theory in the context of C-SCRM, providing a solid framework for understanding and addressing the complex challenges posed by cyber risks within supply chains. This theoretical perspective emphasizes the importance of a proactive and comprehensive approach to risk management, encompassing the identification, assessment, treatment, and monitoring of risks by considering risk management as an integral part of supply chain strategies, as organizations can effectively respond to and mitigate potential threats accordingly (Hampton et al, 2021). Another approach adopted by Boyson (2014) incorporated elements of cybersecurity, supply chain management, and enterprise risk management, engaging C-SCRM as an integrative discipline to facilitate better comprehension and management of complex risks associated with cyber supply chains. Gurtu & Johny (2021) further expanded upon Boyson's (2014) integrative approach by proposing a systematic and phased approach to conceptualise the dynamics of C-SCRM, involving the phases of recognizing the nature and severity of risks, evaluating potential impacts on supply chain, ranking risks based on their significance, implementing mitigation measures, and continuously monitoring risks to aid organizations in effectively prioritizing and addressing potential threats.

According to Gurtu & Johny's (2021) systematic and phased approach to C-SCRM, it is found that organizations can prioritize their efforts and allocate resources effectively to address the most critical risks, reducing vulnerabilities and enhancing their ability to respond to and recover from potential cyber incidents. Additionally, the multilevel risk management perspective adopted by C-SCRM acknowledges the intricate nature of supply chains and the multitude of stakeholders involved, recognizing that risks can originate from individual components, suppliers, or even external actors within the supply chain ecosystem (Boyens et al, 2021). When considering risks at multiple levels, C-SCRM enables organizations to better comprehend the interdependencies and potential cascading effects of cyber risks throughout the supply chain. This holistic perspective offered by Boyens et al (2021) proposes the need to develop robust risk mitigation strategies that take into account the broader ecosystem, minimizing the likelihood of disruptions and optimizing the overall resilience of the supply chain.

In summary, the academic literature surrounding C-SCRM offers valuable insights into various aspects of the discipline. Studies exploring supply chain relationship factors and cyber risk issues provide a deeper understanding of the dynamics and vulnerabilities within supply chains (Hampton

et al., 2021). Research focused on the definition, theory, and research agenda of Supply Chain Risk Management (SCRM) contributes to the theoretical foundations of C-SCRM and informs its practical implementation (Fan & Stevenson, 2018). Additionally, the elucidation of specific C-SCRM programs and frameworks helps organizations manage the rising risk of supply chain compromise related to cybersecurity (Boyens et al., 2022). These scholarly contributions illustrate substantial academic knowledge of C-SCRM but fails to provide practitioners with practical guidelines and best practices to effectively manage cyber risks within their supply chains, hence representing a research gap in literature for this study to contribute to.

2.2 Cybersecurity threats in supply chains

In an era of proliferating digital commerce, supply chains have become increasingly susceptible to a broad range of cybersecurity threats, receiving increasing research attention in the 21st century. Empirical studies from Gordon & Ford (2006) and Urciuoli et al (2013) have attempted to critically explore the nature of cybersecurity risks under 2 distinctive categories. According to Gordon & Ford (2006), type I risks encompass instances like phishing and theft or manipulation of data, and Type II refers to cyberstalking, blackmailing, and corporate espionage. However, while these classifications offer valuable insight into intentional malevolent activities, it is criticized that this approach fails to account comprehensively for cyber risks originating from physical breakdowns and internal organizational activities (Urciuoli et al, 2013). Subsequently, Ghadge et al (2020) further expanded on Gordon & Ford's (2006) categorization approach, proposing five distinct categories of cybersecurity risks into physical threats, breakdown, indirect attacks, direct attacks and insider threats as shown in figure 3 below.

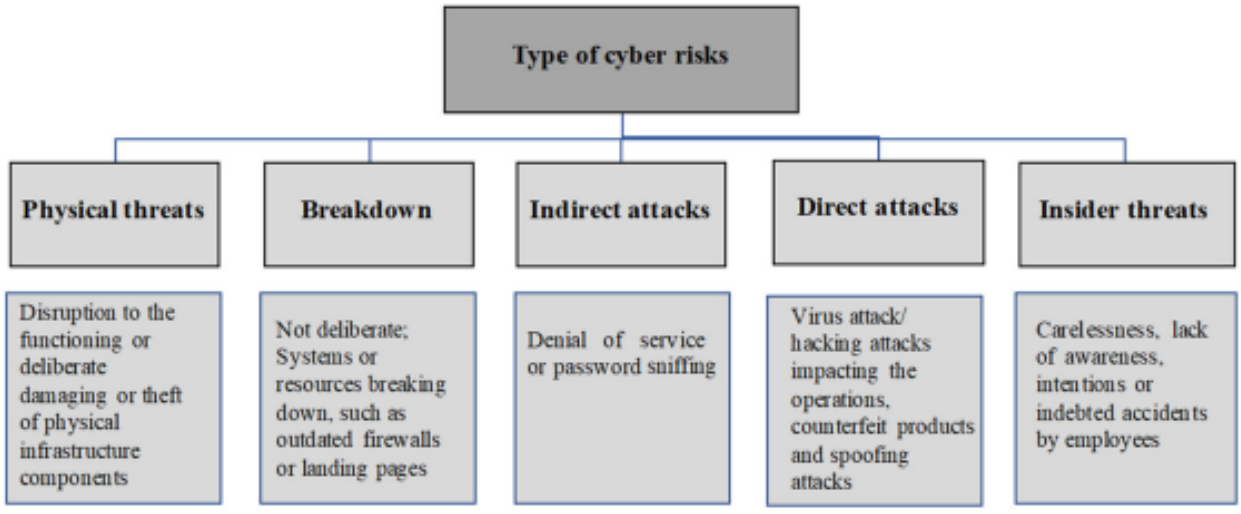

Figure 3: Types of cybersecurity risks (Ghadge et al, 2020, p230)

Ghadge et al's (2020) categorization of physical cybersecurity risks draws upon Boyes' (2015) recognition of tangible asset impacts in the digital supply chain, underscoring the physical attributes of cyber risks that includes potential damage or failure of physical hardware components such as servers, switches, routers, and other Information Communication Technology (ICT) devices. According to Ghadge et al (2020), risks associated with tangible supply chain assets are integral to potential cybersecurity risks, reinforcing the arguments of Faisal et al (2007) that highlighted the potential for substantial disruptions to the cyber supply chain resulting from both natural disasters and intentional acts of damage or theft. Other potential risks lie in the realm of system breakdowns, often due to obsolete firewalls or overdue security updates, potentially causing severe disruptions despite seemingly relatively mundane compared to deliberate attacks or natural disasters (Boyes, 2015; Tran et al., 2016).

In the context of deliberate assaults on cyber systems, the scholarly conversation distinguishes between direct and indirect attacks, both of which play a crucial role in the cybersecurity risk landscape (Ghadge et al, 2020). Direct attacks are exemplified in research by Faisal et al. (2007), Khursheed et al. (2016), and Boone (2017), encompassing instances like hacking or denial of service. These actions primarily aim for immediate intrusion, frequently driven by financial motives or the intent to compromise intellectual property (Khursheed et al, 2016). Furthermore, Boone (2017) argues that these direct assaults are characteristically confrontational, involving an attacker directly targeting and penetrating an organization's cyber defenses. Alternatively, Kunnathur (2015) argues that indirect attacks employ more covert, deceptive tactics, typically luring unsuspecting individuals to inadvertently grant system access to them. According to Williams (2014), these forms of indirect attacks commonly include deploying viruses, worms, Trojans and counterfeit products, or initiating spoofing attacks, as the insidious nature of these attacks, coupled with the rising sophistication of their implementation, underscores their significance in the broader spectrum of cybersecurity threats.

Another pivotal dimension of cyber threats often neglected in the discourse on direct and indirect attacks is categorized as insider threat according to Ghadge et al (2020). It is highlighted that the actions of employees, whether negligent or premeditated, can pose significant, unpredictable threats to a company's cybersecurity, whereby negligence could range from casual disregard for password confidentiality to absent-minded sharing of sensitive information. Additionally, more deliberate actions include purposeful misuse of confidential data or premeditated sabotage against the employer, highlighting the role of the human factors that influence the effectiveness of managing cybersecurity risks, illustrating the need for corresponding strategies to address both Behavioural and technical elements of cybersecurity risks as a whole (Ghadge et al, 2020). The current body of literature on cybersecurity risks in supply chains underscores the significance of understanding the varying origins and nature of these threats. The identified categories proposed by Ghadge et al (2020) provide a comprehensive framework for examining these cybersecurity risks, especially when applied toward the supply chain context as evidential in the studies of Katsaliaki et al (2021); Vu et al (2023) and Cheung et al (2021).

2.2.1 Causes of supply chain cybersecurity threats

According to Pandey et al (2020), understanding the causes of supply chain cybersecurity threats provides a foundation for implementing robust risk mitigation strategies. A large body of empirical have been dedicated on identifying the influential factors behind supply chain vulnerabilities, as the focus on cybersecurity vulnerabilities have received increasing research attention in recent years. In Unal et al's (2020) study, technical vulnerabilities are identified as the most common entry point for cyber threats, whereby the inherent complexities of supply chain networks, coupled with the increasing reliance on digital technologies, create numerous potential weak spots for exploitation. Additionally, Raut et al (2020) argues that these technical vulnerabilities could stem from outdated software, insecure network configurations, or poorly managed data storage practices, highlighting the lack of sufficient technical resources from the organization as well as inadequate technological skills and capabilities from key personnel. This is further elaborated by Kunnathur (2015), challenging that the human element within organizations also plays a crucial role in shaping the threat landscape, including negligence, careless handling of passwords or unintentional sharing of sensitive information, as well as more malicious actions like sabotage or misuse of privileged access.

According to Kunnathur (2015), the complexity of human related causes of supply chain cybersecurity risks can be highlighted by the exploitation of social engineering techniques including phishing, pretexting, and baiting, to manipulate unsuspecting employees into revealing sensitive information or granting unauthorized access. These complexities inevitably undermine the critical interplay between human factors and technical vulnerabilities, as failure to manage or monitor any of the human and technical factors would cause vulnerabilities to cybersecurity supply chain risks (Syed et al, 2022). Kumar & Mallipeddi's (2022) study identified the causes of supply chain cybersecurity threats in relation to organizational factors such as poorly defined or enforced security policies, lack of employee training, and inadequate resource allocation to cybersecurity initiatives, as these organizational related challenged are found to exacerbate both technical and human vulnerabilities. Despite the efforts of numerous empirical studies to explore the common causers of supply chain cybersecurity risks, Melnyk et al (2022) argues that each supply chain is likely to differ in nature and hence the exact causes of cybersecurity risks require a tailormade analysis that incorporates the complex interplay for technical, human, and organizational factors, requiring a case study specific approach to dissect and design corresponding mitigation strategies accordingly. Therefore, this research coheres to Melnyk et als' (2022) arguments to adopt a case study specific approach to identify supply chain cybersecurity threats as opposed to a generalized approach that would hinder the accuracy of findings due to the unique nature of different supply chains.

2.2.2 The impact of cybersecurity threats on supply chain operations and organizational reputation

The impacts of cybersecurity threats on supply chain operations are explored in Pandey et al's (2020) in-depth literature review and industry expert interviews, categorizing these impacts into three areas including supply risks, operational risks and customer risks as shown in figure 4. Under the supply risk dimension, Pandey et al (2020) extends on Zisdisin et al's (2004) recognition of inbound supply disruptions that compromise a firm's ability to meet customer demand, echoing the findings of Bhattacharyya et al (2010) who contend that trust issues associated with contractors are stemmed from substandard manufacturing standards or dubious authenticity of components. Bhattacharyya et al's (2010) analysis of the cyber-espionage group Dragonfly's activities found that cybersecurity risks would compromise the supply of legitimate Industrial Control Systems (ICS) software, signifying the threats posed by unreliable supply chain entities. According to Pandey et al (2020), the range of supply risks caused by cybersecurity threats are likely to emerge from inbound supply activities, pertaining to failure to secure digital supply chain touchpoints or from cyberattacks directed at suppliers

Risk category	Source of risk
Supply risk	Inaccessibility of suppliers
	Theft of vendor credentials
	Breach from the vendor network
	Modification of the source code through malware
	Supply of compromised software
Operational risk	Malfunctioning of the plant
	Sudden interruption in the operation of the plant
	Failure to detect coding errors
	Product specification fraud
	Data theft
Customer risk	Intellectual property theft
	Manipulation of data
	Unauthorized access to customer's data
	Fraudulent communication
	Information sabotage
	Unauthorized payment gateways

Figure 4: Types of supply chain risks caused by cybersecurity threats (Pandey et al, 2020, p109)

Another study by Parker et al (2023) found that cybersecurity risks would disrupt the operations of a supply chain, leading to halted production, delays in delivery, or in extreme cases complete shutdown of operations. Under the operational risk impacts dimension, Pandey et al (2020) argues that cybersecurity risks disrupt a firm's internal operations, thereby affecting the quality and timeliness of production, ultimately affecting the firm's profitability. This is reinforced in the study of Tupa et al (2017), highlighting the increasing susceptibility of operational systems to cyber

threats as organizations progressively digitalize their operations as reflect in the cyber-attack at a blast furnace at a German steel mill. This cyber-attack was evidence of poor cybersecurity and resultant breaches in access controls on the plant's ICSs, leading to significant physical damage and operational disruption, affirming the criticality of managing operational risks (Tupa et al, 2017). Under a customer risk impact dimension also referred to as demand risk impacts by Pandey et al (2020), it is found that cybersecurity threats would also cause disruptions to outbound flows, subsequently impairing customers' likelihood of placing orders with the firm. Additionally, this echoes the findings of Vlajic et als' (2012) study on examining the impacts of cybersecurity risks across food supply chains, finding apparent demand side disruption impacts including damages in market or brand reputation.

2.3 Definition of blockchain and its characteristics

The development of blockchain technology is widely regarded as a revolutionary technological advancement, facilitating a new economic system that ensures authenticity, transparency and shared perceptive in traditionally complex transactions (Kakavand et al, 2017). Introduced by Nakamoto in 2008, blockchain is often portrayed as an assembly of cryptographic, interconnected records highly resistant to alteration, presenting a unique paradigm for information storage. In Nakamoto's (2008) paper "Bitcoin: a peer-to-peer electronic cash system", the blockchain technology was first developed and positioned as a decentralized system behind the cryptocurrency Bitcoin, with data distributed across the network rather than stored in a single centralized database, thus imbuing the system with robustness and resiliency against alteration. According to Farahani et al (2021), blockchain is defined as a digital ledger of transactions that is used to record transactions across a network of computer systems, elucidating its foundational structure under the concept of blocks that store groups of transactions which are hashed and encoded. Additionally, Singh & Singh (2016) highlighted the essential trait of blockchain in the interconnectedness of these blocks, as each one carries a cryptographic hash, a unique identifier of the preceding block.to create an interlinked chain of blocks.

Since its introduction, the characteristics of blockchain has received extensive research attention as a large number of studies have attempted to understand its facilitated features, ensuring effective application to achieve potential benefits (Xu & Zou, 2021; Di Pierro, 2017). According to Jadhav & Deshmukh's (2022) extensive review of blockchain literature, seven defining characteristics and traits of blockchain is identified as illustrated in figure 5. According to Jadhav & Deshmukh (2022), immutability is one of the fundamental characteristics of blockchain, ensuring that data once entered into the system cannot be modified or tampered with. This is achieved through a cryptographic technique known as hashing, which preserves the integrity of block information, hence fortifying the security and reliability of the data stored on the blockchain, echoing the arguments of Hofmann et al (2017) where immutability of blockchain would enable the revolutionization of data transfer processes. Moreover, the decentralised nature of blockchain is a

cornerstone feature that differentiates it from traditional, centralized systems. In a blockchain network, control is not vested in a governing authority or single entity, the network is maintained by a collective of nodes with no centralised ownership (Glaser, 2017).

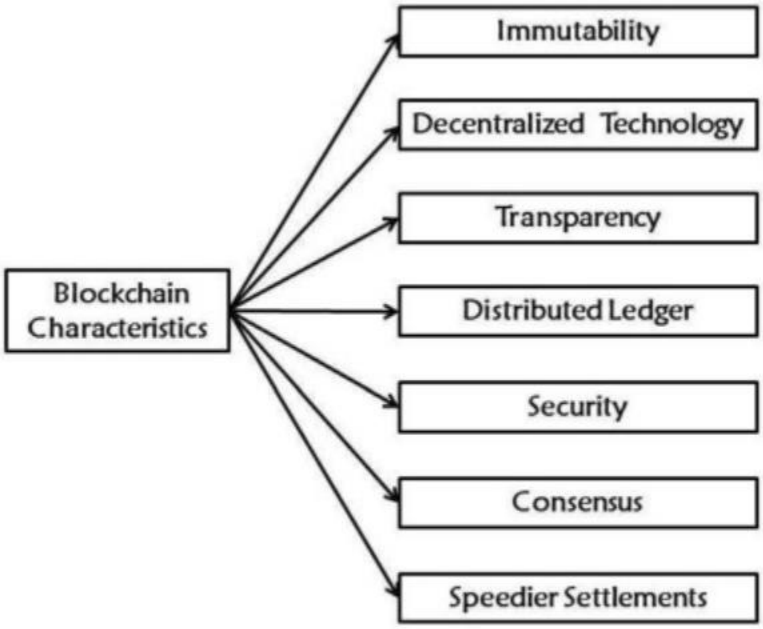

Figure 5: Characteristics of blockchain (Jadhav & Deshmukh, 2022)

According to Jadhav & Deshmukh (2022), a high degree of transparency is another salient trait of blockchain, whereby every participant in the network maintains an identical copy of the stored data. This stimulated transparency coupled with the requirement of majority approval for adding any transaction blocks to the ledger is found to bolster the trustworthiness of the system and mitigates fraud risk, enabling businesses to have a clear and unambiguous view of every part of the system, thereby enhancing accountability (Spano et al, 2022). Furthermore, the use of distributed ledgers in blockchain constitutes a shared, replicated and synchronized database across a decentralized network, as every participating node maintains an identical copy of the ledger, this further enhances the transparency and verifiability of the stored information (Natarajan et al, 2017). The algorithmic process of blockchain establishes a consensus mechanism that ensures the authenticity of records by maintaining a single, truthful copy of the data across all nodes, further preserving the honesty and reliability of records in the blockchain as it is found to eliminate data and communication siloes (Bamakan et al, 2020). The speedier settlement characteristic of blockchain is heavily explored within the context of accounting and financial transactions, as the application of blockchain helps to bypass traditional intermediaries, expediting the settlement

process in a faster and more efficient manner to prevent settlement failures and maintain accurate transaction records (Hasan & Habib, 2022).

2.3.1 Blockchain application in cyber supply chain risk management

The application of blockchain technologies has emerged as one of the fastest growing research topics in the academic field, spanning across a wide range of literature including computer science, information technology, business & management, economics and finance, public policy and governance (Gorkhali & Shrestha, 2020). According to Etemadi et al's (2021) dynamic review of blockchain literature in relation to supply chain disruption risk management, seven key clusters are identified from empirical studies as shown in figure 6. These clusters include the improvements of supply chain resilience, supply chain management via the implementation of smart contracts, enhanced traceability in database systems, strengthening cybersecurity, privacy, security and monitoring counterfeited products across supply chain activities (Etemadi et al, 2021). The fourth cluster identified by Etemadi et al (2021) directly addresses the application of blockchain in C-SCRM, echoing the findings of Vanajakumari et al (2020) whereby the immutability and transparency characteristics of blockchain would help to ensure a robust platform for secure, transparent, and immutable data sharing across the supply chain, enhancing the trustworthiness of the information flow. This is also reinforced by Sarode et al (2021) where blockchain immutability prevents unauthorized alteration of data, effectively protecting the supply chain against data tampering or manipulation risks that represent common cybersecurity threats.

Main Subjects	Keywords
Cluster 1: Digitalization for improved supply chain resilience	Additive manufacturing; blockchain technology; cryptocurrency; industry 4.0; RFID; supply chain resilience; supply chain risk management
Cluster 2: Employing blockchain technology with smart contracts in supply chain management	Blockchain; IoT; risk management; smart contracts; supply chain management
Cluster 3: Traceability database systems to ensure food safety and security	Distribute ledger technology; food safety; food security; food supply chain; traceability
Cluster 4: Blockchain's roles in strengthening cybersecurity	cloud computing; cryptography; cybersecurity; Internet of things
Cluster 5: Privacy and security challenges and blockchain solutions	Blockchain; distributed ledger; privacy; security
Cluster 6: Security of smart contracts in Ethereum platforms	Ethereum; smart contract
Cluster 7: Monitoring counterfeited products in the supply chain	Counterfeit; supply chain

Figure 6: Key clusters in blockchain and supply chain related literature (Etemadi et al, 2021, p15)

Additionally, Wylde et al (2022) found that the transparent nature of blockchain provides improved traceability across supply chains, as every transaction or action is recorded and can be traced back, which can contribute to early identification and mitigation of cyber risks. The facilitated transparency also aids in ensuring compliance and trust among stakeholders, whereby the

application of smart contracts in particular is found to further increase trust and compliance due to its elimination of the need for third party intermediaries (Turjo et al, 2021). According to Turjo et al (2021), smart contracts can ensure the automated and secure exchange of digital assets or services across the supply chain, increasing efficiency and reducing cyber risks. In Mukherjee et als' (2021) study on blockchain application in agricultural supply chains, the decentralised architecture of blockchain is found to greatly enhance resilience against cyber-attacks, as the distribution of data across multiple nodes would make the supply chain system highly resilient to system failures, in the event of nodes being compromised the overall system would continue to operate unaffectedly. Whyte et al's (2022) study critically explored the data integrity and assurance effects of blockchain application in cyber supply chain risk management, finding that organizations can verify the authenticity of vendors and their products/services with ease, mitigating risks of counterfeit or compromised components entering the supply chain.

2.4 Summary of literature

The nascent field of blockchain technology and its application in Cyber Supply Chain Risk Management (C-SCRM) has garnered notable scholarly attention in the past decade, underscoring the growing recognition of its transformative potential across myriad domains. Theoretical and conceptual groundwork laid by Nakamoto (2008) established blockchain as a collection of securely linked records protected by cryptographic measures, providing a firm basis for subsequent investigations into the practical applications of this disruptive technology. In relation to the theoretical background of C-SCRM, studies have explored different risk management models that incorporate the principles of blockchain technology, attempting to mitigate the emerging threats and vulnerabilities in the digital realm (Urciuoli, 2016). While supply chain risks were once understood predominantly through traditional risk models (Jüttner et al., 2003; Manuj & Mentzer, 2008), the advent of blockchain has necessitated the reconceptualization of risk identification and management processes (Urciuoli, 2016). However, more in-depth exploration of the intricacies of these emerging models remains a relatively uncharted area of investigation.

When examining cybersecurity threats in supply chains, studies have begun categorizing cyber risks into different types, such as Type I and Type II (Gordon and Ford, 2006; Urciuoli et al., 2013), and Ghadge et al's 2020 five types of cybersecurity risks including physical, breakdowns, indirect attacks, direct attacks and insider threats, receiving widespread academic recognition and acceptances. The impact of cybersecurity threats on supply chain operations and organizational reputations has been another area of research focus. Studies have demonstrated that cybersecurity threats not only disrupt operations but can also inflict substantial reputational damage (Boyes, 2015; Tran et al., 2016). Despite these advancements, there's a need for more nuanced and context-specific explorations into the effects of various cyber threats on different types of supply chains. In relation to the definition of blockchain and its characteristics, while initial studies have offered broad definitions (Nakamoto, 2008; Singh & Singh (2016), more recent literature has begun to

dissect the unique characteristics of blockchain technology, such as its immutability, decentralisation, transparency, distributed ledger, security, consensus and speedier settlements (Jadhav & Deshmukh, 2022). However, research that critically evaluates these characteristics, especially in the context of C-SCRM remains relatively scarce and represents a research gap for this study to contribute to.

Overall, the literature on the application of blockchain in C-SCRM is still in its nascent stage. While the potential of blockchain for enhancing transparency and security in supply chains has been noted (Tran et al., 2016), empirical studies investigating the strategic deployment of blockchain for managing specific cyber risks in supply chains are still lacking. There are significant research gaps, particularly in the exploration of blockchain's potential in the context of specific cyber risks in supply chains and its limitations, these gaps provide ample opportunities for further research as this study will attempt to address. In consideration of empirical academic knowledge over cyber supply chain risk management and the application of blockchain technologies, a theoretical framework of this study is designed as shown in figure 7.

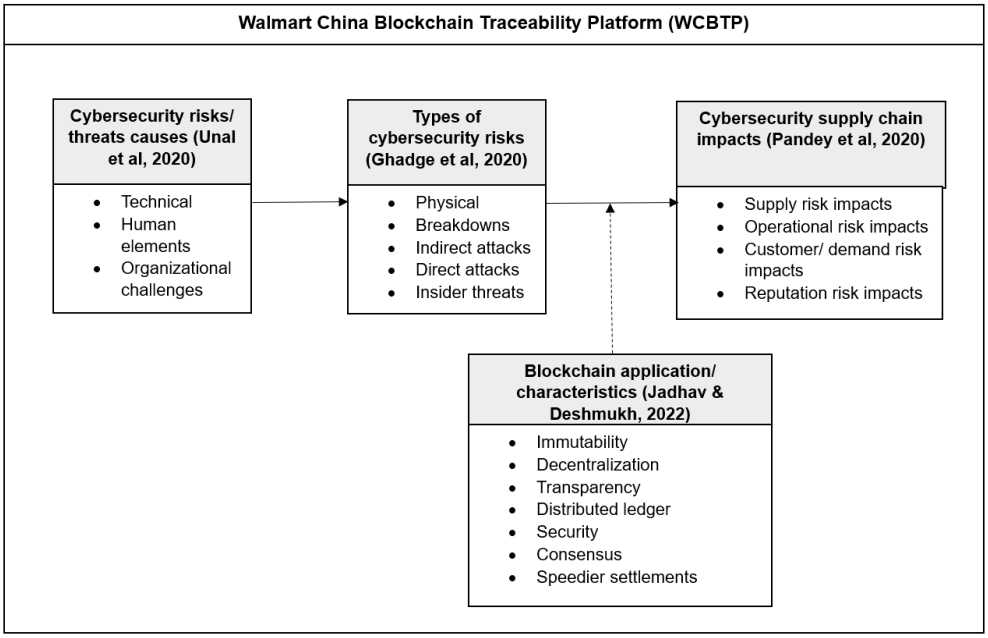

Figure 7: Theoretical framework

The proposed theoretical framework for this study draws upon empirical academic knowledge and theories spanning multiple facets of cybersecurity supply chain risk management and blockchain technology. The foundation of the framework lies in the understanding of cybersecurity risks and threats causes, classified into technical, human elements, and organizational challenges (Unal et al., 2020). These underlying causes manifest into various types of cybersecurity risks, including physical breakdowns, indirect attacks, direct attacks, and insider threats (Ghadge et al., 2020).

These diverse types of risks can potentially generate an array of impacts on the supply chain, which, according to Pandey et al. (2020), can be categorised into supply risk impacts, operational risk impacts, customer/demand risk impacts, and reputation risk impacts. These impacts, stemming from varying cyber threats, pose significant challenges to the functioning and integrity of supply chains, necessitating robust management and mitigation mechanisms.

The pivot in this framework is the application of blockchain technology, characterised by its unique attributes of immutability, decentralisation, transparency, security, and consensus, among others (Jadhav & Deshmukh, 2022). As a transformative technology, blockchain serves as a strategic tool that can be harnessed to address and manage the identified cyber risks and mitigate their impacts on supply chains. Given the specific context of this study - the Walmart China Blockchain Traceability Platform (WCBTP) - this framework not only aligns with the operational realities of a leading global retail giant but also incorporates the cutting-edge blockchain technology platform that Walmart China has implemented. Hence, the framework offers a comprehensive, multifaceted lens to explore and examine the intricate relationships between cyber threats, their impacts on supply chains, and the potential of blockchain technology in managing these risks in a real-world context.

3. Methodology

This chapter delves into the methodological design implemented in this study, justifying the chosen research methods, approaches and tools deployed throughout the research process. Kothari (2004) suggests that methodology employed in a study dictates the steps taken to accomplish the set objectives, necessitating the selection of the most suitable research methods and approaches that best align with the study's goals. Given the array of research methods and tools available for scholarly studies, it's vital to consider the distinct roles each method plays and take into account their potential limitations to effectively select those that resonate with the nature and requirements of the study (Garg, 2016). Therefore, this chapter will elucidate the reasoning behind each selected research method, approach and tools, illustrating the rationale for their choice while highlighting the benefits they offer in achieving the research objectives. Concurrently, this chapter discusses the discernible limitations and the measures undertaken to mitigate their impacts. The structure of this chapter is patterned after Saunders et al's (2007) research onion framework as illustrated in Figure 8 below. It sequentially discusses the methodological design from the research philosophy layer through to approach, strategy, choice, time horizon, data collection, and data analysis layers. The chapter concludes with a discussion of research ethics.

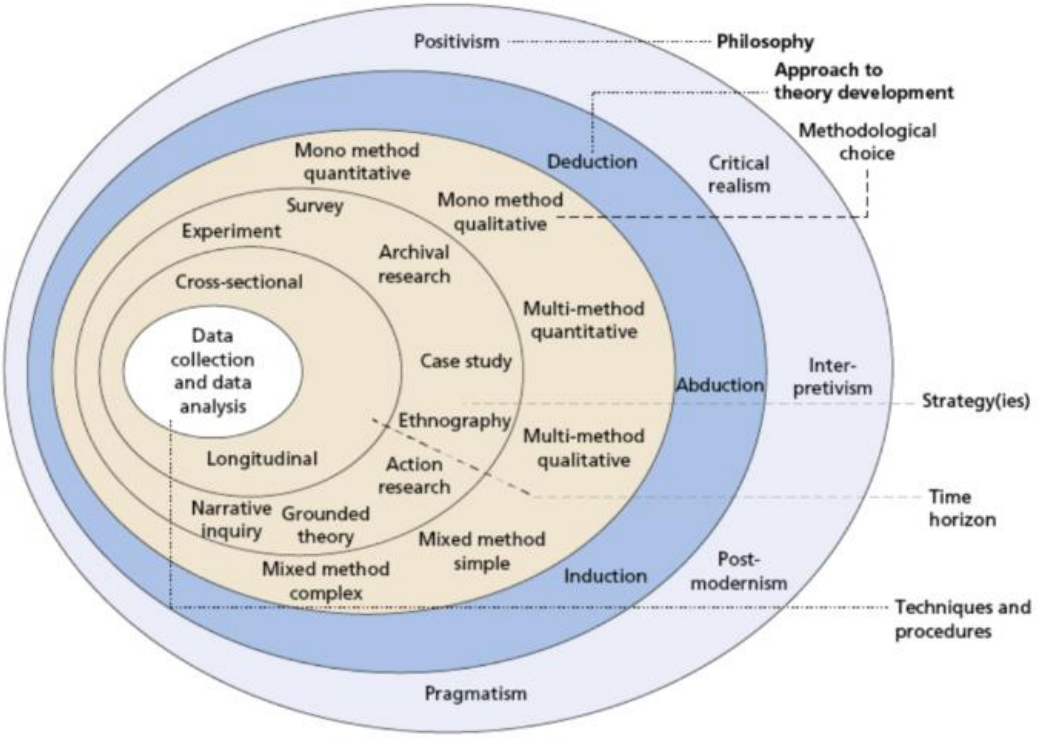

Figure 8: Research onion framework (Saunders et al, 2007)

3.1 Research philosophy

As illustrated in research onion framework articulated by Saunders et al (2007), the selection of a research philosophy represents the fundamental layer that establishes the overarching plan for the research study, informing how research procedures are implemented. According to Crossan (2003), a research philosophy embodies perspectives on the nature and operation of the world, concentrating predominantly on the progression of knowledge, the understanding of reality, and the essence of existence. Therefore, the selected research philosophy intrinsically shapes the way data is gathered, analysed, and utilised to contribute to research knowledge, by directing how the perceived reality influences the evolution of knowledge in the specified research area. Within the spectrum of research philosophies, Saunders et al (2015) spotlight three major paradigms under ontological, epistemological and axiological, each of which subscribes to distinct philosophical principles. Ontological philosophy probes into the nature of reality, questioning whether a single objective reality or numerous subjective realities exist (Bahari, 2010). Conversely, epistemological philosophy delves into how knowledge is developed, centralising the creation of an unbiased research methodology that aids the cultivation of objectively verified knowledge about the research subject (Al-Ababneh, 2020). Axiological philosophy, on the other hand, scrutinises the value of a research phenomenon, emphasising the significance of research ethics in formulating the research design (Killan, 2013).

The primary goal of this research study is to construct knowledge by assessing the potential and application of blockchain technology in managing cybersecurity risks in Walmart's supply chain. Accordingly, an epistemological research philosophy has been adopted, enabling an objective methodology to cultivate knowledge on the integration of blockchain technology in managing cybersecurity risks within supply chains. This approach acknowledges that multiple interpretations may exist concerning the application of blockchain technology in disparate supply chain environments. Additionally, the epistemological branch of pragmatism has been selected for this study. This provides the researcher the opportunity to concentrate on real-world situations, accepting the reality that is perceived to be true if it is deemed useful and can be objectively corroborated using the chosen research methods (Morgan, 2014). The pragmatic philosophy offers the researcher a degree of flexibility, allowing the selection of best practices in research methods and tools aligned with the requirements of the research (Kaushik & Walsh, 2019). This approach is particularly beneficial for this study, as it navigates potential limitations associated with data accessibility, allowing the use of accessible and relevant data to provide a comprehensive solution to the research problem.

3.2 Research approach

Saunders et al (2007) note two distinct research approaches under inductive and deductive reasoning, both of which determine the progression of research activities and the way knowledge is constructed and findings are derived. Inductive reasoning represents a bottom-up approach, beginning with the observation of a set of empirical data relevant to the research interest. The researcher actively seeks patterns within the data, thereby creating knowledge based on the identified data trends (Hodkinson, 2008). Furthermore, Hodkinson (2008) suggest that inductive research is particularly suitable for research areas with limited prior studies, as it allows for the generation of new theories and insights to fill the existing research gaps. However, Zalaghi & Khazaei (2016) caution that inductive studies may suffer from a lack of rigor, with biased observations and inaccurate data sources potentially undermining the validity of the findings.

Contrastingly, deductive reasoning embodies a top-down approach, suitable for research areas with an abundance of existing studies and established academic knowledge (Soiferman, 2010). The deductive process starts with the examination of empirical studies, identifying key research themes, trends, and gaps in the literature of interest. The researcher then aligns the research design with the identified gaps, drawing from existing academic knowledge and theories to shape the research scope. This alignment allows for the development of data collection methods that are consistent with established academic knowledge, enhancing the validity and reliability of the findings compared to an inductive approach. Despite the significant advantages of a deductive approach, the present study necessitates an inductive approach due to the novelty of the topic and the lack of directly comparable studies. The focus is on the application of blockchain technology in managing cybersecurity risks in Walmart's supply chain, a field with limited prior research. Thus, an

inductive approach, akin to the one adopted by Uddin & Venkatesh (2019) in their study of the Indian food supply chain is employed. Themes from existing cybersecurity and supply chain management literature are integrated into the design of relevant data collection parameters, aiming to contribute fresh insights to the identified research gap.

3.3 Research strategy

This study employs a case study research strategy coupled with qualitative survey methods, focusing on the specific case of Walmart's supply chain and its use of blockchain technology for managing cybersecurity risks within the WCBTP system. Feagin et al (2016) asserts that a case study research strategy is suitable for investigations where the researcher seeks to explore a contemporary phenomenon in its real-life context, especially when the boundaries between the phenomenon and context are not clearly evident. The case study approach allows for an in-depth investigation of the subject, contributing to a holistic understanding of the phenomenon being studied, which in this context is the application and impact of blockchain technology in supply chain risk management.

Concurrently, this study incorporates a qualitative survey research strategy to gather primary data from employees within Walmart's supply chain department. This strategy offers the flexibility to capture a wide range of information, including perceptions, attitudes, experiences, and knowledge related to the implementation and effectiveness of the blockchain-based system for managing cybersecurity risks. According to Braun et al (2021) qualitative surveys provide rich, textural data, enabling an understanding of the context and helping to explain the intricacies of the phenomenon under study.

The adoption of these research strategies mirrors the methodological approach employed by several previous studies in similar domains, such as the exploration of new technological applications in supply chain management. For instance, Ghadge et al. (2020) effectively employed a case study approach in their examination of blockchain technology adoption in supply chains, while Unal et al. (2020) leveraged qualitative surveys to gauge perceptions and experiences related to cybersecurity risks in supply chain contexts. These precedents demonstrate the feasibility and potential effectiveness of the chosen strategies for the current research on Walmart's blockchain implementation.

3.4 Research choice

In alignment with the chosen research strategy, this study opts for a qualitative research choice, fitting to both the case study and survey methodologies. Drawing upon Bryman (2016), qualitative research choice is advantageous in scenarios where the aim is to explore a complex phenomenon

in-depth, providing nuanced insights and capturing the richness and complexity of human experiences. It empowers researchers to delve into the intricacies of the subject matter, understand perceptions, attitudes, behaviours, and to capture the richness of the phenomenon at hand. Similarly, in this case, the application and impacts of blockchain technology in Walmart's supply chain risk management.

Qualitative research choice aligns perfectly with the survey strategy, as it enables the collection of deep, textured data from participants (Njie & Asimiran, 2014). The open-ended nature of qualitative data collection promotes an exploratory dialogue, allowing respondents to express and expand upon their responses freely. This can potentially unravel new insights and illuminate previously undisclosed facets of the research topic, through the respondents' unique experiential knowledge (Njie & Asimiran, 2014). However, the openness of qualitative data collection also places a considerable onus on the researcher's role in maintaining objectivity and ensuring accurate observations (Smith, 2015). The researcher should exercise reflective listening, accurately capture and paraphrase key points expressed by the respondents, and ensure that they stay focused on the research-specific topics during the discussion (Litchfield et al., 2017). This approach will help mitigate potential biases and enhance the credibility and validity of the data collected.

3.5 Research time horizon

In alignment with the objectives and structure of this research, a cross-sectional time horizon is employed. This strategy involves the engagement of all participants, in this case, 20 employees of Walmart China Blockchain Traceability Platform (WCBTP), in a single instance of data collection via online qualitative surveys. A cross-sectional approach is notably relevant as it captures the insights, experiences, and perspectives of the participants at a specific point in time, which is vital in studies that aim to understand current circumstances and phenomena (Levin, 2006)

3.6 Data collection

In this study, primary data were gathered using qualitative surveys directed at 20 participants working within the Walmart China Blockchain Traceability Platform (WCBTP). As a rule of thumb in qualitative research according to Mason (2010), a sample size between 10 to 30 is deemed sufficient for comprehensive data collection. Thus, the selected sample size was within the recommended range, ensuring broad insights while maintaining manageable data for an in-depth examination. Additionally, the participants were identified using a purposive sampling method, ensuring that each individual held relevant experience or knowledge regarding the WCBTP. The sampling strategy targeted those involved in various aspects of the blockchain system, from technical operations and maintenance to managerial roles and strategic decision-making. This

approach guaranteed the collection of diverse insights into the research topic (Campbell et al, 2020), enriching the understanding of the practical use of blockchain technology in mitigating supply chain cybersecurity risks.

Upon the identification of suitable participants, qualitative surveys were disseminated via the Qualtrics platform, an online tool that allowed for efficient distribution and collection of responses. By using Qualtrics, the study ensured an orderly collection process, ease of data management, and the ability to reach out to participants regardless of their geographical locations. The anonymity of participants was also secured throughout the data collection process, thereby adhering to ethical research considerations. Each survey was constructed with a series of open-ended questions, aimed at eliciting comprehensive responses that would contribute valuable data for the research. The questions probed into participants' experiences, perceptions, challenges, and successes regarding the implementation and functioning of the WCBTP. Through the personal networks of the researcher, this method of data collection served to tap into a well of practical, first-hand knowledge that would not have been accessible through secondary data sources alone.

The decision to collect qualitative data through surveys provided an avenue for participants to express their thoughts and experiences in their own words, thus enriching the depth of the data and enhancing the understanding of the research problem (Branthwaite & Patterson, 2011). These responses helped in generating meaningful insights that contributed significantly to fulfilling the research objectives.

3.7 Data analysis

In line with the qualitative nature of the data collected in this study, a thematic analysis approach was employed, which was instrumental in detecting, analysing, and reporting themes within the data. This method offered an organized and detailed way of interpreting rich, complex data. The data analysis process was carried out in five principal stages, which closely mirrored King & Brooks' (2018) model. Firstly, the researcher extensively read through the completed qualitative survey responses to thoroughly familiarize themselves with the raw data and grasp an overall understanding of the material. The aim at this stage was to discern implicit and explicit ideas that align with the research objectives. Secondly, the process of initial coding began, involving the identification of significant segments of text and assigning them descriptive labels. These codes served as a mechanism to distil, summarize and sort the data into meaningful clusters. Next, the researcher embarked on the search for potential themes by inspecting the codes and considering how different codes might combine to form an overarching theme. At this stage, themes were considered as tentative and subject to further refinement.

The fourth step involved a detailed review of these tentative themes against the coded extracts and the entire dataset. This step tested the validity of potential themes concerning the data. The relationships between the themes, sub-themes, and coded extracts were then examined and

depicted through a thematic map to visualize the interconnectivity of the identified themes. Finally, the researcher refined and finalized the themes, ensuring they accurately represented the dataset. Each theme was given a succinct and informative name that encapsulated its essence. The write-up of the analysis provided a concise, coherent, and logical account of the themes, underpinned by ample evidence from the data. A critical examination of the themes relative to existing academic knowledge in the field also took place, providing context and depth to the analysis. The thematic analysis method offered a systematic yet flexible approach to derive insights from the qualitative data collected, bringing valuable contributions to the research objectives.

3.8 Ethical considerations

In this research, rigorous ethical considerations were upheld throughout the data collection and analysis processes. Each participant gave informed consent before participating in the study, with explicit knowledge of their right to withdraw at any time as shown in appendix A. To maintain confidentiality, personal identifiers were removed, and anonymous codes were employed in all research materials. The research adhered strictly to the GDPR regulations for data protection: data collected were securely stored, accessible solely to the researcher, and were earmarked for deletion after the study's conclusion. Additionally, in the literature review, all used sources were appropriately referenced to ensure academic integrity. Finally, the research employed respectful, non-intrusive, and unbiased survey questions to prevent causing distress to the participants, further fortifying the study's ethical conduct.

4. Results and findings

This chapter outlines the significant findings from the qualitative surveys administered to 20 participants actively engaged in the Walmart China Blockchain Traceability Platform (WCBTP) project. A brief overview of the participants' roles, their duration of involvement with the WCBTP, and their prior experiences with blockchain technologies is presented in the table 1 below. The roles of the participants ranged from management positions, such as Project Manager (Participant A) and Product Manager (Participant T), to more technical roles like IT Specialist (Participant C), Blockchain Developer (Participant D), and Database Administrator (Participant P). This wide array of roles ensured a holistic understanding of the project, combining both the strategic and operational insights. The duration of experience within the WCBTP project varied between 1 and 4 years, with the Network Architect (Participant H) possessing the most experience. This mix of tenure allowed for varied perspectives, from fresh insights to those developed from prolonged project involvement.

Table 1: Participant information

Pseudonymised code	Role in WCBTP	Experience	Previous blockchain experience
Participant A	Project Manager	3 years	No
Participant B	Supply Chain Analyst	2 years	Yes
Participant C	IT specialist	2.5 years	Yes
Participant D	Blockchain Developer	3.5 years	Yes
Participant E	System Auditor	1 year	No
Participant F	Quality Assurance Manager	2 years	Yes
Participant G	Data Analyst	1.5 years	Yes
Participant H	Network Architect	4 years	Yes
Participant I	Operations Manager	2 years	No
Participant J	Senior Software Engineer	3 years	Yes
Participant K	Security Analyst	1.5 years	Yes
Participant L	Data Protection Officer	3 years	No
Participant M	System Administrator	2 years	Yes
Participant N	Technical Writer	1 year	No
Participant O	Quality control inspector	1.5 year	No
Participant P	Database Administrator	3 years	Yes
Participant Q	Business Analyst	2 years	No
Participant R	IT Consultant	2.5 years	Yes
Participant S	Systems Analyst	3 years	YEs
Participant T	Product Manager	2.5 years	No

In terms of previous blockchain experience, the group was evenly split with ten participants having had exposure to blockchain technologies prior to their involvement in the WCBTP project. This previous experience ranged from developing software for blockchain systems (Participant J -

Senior Software Engineer) to conducting security analysis for blockchain platforms (Participant K - Security Analyst). Conversely, the remaining ten participants, including the Project Manager (Participant A) and the Quality Control Inspector (Participant O), had their first exposure to blockchain technology through the WCBTP project. The blend of past experiences allowed for a diverse range of insights, providing an understanding of the adaptability and learning curve associated with implementing new technologies like blockchain.

4.1 Cybersecurity risks and threats in Walmart's supply chain

The thematic analysis of the survey responses identified several key cybersecurity risks and threats prevalent within Walmart's supply chain as summerised in table 2. These risks were frequently discussed across the surveys, reflecting their significance in the project's context. One of the most commonly cited risks was that of unauthorized access. As noted by several participants (A, D, G, K, O, P, R, T), this involves individuals obtaining unauthorized access to sensitive data or systems. As noted by Pandey et al (2020), unauthorized access can lead to significant damage to both infrastructure and reputation. Data breaches were another significant concern, with participants B, D, E, F, G, H, J, K, L, M, O, P, R, S, T, all highlighting the risks associated with unauthorized and potentially harmful data exposure. As Bhattacharyya et al (2010) highlight, data breaches can have a profound impact on operations and the trustworthiness of an organization.

Table 2: Cybersecurity risks and threats in Walmart's supply chain

Key Themes	**Sub-codes**	**Participants**	**Key meaning Phrases**
Unauthorized Access	Unauthorized System Access, Data Access	A, D, G, K, O, P, R, S	"Unauthorized access", "Unauthorized system access", "Risk of unauthorized system access"
Data Breaches	Potential Data Breaches	B, C, E, F, I, J, L, M, N, Q, T	"Data breaches", "Potential data breaches", "Risk of data breaches"
Data Tampering	Potential Data Tampering	A, B, H	"Potential data tampering", "Threats of data tampering"
Phishing	Phishing Attempts	F, G, J, O	"Phishing attempts", "Threats of phishing"
Malware Attacks	Malware Incidents, Ransomware Attacks	H, J, R, S	"Malware incidents", "Threat of ransomware attacks", "Threat of malware attacks"

System Vulnerabilities	Inherent System Vulnerabilities	D, E	"System vulnerabilities", "Risk of system vulnerabilities"
Compliance Risks	Potential Compliance Issues	L	"Potential compliance issues due to breaches"
DDoS Attacks	DDoS Attacks	K	"Distributed Denial of Service (DDos) attacks"

Data tampering, identified as a major risk by participants A and H, underscores the importance of maintaining data integrity within a blockchain system. In line with the work of Parker et al (2023) unauthorized alterations to data within a blockchain can compromise the validity and reliability of the entire system. The threats of phishing and malware were also present in the data, with participants F, H, K, and O drawing attention to these risks. Tupa et al (2017) identifies these as common cybersecurity threats, noting the damage they can cause to systems and data. A unique threat highlighted by participant D involved system vulnerabilities. The existence of inherent weaknesses in a system that can be exploited by external parties is a common theme in cybersecurity discourse (Tapscott and Tapscott, 2016). Finally, participant L brought attention to the potential risks associated with compliance. This underlines the importance of adhering to data protection and cybersecurity regulations (Vlajic et al, 2012).

4.2 Impacts of cybersecurity risks on Walmart's supply chain operations

The impacts of cybersecurity risks on Walmart's supply chain operations can be felt in several key areas as summerised in table 3. The participants in this study identified operational disruption, risk to data integrity, impact on delivery and efficiency, financial implications, and issues with regulatory compliance as the primary areas of concern. A substantial theme that emerged from the survey is the potential for operational disruption due to cybersecurity risks. Participants across multiple roles noted that unauthorized system access, data breaches, or malware attacks could significantly disrupt supply chain processes. This finding aligns with the work of Ghadge et al (2020) who emphasized that cybersecurity breaches could result in severe disruptions to the supply chain, leading to inefficiencies and, in some cases, a complete halt in operations. Another prominent concern that emerged from the data was the threat to data integrity. Many participants identified the compromise of data integrity as a substantial risk, as breaches could result in loss of data, thereby disrupting supply chain operations. This concern mirrors findings in the literature that point to data integrity as a critical component of supply chain management (Urciuoli et al, 2013).

Table 3: Impacts of cybersecurity risks on Walmart's supply chain operations

Key Themes	**Sub Codes**	**Participants**	**Key Meaning Phrases**
Operational Disruption	Supply Chain Processes	A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T	"Could disrupt our supply chain processes", "Significant disruptions in our supply chain operations", "Interruptions in supply chain processes", "Could result in severe service disruptions"
Data Integrity	Risk to Data	A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T	"Compromise the integrity of our data", "Could compromise the integrity of critical data", "Risk to data integrity"
Delivery and Efficiency	Timeliness and Quality	A, B, C, E, F, J, K, L, M, N, O, P, Q, R, S, T	"Impacting the timely delivery of products", "Causing delivery delays", "Could cause delayed deliveries", "Result in potential downtime, loss of data, and interruptions to the supply chain"
Financial Impacts	Cost implications	C, E, I, K, L, M, N, Q, R, S, T	"Potentially causing inefficiencies across the board", "Potentially inflate operational costs", "Could lead to considerable financial losses", "Potential financial penalties"
Regulatory Compliance	Legal Consequences	D, M, N, O, R	"Potential regulatory violations", "Possibility of incurring financial penalties", "Potential regulatory violations and the possibility of incurring financial penalties"

The participants also highlighted the potential impact of cybersecurity risks on delivery and efficiency. Risks such as unauthorized access or data breaches can lead to delays in product delivery, which in turn could harm Walmart's reputation for efficiency and reliability (Urciuoli et al, 2013). Furthermore, the threat of cybersecurity breaches could potentially inflate operational costs, making processes less efficient and eroding profit margins. Financial implications are another key theme that emerged from the participants' responses. These implications include not only direct financial losses resulting from cyber-attacks but also the potential for financial penalties due to regulatory violations. This is consistent with previous research which identified the potential for significant financial impacts arising from cybersecurity risks (Tran et al., 2016). Finally, issues with regulatory compliance were raised by several participants, who expressed concern that

cybersecurity breaches could result in regulatory violations, leading to financial penalties and harm to the company's reputation. This finding reinforces the argument by Boyes (2015) that non-compliance with data protection regulations can lead to severe legal and financial consequences for companies.

4.3 Impacts of cybersecurity risks on Walmart's corporate reputation

The issue of cybersecurity risks and the impact they can have on a company's reputation is a recurrent theme among the participants as summerised in table 4. As per the thematic analysis, impacts on Walmart China's corporate reputation due to cybersecurity risks can be grouped under four major themes: Reputational damage, media attention, stakeholder trust, and operational delays. Reputational damage is evidently a major concern among the participants. The potential for damage to Walmart's corporate reputation in the event of failed cybersecurity measures is a recurring issue, with several participants highlighting the importance of maintaining stringent cybersecurity measures to prevent any potential damage The consequences of reputational damage can be severe, impacting a company's market value, trust among stakeholders, and even its survival in the market (Tupa et al, 2017).

Table 4: Impacts of cybersecurity risks on Walmart's corporate reputation

Key Themes	**Sub Codes**	**Participants**	**Key Meaning Phrases**
Impact on Reputation	Reputational Damage	Participants M, R, T, L	"Potential damage to corporate reputation if cybersecurity measures fail"; "Instances of breaches have led to reputational damage affecting corporate image."
Media Attention	Negative Publicity	Participants K, P	"Cybersecurity risks were highlighted in media, causing brief negative impact"; "Incidents of data breaches and unauthorized access were reported in media negatively impacting corporate reputation."
Stakeholder Trust	Erosion of Trust	Participants N, Q	"Cybersecurity incidents erode stakeholder trust and can damage reputation"; "Data breaches, even if promptly addressed, affected perception of platform, eroding trust."
Operational Delays	Supply Chain Disruptions	Participant O	"Minor cybersecurity breach led to temporary halt in operations and brief negative impact on reputation."

Media attention is another theme highlighted by the participants. Cybersecurity risks that gained media attention reportedly had a brief negative impact on the company's reputation. In an era where news is disseminated rapidly via numerous channels, it is vital that companies manage cybersecurity threats efficiently and effectively to prevent any negative publicity (Vlajic et al, 2012). The erosion of stakeholder trust due to cybersecurity risks is another significant theme that emerged. Participants acknowledged that cybersecurity incidents could cause a loss of stakeholder trust and damage the company's reputation. Trust is the bedrock of any successful business (Spano et al, 2022), and maintaining it in the face of cybersecurity risks is paramount. Operational delays due to cybersecurity risks were also identified as a reputational risk. While these were reported to be temporary, the fact that such incidents can negatively impact corporate reputation underscores the importance of robust and effective cybersecurity measures.

4.4 Effectiveness of the WCBTP platform on managing cybersecurity risks

The analysis of responses from the participants suggested that the implementation of blockchain technology within the WCBTP platform has been instrumental in managing and mitigating cybersecurity risks as summerised in table 5 below. The technology's inherent features such as decentralization, encryption, and immutability have significantly enhanced Walmart China's ability to safeguard its supply chain processes and sensitive data from cyber threats. A key benefit of the blockchain identified across the participants is its ability to enhance security through data encryption (Gorkhali & Shrestha, 2020). This was reflected in the responses of participants A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, and T, who mentioned that the cryptographic features of blockchain have significantly bolstered data protection and overall system security within the WCBTP. As such, the blockchain technology has helped reinforce the defence against cybersecurity risks, aligning with Gorkhali & Shrestha (2020), who argued that the encryption attribute of blockchain could provide robust data protection.

Table 5: Effectiveness of the WCBTP platform on managing cybersecurity risks

Key Themes	**Sub Codes**	**Participants**	**Key Meaning Phrases**
Enhanced Security	Data Encryption	A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T	"Significantly bolstered our system's security", "Cryptographic features have enhanced our data protection", "Enhanced data protection", "Improved our data handling processes", "Bolstered our defences against cybersecurity risks", "High degree of data security"

Decentralization	Distributed Nature	B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T	"Minimized single points of failure", "Decentralized nature of blockchain has minimized data tampering risks", "Decentralization and encryption significantly enhance data security", "Decentralization and cryptographic features, offered improved data security", "Decentralization and immutability offer enhanced security"
Data Integrity	Immutability	C, G, J, M, O, S	"Blockchain has significantly bolstered our defences", "Immutability and encryption offer enhanced security", "Immutable nature of blockchain ensures a high degree of data security"
Transparency	Visibility of Transactions	C, F, H, I, J, K, M, P, Q, R	"More secure and transparent platform for data handling", "Transparent system, blockchain technology has significantly bolstered our defences", "Decentralized, immutable, and transparent system

The second key theme highlighted by the participants was the decentralized nature of blockchain technology (Etemadi et al, 2021). Participants B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, and T emphasized that this feature minimizes single points of failure and data tampering risks. This finding is consistent with the views of Sarode et al (2021), who emphasized the role of decentralization in enhancing data security by eliminating centralized control and reducing vulnerability to hacking attempts. Immutability, another integral feature of blockchain, emerged as a significant theme contributing to data integrity, a viewpoint echoed by participants C, G, J, M, O, and S. This aligns with the concept of immutability as described by Singh & Singh (2016), where once data is recorded on a blockchain, it cannot be altered, thus providing a reliable and accurate history of transactions. Lastly, the transparency offered by blockchain was identified as a critical benefit by participants C, F, H, I, J, K, M, P, Q, and R. This finding correlates with the views of Jadhav & Deshmukh (2022), who argued that blockchain technology ensures a high degree of transparency by making all transactions visible and verifiable to all parties involved.

4.5 Implementation and execution challenges of WCBTP

Implementing a blockchain system in a complex supply chain environment such as Walmart's is a challenging endeavour as summerised in table 6 below. Participants A, C, D, G, K, O, Q, S

collectively highlighted the "Technical complexity" of understanding the intricacies of blockchain technology. This aligns with the insights of Jadhav & Deshmukh (2022), who recognized that grasping the complexity of blockchain technology could be a significant hurdle in its application. The "Integration Challenges" identified by the majority of the participants (B, E, F, H, I, J, L, M, N, P, R, T) indicates the difficulties in blending the new technology with existing systems. This reflects Vanajakumari et al's (2020) assertion that ensuring compatibility between blockchain technology and existing systems could pose significant challenges, as it demands a clear understanding of the technology and its potential impacts on current processes.

Table 6: Implementation and execution challenges of WCBTP

Key Themes	**Sub Codes**	**Participants**	**Key Meaning Phrases**
Technical complexity	Blockchain understanding	A, C, D, G, K, O, Q, S	"Understanding blockchain's complexity was challenging", "Complex nature of blockchain technology", "Grasping intricacies of blockchain", "Difficulty in deciphering blockchain functionality"
Integration challenges	Compatibility with existing systems	B, E, F, H, I, J, L, M, N, P, R, T	"Integrating blockchain with existing systems was difficult", "Ensuring compatibility of blockchain with current systems", "Adapting existing supply chain processes", "Challenges in seamless integration"
Regulatory compliance	Data protection and regulations	B	"Challenges meeting data protection regulations", "Ensuring compliance with regulatory requirements", "Balancing blockchain features with data regulations"
Training and education	Staff training and education	D, G, I, M, O, S	"Staff training and education were required", "Need for continuous learning", "Training in new technologies was crucial", "Significant knowledge enhancement needed"
Resource constraints	Time and resource investment	C, D, E, G, H, K, M, N, O, P, Q, R, S, T	"Blockchain implementation required substantial resources", "Time investment for blockchain integration", "Need for significant resource allocation", "Challenges in resource and time management"

Regulatory compliance was another challenge, specifically highlighted by participant B. The participant's experiences emphasize the difficulties in ensuring data protection and regulatory compliance, mirroring the views of Bamakan et al (2020) on the challenges of maintaining compliance in an evolving technological landscape. The challenge of "Training and Education" was shared by several participants (D, G, I, M, O, S). They underlined the need for continuous learning and staff training to effectively implement the new technology. This requirement aligns with the perspective of Peters and Panayi (2016), who argued that training and education form an integral part of blockchain technology implementation, given its unique and complex nature. Finally, the constraint of resources, including time and financial investments, was mentioned by a broad set of participants (C, D, E, G, H, K, M, N, O, P, Q, R, S, T). This resonates with the viewpoint of Etemadi et al (2021) who suggested that significant resource and time allocation is a common challenge in blockchain implementations.

4.6 Factors driving successful implementation of the WCBTP system

The successful implementation of the WCBTP system is reported by participants to be due to a confluence of factors, prominently mentioned were technical expertise, regular security assessments, strong stakeholder commitment, adequate training and education, effective communication, iterative development approach, regulatory compliance, and scalability and adaptability of the blockchain solution as summerised in table 7 below. Technical expertise emerged as a key factor across responses, reflecting the intricate knowledge and skills required to implement and manage a blockchain-based system. This aligns with previous literature, such as the work of Mukherjee et al (2021), highlighting the significance of technical expertise in the successful implementation of blockchain technology.

Table 7: Factors driving successful implementation of the WCBTP system

Key Themes	**Sub Codes**	**Participants**	**Key Meaning Phrases**
Technical Expertise	Staff Skills	A, C, D, H, K, M, O, Q	"Technical skills developed within the team", "The technical expertise of our team was critical"
Security Assessments	Risk Management	A, I, M	"Continuous security assessments we conducted", "Stringent testing procedures were key"
Stakeholder Commitment	Management Support	A, D, H, J, K, M, O, Q	"Strong commitment from all our stakeholders", "Strong organizational support was pivotal"

Training and Education	Knowledge Transfer	B, E, F, H, J, L, N, P	"Continuous training was necessary", "Comprehensive staff training was a key factor"
Effective Communication	Collaboration	D, E, F, J, N, P, R, T	"Clear and effective communication was vital", "Involvement of all stakeholders in the process"
Iterative Approach	Continuous Improvement	H, I, J, K, M, O, P, R	"Iterative approach towards development and implementation", "A readiness to iteratively improve the system"
Regulatory Compliance	Legal Adherence	B	"Clear understanding of regulatory requirements"
Scalability and Adaptability	System Flexibility	B, N, R, T	"Solution's scalability and adaptability was crucial", "Ability to adapt our business processes"

Regular security assessments were mentioned by a number of participants, indicating the critical role of these assessments in identifying and mitigating potential security vulnerabilities. This resonates with the assertion by Wylde et al (2022) that rigorous security assessment is vital in ensuring the robustness of a blockchain system. Stakeholder commitment was another recurrent theme, reflecting the need for organizational support and a shared vision for the successful integration of blockchain technology. This aligns with the work of Turjo et al (2021), who asserted that management support and stakeholder commitment are crucial for successful technological transitions. The theme of training and education was highlighted, underscoring the importance of equipping the team with the requisite knowledge and skills to navigate the complexities of blockchain technology. This mirrors the assertion of Catalini and Gans (2020) on the importance of education and training in harnessing the benefits of blockchain technology.

Effective communication was identified as key to coordinating efforts, facilitating understanding, and fostering a collaborative environment, which is in sync with the views of Etemadi et al (2021) who noted that clear communication is integral to the successful implementation of blockchain technology. Iterative development approach was highlighted by participants, alluding to the process of continuous improvement and fine-tuning of the system. This finding is in agreement with the work of Mougayar (2016), who argued for an iterative approach to blockchain technology implementation. Regulatory compliance emerged as a relevant factor in the case of data protection, reflecting the legal obligations that must be adhered to when implementing technologies that handle sensitive data, which aligns with the views of Atzori (2015), who stated that compliance with regulatory requirements is crucial in blockchain implementations. Finally, scalability and

adaptability of the blockchain solution were emphasized by participants, suggesting the importance of a flexible and scalable blockchain solution that can be adapted to meet the changing needs of Walmart's supply chain, supporting the argument of Tapscott and Tapscott (2017) regarding the need for adaptable blockchain solutions.

4.7 Recommendations on blockchain application in foot retail supply chains

Drawing on the survey results, several recommendations can be deduced that could guide future blockchain applications in food retail supply chains as shown in table 8. The key themes extracted from the thematic analysis included continuous learning and adaptation, robust security measures, rigorous testing and evaluation, effective communication, regulatory compliance, and stakeholder involvement. Continuous Learning and Adaptation were underscored as pivotal for successful blockchain application, with a focus on embracing new technologies and fostering an environment of continuous learning (Sarode et al, 2021). These attributes enable an organization to stay abreast with rapid technological changes, ensuring they leverage the benefits that these advancements bring. In line with the findings of Mohamed & Jaroodi (2019), our survey reiterated the critical role of robust security measures in the successful implementation of blockchain. Ensuring robust cybersecurity measures not only safeguards the system against threats but also builds trust among stakeholders, crucial for the success of any technological implementation.

Table 8: Recommendations on blockchain application in foot retail supply chains

Key Themes	**Sub Codes**	**Participants**	**Key Meaning Phrases**
Continuous Learning & Adaptation	Adaptation to new technologies	A, C, D, I, J, L, M, N, P, Q, R, S, T	"Embrace new technologies", "Importance of continuous learning", "Necessity of agility"
Robust Security Measures	Need for enhanced cybersecurity	B, E, F, H, K, O	"Need for robust cybersecurity measures", "Importance of security in digital business"
Rigorous Testing & Evaluation	Importance of testing and feedback	D, G, K, L, M, N, P, Q, S, T	"Importance of comprehensive testing", "Significance of continuous feedback"
Effective Communication	Communication and documentation	C, F, G, J, O	"Role of effective communication tools", "Significance of clear and effective communication"

Regulatory Compliance	Compliance with data protection regulations	B, F, H	"Importance of regulatory compliance", "Need to understand regulatory requirements"
Stakeholder Involvement	Involvement of all stakeholders	D, I, M, Q	"Involvement of all stakeholders", "Significance of stakeholder commitment"

The necessity for rigorous testing and evaluation was another key theme that emerged. Consistent with the work of Raza & Singh (2022), our survey findings highlight the importance of thorough system testing and the significance of continuous feedback. Such measures can identify potential issues early on, minimizing the likelihood of larger, disruptive problems down the line. Effective Communication surfaced as another key theme in our survey. Clear and effective communication, as well as comprehensive documentation, play a crucial role in ensuring a smooth transition to new technologies (Raza & Singh, 2022). The importance of making complex technologies understandable to all stakeholders cannot be overstated. Regulatory Compliance was a significant theme that echoed through the survey responses. As mentioned in the studies of Yurchenko et al (2020), understanding and complying with regulatory requirements is crucial when integrating blockchain into existing systems. Finally, Stakeholder Involvement was identified as a crucial factor for successful implementation (Rane et al, 2021). Involving all stakeholders and securing their commitment can ensure that the technology is integrated smoothly and effectively into existing systems.

5. Discussion

The primary aim of this discussion chapter is to critically interpret and synthesize the key findings obtained from the research, drawing connections to the academic literature and providing thoughtful analysis within the context of the established research objectives. This chapter serves as a platform to integrate the findings from the empirical investigation of the Walmart case study with the theoretical perspectives elucidated in the literature review. The discussion will be structured according to the four research objectives. Firstly, it will explore the categorisation of potential cybersecurity threats in food retail supply chains, informed by the insights from the Walmart case study and the broader academic literature. Secondly, it will critically evaluate the impacts of these cybersecurity risks on supply chain operations and corporate reputation. The third section will discuss the efficiency of blockchain technology applications in mitigating cybersecurity risks within Walmart's supply chain. The final section will propose recommendations and strategies for organisations aiming to integrate or apply blockchain technologies to manage cybersecurity threats in their supply chains. This structured approach

allows for a comprehensive and nuanced understanding of the research topic, effectively linking practical observations with theoretical underpinnings.

5.1 Cybersecurity threats in food retail supply chains

The categorisation of potential cybersecurity threats in food retail supply chains is a crucial first step in comprehending the cybersecurity landscape within this industry. The empirical investigation of the Walmart case study has revealed several key cybersecurity threats such as unauthorized access, data breaches, data tampering, phishing and malware, system vulnerabilities and compliance issues. The prevalence of these risks, particularly unauthorized access and data breaches, echoes the findings of Pandey et al (2020) and Bhattacharyya et al (2010) who highlighted these threats in their work. However, our empirical findings provide a fresh perspective by demonstrating these risks in the context of a practical, real-world setting, specifically, a multinational food retail supply chain. The repetition of these risks across multiple participants underscores their significance and lends support to the academic literature on the subject. One interesting aspect emerging from the research is the identification of compliance risks. While most literature tends to focus on direct threats such as unauthorized access or data breaches, this study illuminates the risk of non-compliance with data protection and cybersecurity regulations (Vlajic et al, 2012). This new insight from the field complements the academic discourse by expanding the range of identified threats.

Moreover, the finding on system vulnerabilities supports the argument made by Tapscott and Tapscott (2017) on inherent weaknesses in systems, providing a clear, practical example of this issue. This contribution to the field underlines the importance of a comprehensive approach to cybersecurity, incorporating both protective measures against external threats and the strengthening of internal systems. Overall, the findings of this study not only confirm the threats identified in the literature but also add valuable insights by offering a detailed understanding of these threats within the context of a global retail supply chain. The study thus contributes to the academic field by augmenting the existing knowledge of cybersecurity threats, emphasizing the need for tailored, industry-specific threat assessments. This understanding is fundamental for developing effective cybersecurity strategies in the food retail industry and the broader supply chain domain.

5.2 Impacts of cybersecurity risks on supply chain operations and corporate reputation

The study's findings show that cybersecurity risks can significantly affect various facets of supply chain operations including operational disruption, risk to data integrity, impact on delivery and efficiency, financial implications, and regulatory compliance issues. The potential for operational disruption due to cybersecurity risks, as highlighted by our participants, confirms the work of Ghadge et al (2020), further providing practical, tangible examples of such disruption in the

context of a global retail supply chain. However, the study goes a step further, illustrating how these disruptions can have ripple effects, leading to inefficiencies or even a complete halt in operations, thus expanding upon existing academic knowledge. The threat to data integrity is another major concern echoed by many participants, substantiating the emphasis on data integrity in supply chain management highlighted by Urciuoli et al (2013). However, the research provides a more nuanced understanding of this issue by shedding light on how breaches can result in loss of data, disrupting supply chain operations. The potential impact of cybersecurity risks on delivery and efficiency identified in this study aligns with academic literature (Urciuoli et al, 2013), providing empirical support for theoretical assertions.

Furthermore, the findings also suggest that cybersecurity breaches could potentially inflate operational costs, making processes less efficient and eroding profit margins, a perspective not widely discussed in the academic discourse, thus contributing a new dimension to existing knowledge. Additionally, the research findings corroborate the significant financial implications and regulatory compliance issues identified in prior research (Tran et al., 2016; Boyes, 2015). However, our study provides a real-world context, demonstrating how non-compliance can lead to severe legal and financial consequences, thereby enriching the academic field's understanding of these issues. In terms of corporate reputation, our findings highlight that cybersecurity risks can lead to reputational damage, increased media attention, erosion of stakeholder trust, and operational delays, which aligns with Tupa et al (2017), Vlajic et al (2012), and Spano et al (2022). However, the inclusion of operational delays due to cybersecurity risks as a reputational risk provides a fresh perspective, adding depth to the existing body of knowledge. the research findings confirm and enrich the academic understanding of the impacts of cybersecurity risks on supply chain operations and corporate reputation, providing a more nuanced, context-specific understanding of these issues. The insights gained from this study underscore the critical need for effective cybersecurity strategies to safeguard supply chain operations and protect corporate reputation.

5.3 Efficiency of blockchain technology applications in mitigating cybersecurity risks

The third research objective sought to investigate the efficiency of blockchain technology applications in managing cybersecurity risks within Walmart's supply chain. The findings from this study underscore the effectiveness of blockchain technology, particularly the Walmart China Blockchain Traceability Platform (WCBTP), in enhancing cybersecurity. In particular, the inherent attributes of blockchain technology such as decentralization, encryption, immutability, and transparency were reported to significantly enhance supply chain security, supporting existing academic perspectives (Gorkhali & Shrestha, 2020; Etemadi et al, 2021; Sarode et al, 2021; Singh & Singh, 2016; Jadhav & Deshmukh, 2022). However, the findings from the survey responses provide empirical insights into how these features work in a real-world context, thereby providing

a valuable contribution to the academic understanding of the applicability of blockchain in managing cybersecurity risks.

The study's findings indicate that the WCBTP's blockchain technology has been particularly effective in bolstering data protection and overall system security. This underpins the academic work of Gorkhali & Shrestha (2020), who propounded that the encryption attribute of blockchain could provide robust data protection. The decentralized nature of blockchain technology was also identified as an effective measure against cybersecurity risks, aligning with the views of Etemadi et al (2021) and Sarode et al (2021). Moreover, the research extends these insights by demonstrating how decentralization can practically reduce the vulnerability to hacking attempts in a complex supply chain environment like Walmart's. The study further emphasizes the importance of immutability and transparency offered by blockchain, underpinning the views of Singh & Singh (2016) and Jadhav & Deshmukh (2022). However, our findings extend these insights by showcasing how these features can provide a reliable and accurate history of transactions, enhancing traceability, and accountability in a supply chain context, offering valuable insights for businesses seeking to adopt blockchain technology to enhance their cybersecurity measures.

5.4 Recommendations for blockchain application to manage cybersecurity threats

The final research objective of this study was to propose recommendations for organizations aiming to integrate or apply blockchain technologies to manage cybersecurity threats within their supply chains. This was achieved by drawing upon potential implementation challenges and corresponding mitigation strategies. The recommendations put forward in this study are substantiated by the empirical findings, which are uniquely positioned to provide practical insights for organizations in the field. The first recommendation emphasized the necessity of continuous learning and adaptation for successful blockchain application. This is a unique insight drawn from the responses of the participants, further strengthening the arguments of Sarode et al (2021), who identified continuous learning as a critical factor for successful technological implementation.

The study also recommends maintaining robust security measures, which aligns with previous academic perspectives (Mohamed & Jaroodi, 2019). Yet, the study provides a unique contribution by offering an empirical basis for this argument, emphasizing its significance in a practical context. Similarly, the importance of rigorous testing and evaluation as a recommendation, as identified by the survey findings, strengthens the views of Wylde et al (2022), yet provides a unique perspective by highlighting its practical significance in the context of implementing blockchain in supply chains. Effective communication emerged as a pivotal factor for successful implementation from the empirical data, which aligns with the views of Raza & Singh (2022). However, our research extends this by emphasizing how effective communication can facilitate a smooth transition to new technologies in real-world supply chain contexts.

The importance of regulatory compliance, highlighted in this study, supports the views of Atzori (2015). Nonetheless, our research extends these insights by showcasing how organizations can practically ensure compliance when integrating blockchain into existing systems. Finally, our research emphasizes stakeholder involvement as a crucial factor, echoing the arguments of Rane et al (2021). Yet, the findings from the study offer a fresh perspective on how stakeholder involvement can practically ensure a smoother integration of technology into existing systems. In summary, the recommendations proposed in this research provide a unique blend of academic perspectives and empirical insights, significantly contributing to the body of knowledge on blockchain applications in managing cybersecurity risks within supply chains. This offers valuable directions for businesses seeking to implement blockchain technology.

6. Conclusion

This research study was set out to investigate and categorize potential cybersecurity threats in food retail supply chains, evaluate their impacts, examine the efficiency of blockchain technology in mitigating these risks, and propose practical recommendations for organizations wishing to leverage blockchain technology for cybersecurity. Drawing upon a broad review of academic literature and an in-depth investigation of the Walmart China Blockchain Traceability Platform (WCBTP) case study, this research has provided substantial insights into these objectives. The investigation of cybersecurity threats within Walmart's supply chain revealed several significant risks, including unauthorized access, data breaches, data tampering, phishing, malware, system vulnerabilities, and compliance-related issues. The impacts of these threats were found to be profound, affecting areas such as operational disruption, data integrity, delivery and efficiency, financial implications, and regulatory compliance. These findings contribute to the academic discourse on cybersecurity risks within the context of food retail supply chains, providing empirical evidence that complements existing theoretical perspectives.

The study also critically evaluated the effectiveness of the WCBTP in managing cybersecurity risks. Through the inherent features of blockchain technology—decentralization, encryption, immutability, and transparency—WCBTP has significantly enhanced Walmart China's ability to safeguard its supply chain processes and sensitive data from cyber threats. This supports and extends previous academic perspectives on the value of blockchain technology in enhancing supply chain security, offering evidence of its practical effectiveness. Furthermore, the research surfaced implementation challenges such as technical complexity, integration challenges, regulatory compliance, training and education, and resource constraints. The empirical evidence from this study adds a practical dimension to the academic understanding of these challenges, enriching the discourse on the real-world complexities of blockchain implementation in supply chains.

The study proposed several recommendations for organizations aiming to integrate blockchain technology, including continuous learning and adaptation, robust security measures, rigorous

testing and evaluation, effective communication, regulatory compliance, and stakeholder involvement. These recommendations, drawn from real-world experiences and perspectives, not only support existing academic views but also provide unique, empirically-grounded insights that could guide future blockchain applications in food retail supply chains. The findings and recommendations of this study bear significant implications for both academics and practitioners. For academics, the study contributes to the body of knowledge on cybersecurity risks in supply chains, the role of blockchain technology in mitigating these risks, and the practical aspects of implementing blockchain technology. For practitioners, particularly those in the food retail industry, the study provides valuable insights into the practical challenges and opportunities of leveraging blockchain technology for cybersecurity, offering potential pathways for its effective implementation.

6.1 Limitation of study and implications for future studies

Despite the significant insights this study provides, there are inherent limitations that need to be acknowledged. Firstly, the research is primarily based on a single case study, that of Walmart China. Although this approach has facilitated a detailed exploration of the topic, the findings may not be generalizable across different retail contexts, supply chain configurations, or geographic locations. Future research could benefit from considering multiple case studies in diverse settings to obtain a broader understanding of the challenges and opportunities associated with the application of blockchain technology for cybersecurity in supply chains. Secondly, while the study offered an in-depth examination of the role of blockchain technology in mitigating cybersecurity risks within supply chains, it did not explore other potentially relevant technologies, such as artificial intelligence or advanced data analytics. Future research could consider these or other emerging technologies to provide a more comprehensive view of the technological landscape for managing cybersecurity risks in supply chains.

Thirdly, the study relied on survey responses from participants involved in the implementation and management of the WCBTP. As a result, the insights derived could be influenced by the participants' perceptions, experiences, and understanding of the issues under consideration. To mitigate this limitation, future research could adopt a multi-method approach, combining surveys with other data collection methods such as interviews or document analysis to gain a richer, more nuanced understanding of the subject matter. Finally, the fast-paced nature of technological advancements and cybersecurity threats means that the findings of this study represent a snapshot in time. As technology and cybersecurity landscapes evolve, the risks, mitigation strategies, and effectiveness of technologies like blockchain may change. Therefore, there is a need for continuous research in this area to stay abreast of these changes and provide up-to-date insights to academics and practitioners. Addressing these limitations in future studies can contribute to a more robust understanding of the complex interplay between cybersecurity risks, supply chain management, and the role of technologies like blockchain in managing these risks.

References

Al-Ababneh, M. M. (2020). Linking ontology, epistemology and research methodology. *Science & Philosophy*, *8*(1), 75-91.

Appasani, B., Mishra, S. K., Jha, A. V., Mishra, S. K., Enescu, F. M., Sorlei, I. S., ... & Bizon, N. (2022). Blockchain-enabled smart grid applications: Architecture, challenges, and solutions. *Sustainability*, *14*(14), 8801.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?. *Available at SSRN 2709713*.

Bahari, S. F. (2010). Qualitative versus quantitative research strategies: contrasting epistemological and ontological assumptions. *Sains Humanika*, *52*(1).

Baldwin, J. (2022). *Cyber Supply Chain Risk Management (C-SCRM) across the Defense Industrial Base (DIB): A Cross-Sectional Survey of Nistir 8276 Key Practices* (Doctoral dissertation, Capitol Technology University).

Bamakan, S. M. H., Motavali, A., & Bondarti, A. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, *154*, 113385.

Bhat, S. A., Huang, N. F., Sofi, I. B., & Sultan, M. (2021). Agriculture-food supply chain management based on blockchain and IoT: a narrative on enterprise blockchain interoperability. Agriculture, 12(1), 40.

Bhattacharya, A., Geraghty, J., & Young, P. (2010). Supplier selection paradigm: An integrated hierarchical QFD methodology under multiple-criteria environment. *Applied Soft Computing*, *10*(4), 1013-1027.

Boone, A. (2017), "Cyber-security must be a C-suite priority", Computer Fraud & Security, Vol. 2017 No. 2, pp. 13-15. Boyes, H. (2015), "Cybersecurity and cyber-resilient supp

Boyens, J. M., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2020). Case studies in cyber supply chain risk management: summary of findings and recommendations.

Boyens, J. M., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). Cybersecurity Supply Chain Risk Management for Systems and Organizations.

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2021). *Cyber Supply Chain Risk Management Practices for Systems and Organizations* (No. NIST Special Publication (SP) 800-161 Rev. 1 (Draft)). National Institute of Standards and Technology.

Boyes, H. (2015), "Cybersecurity and cyber-resilient supply chains", Technology Innovation Management Review, Vol. 5 No. 4, pp. 28-34.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342-353.

Branthwaite, A., & Patterson, S. (2011). The power of qualitative research in the era of social media. *Qualitative Market Research: An International Journal*, *14*(4), 430-440.

Braun, V., Clarke, V., Boulton, E., Davey, L., & McEvoy, C. (2021). The online survey as a qualitative research tool. *International journal of social research methodology*, *24*(6), 641-654.

Bryman, A. (2006). Integrating quantitative and qualitative research: how is it done?. *Qualitative research*, *6*(1), 97-113.

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., ... & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of research in Nursing*, *25*(8), 652-661.

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. *Communications of the ACM*, *63*(7), 80-90.

Cheung, K. F., Bell, M. G., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*, 102217.

Cheung, K. F., Bell, M. G., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*, 102217.

Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: implications for operations and supply chain management. Supply Chain Management: An International Journal, 24(4), 469-483.

Crossan, F. (2003). Research philosophy: towards an understanding. *Nurse Researcher (through 2013)*, *11*(1), 46.

Di Pierro, M. (2017). What is the blockchain?. *Computing in Science & Engineering*, *19*(5), 92-95.

Etemadi, N., Borbon-Galvez, Y., Strozzi, F., & Etemadi, T. (2021). Supply chain disruption risk management with blockchain: A dynamic literature review. Information, 12(2), 70.

: A dynamic literature review. *Information*, *12*(2), 70.

Faisal, M.N., Banwet, D.K. and Shankar, R. (2007), "Information risks management in supply chains: an assessment and mitigation framework", Journal of Enterprise Information Management, Vol. 20 No. 6, pp. 677-699.

Fan, Y., & Stevenson, M. (2018). A review of supply chain risk management: definition, theory, and research agenda. *International journal of physical distribution & logistics management*, *48*(3), 205-230.

Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications*, *177*, 102936.

Feagin, J. R., Orum, A. M., & Sjoberg, G. (Eds.). (2016). *A case for the case study*. UNC Press Books.

Forbes (2019), How Walmart and others are riding a blockchain wave to supply chain paradise, available at: https://www.forbes.com/sites/biserdimitrov/2019/12/05/how-walmart-and-others-are-riding-a-blockchain-wave-to-supply-chain-paradise/, last accessed 01/06/2023

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.

Garg, R. (2016). Methodology for research I. *Indian journal of anaesthesia*, *60*(9), 640.

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223-240.

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.

Gordon, S. and Ford, R. (2006), "On the definition and classification of cybercrime", Journal in Computer Virology, Vol. 2 No. 1, pp. 13-20.

Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: A literature review. *Journal of Management Analytics*, *7*(3), 321-343.

Gurtu, A., & Johny, J. (2019). Potential of blockchain technology in supply chain management: a literature review. International Journal of Physical Distribution & Logistics Management, 49(9), 881-900.

Gurtu, A., & Johny, J. (2021). Supply chain risk management: Literature review. *Risks*, *9*(1), 16.

Hached, M. A. (2021). Supply chain cybersecurity and the implementation of Blockchain technology (Doctoral dissertation, Universidade NOVA de Lisboa (Portugal)).

Hampton, C., Sutton, S. G., Arnold, V., & Khazanchi, D. (2021). Cyber supply chain risk management: toward an understanding of the antecedents to demand for assurance. *Journal of Information Systems*, *35*(2), 37-60.

Hang, S. (2020), Walmart China subsidiary teams up with VeChain to trace food products, available at: https://cointelegraph.com/news/walmart-china-subsidiary-teams-up-with-vechain-to-trace-food-products, last accessed 02/06/2023

Hasan, I., & Habib, M. M. (2022). Blockchain technology to ensure traceability of agriculture supply chain management. *International Supply Chain Technology Journal*, *8*(09).

Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. IEEE Internet of Things Journal, 8(8), 6222-6246.

Hodkinson, P. (2008). Grounded theory and inductive research. In *Researching social life* (No. 5, pp. 80-100). Sage Publications Ltd.

Hofmann, F., Wurster, S., Ron, E., & Böhmecke-Schwafert, M. (2017, November). The immutability concept of blockchains and benefits of early standardization. In *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)* (pp. 1-8). IEEE.

Jadhav, J. S., & Deshmukh, J. (2022). A review study of the blockchain-based healthcare supply chain. *Social Sciences & Humanities Open*, *6*(1), 100328.

Jaikaran, C. (2018). Cyber supply chain risk management: An introduction. In *US Library of Congress*.

Kakavand, H., Kost De Sevres, N., & Chilton, B. (2017). The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. *Available at SSRN 2849251*.

Katsaliaki, K., Galetsi, P., & Kumar, S. (2021). Supply chain disruptions and resilience: A major review and future research agenda. *Annals of Operations Research*, 1-38.

Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a research paradigm and its implications for social work research. *Social sciences*, *8*(9), 255.

Khursheed, A., Kumar, M. and Sharma, M. (2016), "Security against cyber-attacks in food industry", International Journal of Control Theory and Applications, Vol. 9 No. 17, pp. 8623-8628.

Killam, L. (2013). *Research terminology simplified: Paradigms, axiology, ontology, epistemology and methodology*. Laura Killam.

King, N., & Brooks, J. (2018). Thematic analysis in organisational research. *The SAGE handbook of qualitative business and management research methods: Methods and challenges*, 219-236.

Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.

Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*, *31*(12), 4488-4500.

Kunnathur, A. (2015), "Information security in supply chains: a management control perspective", Information and Computer Security, Vol. 23 No. 5, pp. 476-496.

Levin, K. A. (2006). Study design III: Cross-sectional studies. *Evidence-based dentistry*, *7*(1), 24-25.

Mason, M. (2010, August). Sample size and saturation in PhD studies using qualitative interviews. In *Forum qualitative Sozialforschung/Forum: qualitative social research* (Vol. 11, No. 3).

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, *60*(1), 162-183.

Mohamed, N., & Al-Jaroodi, J. (2019, January). Applying blockchain in industry 4.0 applications. In *2019 IEEE 9th annual computing and communication workshop and conference (CCWC)* (pp. 0852-0858). IEEE.

Morgan, D. L. (2014). Pragmatism as a paradigm for social research. *Qualitative inquiry*, *20*(8), 1045-1053.

Mougayar, W. (2016). *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons.

Mukherjee, A. A., Singh, R. K., Mishra, R., & Bag, S. (2021). Application of blockchain technology for sustainability development in agricultural supply chain: Justification framework. *Operations Management Research*, 1-16.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*.

Natarajan, H., Krause, S., & Gradstein, H. (2017). Distributed ledger technology and blockchain.

NIST (2016), Cybersecurity supply chain risk management, available at: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management, last accessed 16/06/2023

Njie, B., & Asimiran, S. (2014). Case study as a choice in qualitative methodology. *Journal of research & method in Education*, *4*(3), 35-40.

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103-128.

Park, A., & Li, H. (2021). The effect of blockchain technology on supply chain sustainability performances. Sustainability, 13(4), 1726.

Parker, S., Wu, Z., & Christofides, P. D. (2023). Cybersecurity in process control, operations, and supply chain. *Computers & Chemical Engineering*, 108169.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669-710.

Qian, J., Wu, W., Yu, Q., Ruiz-Garcia, L., Xiang, Y., Jiang, L., ... & Yang, P. (2020). Filling the trust gap of food safety in food trade between the EU and China: An interconnected conceptual traceability framework based on blockchain. Food and Energy Security, 9(4), e249.

Rane, S. B., Thakker, S. V., & Kant, R. (2021). Stakeholders' involvement in green supply chain: a perspective of blockchain IoT-integrated architecture. *Management of Environmental Quality: An International Journal*, *32*(6), 1166-1191.

Raut, R. D., Gotmare, A., Narkhede, B. E., Govindarajan, U. H., & Bokade, S. U. (2020). Enabling technologies for Industry 4.0 manufacturing and supply chain: concepts, current status, and adoption challenges. *IEEE engineering management review*, *48*(2), 83-102.

Raza, Z., & Singh, A. K. (2022). A framework for the blockchain and IoT-based supply chain management system. *International Journal of Applied Logistics (IJAL)*, *12*(1), 1-30.

Sarode, R. P., Poudel, M., Shrestha, S., & Bhalla, S. (2021). Blockchain for committing peer-to-peer transactions using distributed ledger technologies. *International Journal of Computational Science and Engineering*, *24*(3), 215-227.

Saunders, M. N., Lewis, P., Thornhill, A., & Bristow, A. (2015). Understanding research philosophy and approaches to theory development.

Saunders, M., Lewis, Philip., & Thornhill, A. (2007). Research methods. *Business Students 4th edition Pearson Education Limited, England*, *6*(3), 1-268.

Singh, S., & Singh, N. (2016, December). Blockchain: Future of financial and cyber security. In *2016 2nd international conference on contemporary computing and informatics (IC3I)* (pp. 463-467). IEEE.

Smith, J. A. (2015). Qualitative psychology: A practical guide to research methods. *Qualitative psychology*, 1-312.

Soiferman, L. K. (2010). Compare and Contrast Inductive and Deductive Research Approaches. *Online Submission*.

Spanò, R., Massaro, M., Ferri, L., Dumay, J., & Schmitz, J. (2022). Blockchain in accounting, accountability and assurance: an overview. *Accounting, Auditing & Accountability Journal*, *35*(7), 1493-1506.

Syed, N. F., Shah, S. W., Trujillo-Rasua, R., & Doss, R. (2022). Traceability in supply chains: A Cyber security analysis. *Computers & Security*, *112*, 102536.

Tan, B., Yan, J., Chen, S., & Liu, X. (2018). The impact of blockchain on food supply chain: The case of walmart. In Smart Blockchain: First International Conference, SmartBlock 2018, Tokyo, Japan, December 10–12, 2018, Proceedings 1 (pp. 167-177). Springer International Publishing.

Tapscott, D., & Tapscott, A. (2017). How blockchain will change organizations. *MIT Sloan Management Review*, *58*(2), 10.

Topping, C., Dwyer, A., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. *Computers & Security*, *108*, 102324.

Tran, T., Childerhouse, P. and Deakins, E. (2016), "Supply chain information sharing: challenges and risk mitigation strategies", Journal of Manufacturing Technology Management, Vol. 27 No. 8, pp. 1102-1126

Turjo, M. D., Khan, M. M., Kaur, M., & Zaguia, A. (2021). Smart supply chain management using the blockchain and smart contract. *Scientific programming*, *2021*, 1-12.

Uddin, M. A., & Venkatesh, N. (2019). Managing Supply Chain of Food Industry in India.

Ünal, V., Ömürgönülşen, M., Belbağ, S., & Soyasal, M. (2020). The internet of things in supply chain management. In *Logistics 4.0* (pp. 27-34). CRC Press.

Urciuoli, L., Männistö, T., Hintsa, J. and Khan, T. (2013), "Supply chain cyber security – potential threats", Information & Security: An International Journal, Vol. 29, pp. 51-68.

Vanajakumari, M., Analytics, B., Mittal, S., Stoker, G., & Clark, U. (2020). Leader-Driven Supply Chain Cybersecurity Framework. In *Proceedings of the Conference on Information Systems Applied Research ISSN* (Vol. 2167, p. 1508).

Vlajic, J. V., Van der Vorst, J. G., & Haijema, R. (2012). A framework for designing robust food supply chains. *International Journal of Production Economics*, *137*(1), 176-189.

Vu, N., Ghadge, A., & Bourlakis, M. (2023). Blockchain adoption in food supply chains: A review and implementation framework. *Production Planning & Control*, *34*(6), 506-523.

Walmart (2021), Blockchain in the food supply chain, what does the future look like? Available at: https://tech.walmart.com/content/walmart-global-tech/en_us/news/articles/blockchain-in-the-food-supply-chain.html, last accessed 01/06/2023

Whyte, S. T., Omoyiola, B. O., & Okoni, B. (2022). Use of Blockchain Technology in Data Integrity Assurance. *Available at SSRN 4043164*.

Williams, C. (2014), "Security in the cyber supply chain: is it achievable in a complex, interconnected world?", Technovation, Vol. 34 No. 7, pp. 382-384

Windelberg, M. (2016). Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection*, *12*, 4-11.
Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342-353.

World Economic Forum (2022), Is blockchain really secure? Here are four pressing cyber threats you must consider, available at: https://www.weforum.org/agenda/2023/02/blockchain-has-high-potential-but-beware-of-cyber-threats-8642651f20/, last accessed 01/06/2023

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: a review. *SN Computer Science*, *3*(2), 127.

Xi, P., Zhang, X., Wang, L., Liu, W., & Peng, S. (2022). A review of Blockchain-based secure sharing of healthcare data. Applied Sciences, 12(15), 7912.

Xu, J., Guo, S., Xie, D., & Yan, Y. (2020). Blockchain: A new safeguard for agri-foods. Artificial Intelligence in Agriculture, 4, 153-161.

Xu, Z., & Zou, C. (2021). What can blockchain do and cannot do?. *China Economic Journal*, *14*(1), 4-25.

Yurchenko, A., Moni, M., Peters, D., Nordholz, J., & Thiel, F. (2020, May). Security for Distributed Smart Meter: Blockchain-based Approach, Ensuring Privacy by Functional Encryption. In *CLOSER* (pp. 292-301).

Zalaghi, H., & Khazaei, M. (2016). The role of deductive and inductive reasoning in accounting research and standard setting. *Asian Journal of Finance & Accounting*, *8*(1), 23-37.