Volume 3 Issue 1 (2026) 73-91
E-ISSN 2988-6740| © Authors. CC BY-SA
https://doi.org/10.59261/iclr.v3i1.31
https://iclr.polteksci.ac.id/

Indonesian Cyber Law Review

Cross-Jurisdictional Law Against Cybercrime Using Private Blockchain in Global Supply Chain: A Case Study of the Food Industry

Wahyu Beny Mukti Setiyawan
Universitas Negeri Semarang, Indonesia
*Corresponding Author: muktibeny@mail.unnes.ac.id

ABSTRACT

This study examines the cross-jurisdictional legal challenges in addressing cybercrime involving private blockchain technology in the global food supply chain. The research aims to identify cybersecurity risks, evaluate the adequacy of national and international regulations, and analyze mitigation strategies implemented by companies. A qualitative approach with a case study design was used, involving in-depth interviews with company managers, IT security teams, and regulators, as well as observations of blockchain implementation and documentation analysis. The findings indicate that private blockchains, while improving traceability and transparency, remain vulnerable to internal threats, malware, phishing, and system vulnerabilities. Legal challenges include overlapping jurisdictions, regulatory differences, and complex extradition processes, which hinder timely law enforcement. Companies adopt comprehensive mitigation strategies, including role-based access control, secure smart contracts, encryption, and collaboration with international regulators. The study concludes that an integrative approach combining technological safeguards, internal governance, and cross-jurisdictional legal coordination is critical to ensuring data integrity, regulatory compliance, and the resilience of global food supply chains to cyberthreats. This research contributes to understanding the intersection of blockchain technology, cybersecurity, and international law in the context of global trade.

Keywords: cross-jurisdictional law, cybercrime, private blockchain, global food supply chain, regulatory compliance

Article received on 15-07-2025 — Final revised on 13-11-2025 — Approved on 19-12-2025

Introduction

Advances in information technology have brought fundamental changes to various aspects of human life, including international trade and global supply chain management, where efficiency, traceability, and security are crucial. One innovation that is increasingly being implemented is blockchain, a decentralized and transparent transaction recording system that allows every transaction to be permanently recorded and verified by authorized parties. In the context of the food industry, blockchain is being utilized to ensure product

safety, reduce the risk of fraud or contamination, and improve distribution efficiency from producer to consumer. The advantages of this technology not only emphasize data accuracy and transparency but also play a role in building consumer trust in product quality and origin. However, behind these significant benefits, there are serious challenges related to cybersecurity, particularly in dealing with the possibility of internal and external attacks that can threaten data integrity (Ali et al., 2021). Although blockchain systems offer a higher level of security than conventional systems through encryption and consensus mechanisms, the risk of attacks remains, particularly on private blockchains that connect multiple parties across jurisdictions. This situation raises complex legal and technical issues, as a cybersecurity breach on a private network affects not only one party but can impact the entire global supply chain, causing financial losses, distribution disruptions, and questions of legal responsibility between countries (Lu et al., 2020).

Cybercrime occurring within the context of global supply chains has far-reaching and complex impacts, ranging from financial losses to companies, disruptions to food distribution, and even a decline in consumer confidence in product safety and quality. Furthermore, cross-jurisdictional legal risks are becoming increasingly crucial, as transactions and data stored on private blockchains are not confined to a single country but can involve multiple jurisdictions simultaneously (Ramanan & Nakayama, 2020). This situation raises fundamental questions regarding the legal authorities authorized to handle cybercrime cases, the legal responsibility of perpetrators, and the international law enforcement mechanisms that can be implemented to ensure compliance and protection for all parties involved. These issues are further complicated by differences in regulations and legal procedures across countries that can hinder effective investigations and law enforcement processes. Therefore, this situation emphasizes the urgent need for a comprehensive understanding of the interaction between blockchain technology, cybersecurity threats, and cross-jurisdictional legal frameworks, particularly in the context of the global food industry, so that risk mitigation strategies, regulatory policies, and corporate governance practices can be effectively designed to address the multidimensional legal and technical challenges (Centobelli et al., 2022).

In this context, there are several crucial issues that need to be addressed in managing private blockchains in the global food supply chain. First, the vulnerability of private blockchains to cybercrime remains a significant challenge. Although private blockchains are designed with more stringent security mechanisms than public blockchains, such as data encryption and access restrictions, the risk of attacks from both internal and external parties remains possible and has the potential to compromise the integrity and accuracy of transaction data. This is crucial considering that data errors or manipulation can directly impact product security and consumer trust. Second, cross-jurisdictional jurisdictions present complex challenges when cybercrime involves parties from different countries (Shamshad et al., 2020). These issues include determining the jurisdiction authorized to handle cases, extradition procedures, law enforcement cooperation mechanisms, and the application of relevant international trade regulations. This demonstrates that law enforcement against cybercriminals cannot be carried out unilaterally but requires effective cross-border coordination. Third, regulatory compliance with technology is a critical issue, as national and international regulations often have not fully adapted to blockchain developments, both technically and legally. This mismatch creates legal loopholes and potential conflicts between jurisdictions, requiring companies utilizing private blockchains to develop additional internal protocols and risk mitigation strategies to ensure legal compliance and comprehensive supply chain security (Li et al., 2021).

Based on a recent literature review, the use of private blockchains in the food industry has been shown to play a crucial role in ensuring product traceability, increasing transaction

transparency, and reducing fraudulent practices during distribution. This technology allows every stage of the supply chain to be permanently recorded and verifiable by authorized parties, significantly minimizing the potential for data errors and fraud. However, although private blockchains are designed with a higher level of security than public blockchains, these systems still face the risk of internal and external attacks, including the possibility of data manipulation by authorized parties and the exploitation of existing technical vulnerabilities (Polge et al., 2021). From a legal perspective, several studies emphasize the importance of harmonizing cross-jurisdictional regulations in addressing cybercrime, given that criminal acts in one country can impact parties in other countries, making unilateral law enforcement ineffective. However, research that comprehensively integrates cross-jurisdictional legal analysis with case studies of private blockchain implementation in the food industry remains relatively limited. This underscores the need for studies that simultaneously combine technology, cybersecurity, and international law perspectives to provide practical guidance for companies and regulators in addressing the legal and technical challenges of an increasingly complex global supply chain (Chang et al., 2020).

Several previous studies have explored various aspects related to blockchain, cybersecurity, and international law, although these studies tend to be conducted separately. Studies on blockchain and cybersecurity typically focus on the technical mechanisms supporting blockchain systems, including encryption, consensus, and access control, and identify their potential vulnerabilities to digital attacks, both internal and external. Meanwhile, research in the field of international cyberlaw emphasizes the importance of cooperation between countries in law enforcement against cybercrime, as criminals can operate across jurisdictions, making international legal coordination a key factor in ensuring effective law enforcement and the protection of affected parties (Wang et al., 2021). On the other hand, studies on blockchain in the food supply chain have focused more on improving distribution efficiency, transaction transparency, and product traceability from producer to consumer. However, there is still a lack of research that thoroughly examines the legal risks arising from cybercrime or cross-jurisdictional regulatory challenges. This situation indicates a significant research gap: the lack of studies that simultaneously integrate technical analysis, cybersecurity, and cross-jurisdictional legal perspectives, even though the integration of these three aspects is crucial to ensuring the security, legal compliance, and sustainability of the global food supply chain (R. Yang et al., 2020).

A research gap that has emerged is the limited number of studies that simultaneously explore the interplay between private blockchain, cybercrime threats, and cross-jurisdictional law in the context of the global food industry. Most previous studies tend to address the technology, cybersecurity, or legal regulatory aspects separately, thus failing to provide a comprehensive understanding of the challenges that arise when these three elements are interconnected. This research seeks to address this gap by integrating technical and legal perspectives, while emphasizing analysis through case studies of real-world practices in the food industry (Mazlan et al., 2020). This approach allows for a more comprehensive assessment of the effectiveness of private blockchains in minimizing cyber risks, while simultaneously implementing cross-jurisdictional legal mechanisms to address digital breaches and crimes. Thus, this research not only broadens academic knowledge regarding the relationship between blockchain technology and international law but also provides practical guidance for companies and regulators in managing cybersecurity and legal compliance in the increasingly complex global food supply chain (Toufaily et al., 2021).

This research adopts an interdisciplinary approach that combines various theoretical frameworks and methods to gain a comprehensive understanding of the interaction between blockchain technology, cybersecurity, and cross-jurisdictional law in the context of the food

industry. First, cross-jurisdictional legal theory is used to examine the legal authority, responsibilities of parties, and applicable law enforcement mechanisms in international cybercrime cases, particularly when violations involve actors from various countries. Second, a cyber law and technology approach is applied to evaluate the extent to which national and international regulations are able to anticipate and regulate cyberattacks against private blockchains, including the effectiveness of legal protocols in ensuring data integrity and supply chain security. Third, a qualitative case study is used to gain an in-depth understanding of the dynamics of private blockchain implementation in food industry practice, including the experiences of practitioners and regulators in identifying, analyzing, and mitigating emerging cyber risks. The integration of these three approaches allows the research to not only examine technical and legal aspects separately but also explore how the combination of regulation, technology, and field practice can form an effective strategy for managing cybersecurity and ensuring cross-jurisdictional legal compliance in the global food supply chain (Yu et al., 2021).

This research aims to provide a comprehensive understanding of the interplay between private blockchain technology, cybersecurity, and cross-jurisdictional law in the context of the global food supply chain. First, the research aims to identify the cross-jurisdictional legal challenges that arise when cybercrime occurs within private blockchain networks, including issues related to authority, legal liability, and effective international law enforcement mechanisms. Second, the research focuses on analyzing the cybersecurity risks and vulnerabilities inherent in the implementation of private blockchain in the food industry, including the potential for internal and external attacks, data manipulation, and the exploitation of technical loopholes that could compromise supply chain integrity. Third, the research evaluates the compatibility of national and international regulations with the practical use of blockchain technology, particularly in terms of the legal regime's ability to anticipate cyber threats and support transparency and accountability in the global supply chain. Fourth, the research aims to develop applicable legal and technological recommendations to enhance security, transparency, and legal certainty, while also providing guidance for companies and regulators in addressing cyber risks and ensuring compliance with cross-jurisdictional regulations. With this approach, the research not only expands the academic literature but also generates relevant practical implications for the global food industry, which is increasingly dependent on blockchain technology (Abou-Nassar et al., 2020).

This research is expected to provide broad contributions and benefits across multiple dimensions. From an academic perspective, this research aims to add to the scientific literature that comprehensively discusses the relationship between private blockchain technology, cross-jurisdictional law, and cybersecurity in the context of the global food industry, thereby strengthening the theoretical foundation for further studies. Practically, the findings of this research are expected to guide regulators, legal practitioners, and food industry players in designing cybercrime risk mitigation strategies and ensuring the implementation of private blockchain that is secure, transparent, and in accordance with applicable laws. At the policy level, this research is expected to provide useful input for the development of national and international regulations that are more responsive to technological advances and the operational needs of the global supply chain, thus creating a balance between technological innovation, cybersecurity, and legal certainty that supports the sustainability and effectiveness of the global food supply chain (Makhdoom et al., 2020).

Research Method

This research employs a qualitative method with a case study approach, chosen because it focuses on understanding the complex phenomenon of the interaction between private blockchain technology, cybercrime, and cross-jurisdictional law in the context of global supply chains in the food industry. The case study approach allows researchers to explore real-world practices in depth and gain insights from various stakeholders, including food companies, regulators, and international legal experts, so that the resulting analysis reflects authentic and practically relevant field dynamics (Ul Hassan et al., 2019).

This research was conducted at a food industry company that has implemented private blockchain in its supply chain, as well as at the offices of regulators and legal institutions authorized to handle cybercrime and international trade. The selection of these locations was based on several key considerations. First, the selected companies have direct experience in using private blockchain, thus providing valid and relevant empirical data. Second, regulators and legal experts are important sources of information for gaining an understanding of cross-jurisdictional legal implementation. Third, the research locations reflect the global context of the food supply chain, given that the companies operate across borders, making analysis of international legal aspects relevant and applicable (Shayan et al., 2021).

This research utilizes primary and secondary data to gain a comprehensive understanding. Primary data was obtained through in-depth interviews with food company management responsible for blockchain implementation, the cybersecurity team, and operational staff involved in the process. Interviews were also conducted with national and international regulators dealing with cybersecurity and food trade issues, as well as through direct observation of the company's supply chain processes and use of private blockchain. Meanwhile, secondary data was obtained from company documents, including data security policies, standard operating procedures (SOPs) for blockchain use, and internal audit reports; scientific literature related to private blockchain, international cyber law, and global supply chains; national and international regulations governing cybersecurity, food trade, and cross-jurisdictional law; and reports of cybercrime cases relevant to the food industry supply chain (Yazdinejad et al., 2020).

Data collection in this study was conducted through several primary techniques. First, semi-structured interviews were used to explore informants' experiences, perspectives, and best practices regarding private blockchain implementation and the cross-jurisdictional legal challenges they face. Interview questions were designed to be flexible, allowing for in-depth and contextual data collection based on the situation on the ground. Second, field observations were conducted by directly observing operational activities in supply chains utilizing private blockchain, focusing on data flows, security mechanisms, and potential vulnerabilities to cyberattacks. Third, a documentary study involved analyzing internal company documents, legal regulations, and cybercrime case reports, which were used to complement the interview and observation results and verify the consistency and accuracy of the information obtained (Huang et al., 2020).

The research data was analyzed using thematic analysis, which involved several systematic steps. First, interviews were transcribed to facilitate the identification of patterns, themes, and categories relevant to the research focus. Second, data were coded based on key themes, such as cybercrime risks, cross-jurisdictional legal challenges, and mitigation practices implemented by companies. Third, data triangulation was conducted by comparing findings from interviews, field observations, and documents to ensure the validity and reliability of the information obtained. Fourth, legal case analysis was conducted by examining real-life examples, allowing for an assessment of the effectiveness of national and international law in combating cybercrime (Casino et al., 2021).

To ensure the validity and credibility of the research, the researchers implemented several strategies. First, source triangulation was conducted by comparing information obtained from companies, regulators, and the literature to obtain a comprehensive understanding. Second, method triangulation was implemented by integrating interviews, field observations, and documentation studies to strengthen data accuracy. Third, member checking was conducted by confirming data interpretations with key informants to ensure the researcher's understanding aligned with their perspectives. Fourth, an audit trail was implemented by storing all documents, interview transcripts, and field notes, so that the verification process and transparency of the research could be carried out systematically (Cao et al., 2020).

This research specifically focuses on several key aspects. First, it analyzes the potential cybercrime risks associated with the use of private blockchain in global supply chains in the food industry. Second, it identifies the cross-jurisdictional legal challenges that arise when cybercrime involves parties from various countries. Third, it evaluates the suitability of both national and international regulations governing the implementation of blockchain technology in supply chains. Fourth, it develops recommendations for legal and technological practices, including cyber risk mitigation mechanisms and effective cross-jurisdictional legal governance strategies, to ensure security and compliance in global supply chain operations (Khan et al., 2021).

Result and Discussion

Table 1. Cybercrime Risks in Private Blockchain in Food Industry Supply Chain

Cyber Risk	Impact	Field Findings
Insider Threat	Manipulation of transaction data and distribution of food products	One company experienced an attempted data manipulation by internal staff who had full access to the private blockchain.
Malware and Phishing	Operational disruptions and data theft	The company's IT team noted a phishing attempt against a blockchain operator account that could impact the product's track record.
System Vulnerability	Loss of data integrity and reputation	An internal audit revealed a security flaw in the smart contract that could be exploited to falsify distribution information.

The table shows that while private blockchains offer higher security than conventional systems, these ecosystems remain vulnerable to a variety of complex cyberthreats. Significant threats arise from within organizations through insider threats, where individuals with privileged access can exploit weaknesses in internal controls to unauthorizedly manipulate transaction data, thus threatening the integrity of information within the supply chain. Externally, malware and phishing attacks demonstrate that the human factor remains a crucial weakness, making protection of user interactions and cybersecurity training programs essential components of mitigation strategies. Furthermore, system vulnerabilities, particularly in smart contracts, emphasize that despite the advanced nature of blockchain technology, technical vulnerabilities can still be exploited. Therefore, conducting regular audits, system security testing, and strengthening operational protocols are crucial steps to maintain data integrity, ensure product traceability, and enhance network resilience against both internal and external cyberthreats. This comprehensive approach emphasizes that risk management in private blockchains requires a synergy between technical strategies, internal

policies, and consistent oversight procedures to ensure optimal supply chain security and reliability.

Table 2. Cross-Jurisdictional Legal Challenges to Cybercrime

Legal Challenges	Implications	Field Findings
Layered Jurisdiction	Difficulty in determining which country has the authority to prosecute cyber criminals	Data manipulation cases occur across countries, thus requiring legal coordination between national and international regulators.
Regulatory Differences	Conflict of laws and different enforcement procedures	Some countries have different cybersecurity regulations, making consistent investigation and enforcement difficult.
Extradition and Cooperation Mechanisms	The legal process is slow and complex	The company experienced delays in its investigation due to differences in extradition mechanisms between countries regarding cyber perpetrators.

The above table illustrates that one of the key challenges in addressing cybercrime in global supply chains is closely related to the complexity of cross-jurisdictional laws. Overlapping jurisdictions make it difficult to determine which authority should prosecute perpetrators, while differences in regulations between countries have the potential to create legal conflicts that slow down investigations and law enforcement. Furthermore, lengthy extradition procedures and complex international legal cooperation mechanisms also slow the response to cyber incidents, increasing the risk to a company's operational integrity. This situation emphasizes the need for companies to implement a comprehensive risk mitigation strategy, encompassing compliance with national and international regulations, effective coordination with regulators and legal authorities across borders, adjustments to internal procedures, and proactive mechanisms to maintain data security and product traceability in the global supply chain. Such a holistic approach is essential for companies to navigate cross-jurisdictional legal challenges while maintaining the reputation and sustainability of their supply chains in the digital age.

Tabel 3. Regulatory Compliance Evaluation of Private Blockchain in the Food Industry

Regulatory Aspects	Findings	Impact on Corporate Practices
Compliance with National Regulations	National regulations are quite clear but do not yet specifically regulate blockchain.	The company created additional internal SOPs to ensure transaction security and product traceability.
Harmonization with International Regulations	There are still gaps in cross-jurisdictional laws	Cross-border legal coordination often requires additional consultation and negotiation, especially for data security cases.
Consumer Protection and Data Security	Regulations emphasize product traceability and data privacy	The company uses double encryption and strict access controls to meet consumer security and regulatory standards.

This table illustrates that current regulations are still limited in accommodating the complexities of blockchain technology, particularly private blockchains, in supply chains. While national regulations have established standards for data security and product traceability, rules specifically governing the implementation of private blockchains are still lacking, posing challenges for companies in ensuring legal compliance. The lack of international regulatory alignment further exacerbates the challenges of cross-border coordination, particularly for companies operating globally. As a mitigation measure, companies are developing additional standard operating procedures (SOPs) and strengthening internal security protocols, including the implementation of double data encryption, role-based access controls, and regular internal audits, to ensure the integrity, security, and accuracy of transactions in the supply chain. This comprehensive mitigation approach not only supports compliance with national and international regulations but also enhances stakeholder trust, maintains product traceability, and reduces the risk of cybersecurity breaches that could potentially disrupt the smooth operation of the food supply chain.

Table 4. Technology and Legal Mitigation and Governance Practices

Mitigation Strategy	Implementation	Effectiveness
Internal Security Strengthening	Implementation of role-based access control and routine audits	Reduce the risk of insider threats and ensure the integrity of transaction data.
Cross-Border Collaboration	Cooperation with international regulators and legal authorities	Facilitating coordination of law enforcement against cybercriminals across jurisdictions.
Blockchain Security Protocol	Secure use of smart contracts and data encryption	Ensure traceability of food products and reduce the risk of data manipulation or leakage.

This table illustrates various mitigation practices implemented by companies and regulators to address the risk of cybercrime in the global food supply chain. Strengthening internal security through regular audits and implementing role-based access controls has proven effective in reducing the risk of insider threats, namely the potential misuse of systems by individuals with specific access rights to manipulate data. Furthermore, cross-border cooperation is a crucial component in overcoming legal constraints and regulatory differences between countries, allowing for a faster response to cyber incidents while ensuring compliance with various jurisdictions. From a technological perspective, the implementation of blockchain security protocols, including secure smart contracts and multi-layered data encryption, not only improves product traceability but also maintains the integrity and accuracy of information throughout the supply chain. Therefore, the integration of mitigation strategies encompassing technical, regulatory, and internal procedural aspects provides a crucial foundation for minimizing cyber risk, strengthening stakeholder trust, and ensuring the sustainability and security of operations in the increasingly digitalized global food industry.

Cybercrime Risks in Private Blockchain

The research findings indicate that cyber risks associated with implementing private blockchains in the food industry are multidimensional, encompassing both technical and operational aspects, with the primary threats being insider threats, malware/phishing attacks, and system vulnerabilities. Insider threats arise when staff with full access to the blockchain system can abuse that access to unauthorized transaction data, thereby compromising the integrity of information throughout the supply chain. These findings confirm that even

though private blockchains are built with sophisticated security mechanisms, limitations in internal oversight and access control still pose significant risks to data accuracy and reliability. This aligns with research by Conti et al. (2018), which emphasized that insider threats are one of the most critical threats in private blockchain systems, as the activities of actors with authorized access rights are difficult to detect through standard security procedures. Therefore, an effective risk mitigation strategy needs to integrate strengthened technical protocols, including regular audits, data encryption, and role-based access control, with stringent internal policies, such as internal oversight SOPs and employee training programs. This holistic approach is designed to reduce the potential for data manipulation, maintain the integrity and traceability of transactions, and ensure the security and reliability of the entire food supply chain amidst the ever-evolving complexity of cyber threats (Rahman et al., 2020).

In addition to threats originating from internal factors, this study also reveals the increasing risk of malware and phishing attacks targeting blockchain operator accounts, indicating that the human element remains a major weakness in systems technically designed with high levels of security. This situation emphasizes that advanced technologies such as layered encryption, multifactor authentication, and consensus mechanisms in private blockchains cannot fully guarantee protection if users' digital security awareness and discipline remain low. Consistent with the findings of Li et al. (2020), social engineering-based attacks such as phishing and malware demonstrate that cybercriminals often exploit user negligence or limited digital literacy to penetrate even secure systems. In the context of the global food supply chain, such attacks have the potential to cause serious disruptions to company operations, manipulate transaction data, and even violate international food safety standards. Therefore, cyber risk mitigation cannot focus solely on strengthening technical aspects but must also include improving the quality of human resources through continuous cybersecurity training, attack simulations to test phishing preparedness, and the implementation of strict access control policies based on the principle of "least privilege." This comprehensive approach is a strategic step in realizing a blockchain system that is not only technically robust, but also operationally resilient, by ensuring that every user understands their role in maintaining the authenticity, integrity, and reliability of data throughout the digital food supply chain (Sun et al., 2021).

In addition to risks caused by human factors, this study shows that system vulnerabilities, particularly those related to smart contracts, are a major challenge in implementing private blockchain in the food supply chain. Internal audit results identified vulnerabilities that could potentially be exploited to manipulate product distribution information, which could lead to reduced data integrity, accuracy, and consistency throughout the supply chain. These findings align with (Wenhua et al., 2023), who emphasized that while smart contracts play a crucial role in automating blockchain transactions, they remain vulnerable to exploitation if security protocols are not rigorously implemented and system testing is not thorough. Therefore, implementing best practices in smart contract design, systematic, iterative testing, and thorough internal and external audits are crucial steps in mitigating these risks. In addition to strengthening the technical security and operational stability of the blockchain, this approach also enhances stakeholder trust by ensuring transaction traceability and accuracy, as well as protecting data from potential manipulation and misuse. Therefore, this integrated risk mitigation strategy lays the foundation for creating a secure, transparent, and reliable food supply chain capable of facing the increasingly complex cyber challenges of the digitalization of the global food industry.

The findings of this study highlight that cyber risks in the implementation of private blockchains directly impact the integrity and sustainability of the food supply chain. Disruptions in the form of manipulation or loss of transaction data can hinder product

traceability, challenging companies to ensure that each stage of distribution is recorded accurately, transparently, and verifiable by all stakeholders. The impact of these issues is not only financial, but also impacts the company's reputation and reduces consumer confidence in the safety, quality, and security of food products. These findings align with the results of a study by Saberi et al. (2019), which emphasized the importance of blockchain in maintaining transparency, accountability, and trust in the global food supply chain, particularly in the context of international trade involving multiple parties and legal jurisdictions. Therefore, companies need to implement comprehensive risk mitigation strategies, including strengthening technical security protocols through layered encryption and role-based access control, conducting regular internal and external audits to ensure data accuracy and integrity, and conducting training programs for all blockchain system users to increase awareness and preparedness for cyber threats. With this kind of integrated approach, companies can ensure the reliability, integrity, and traceability of their supply chains, while strengthening consumer trust and supporting the sustainability of food supply chain operations amidst the complexities of the digitalization of the global food industry (Raja Santhi & Muthuswamy, 2022).

In conclusion, the existence of internal, external, and systemic risks in the implementation of private blockchain in the food supply chain emphasizes the importance of implementing a comprehensive and coordinated mitigation strategy. This strategy includes strengthening internal controls through access restrictions and monitoring staff activities, increasing cybersecurity awareness and training for all users, and conducting regular audits to ensure compliance with security protocols and maintain data integrity. The findings of this study indicate that although private blockchains are designed with stronger security mechanisms than conventional systems, this technology remains vulnerable to threats from human factors and technical weaknesses, thus requiring comprehensive risk management. This aligns with cybersecurity literature, which emphasizes that risk mitigation in private blockchain systems must be carried out multidimensionally, incorporating policies, operational procedures, and layered oversight, to optimally maintain data reliability, transparency, and stakeholder trust in the global food supply chain (Han et al., 2020).

Cross-Jurisdictional Legal Challenges to Cybercrime

The findings of this study indicate that law enforcement efforts against cybercrime in the global supply chain face highly complex challenges due to overlapping jurisdictions, differences in regulations between countries, and lengthy extradition processes involving multiple legal and administrative procedures. These conditions create structural barriers in determining the competent authority to prosecute perpetrators, thus slowing the investigation process, reducing the effectiveness of law enforcement, and opening opportunities for perpetrators to exploit existing legal loopholes. This aligns with a study by Meltzer (2013), which emphasized that transnational cybercrime raises serious jurisdictional issues due to differences in legal systems and interpretations between countries, while the nature of digital attacks allows perpetrators to operate without geographical boundaries. In the context of implementing private blockchain in the global food supply chain, these challenges are even more pronounced because the decentralized system involves multiple entities from countries with varying legal frameworks and regulatory standards. Therefore, it is necessary to establish a more adaptive international legal framework and strengthen cross-jurisdictional coordination mechanisms capable of responding to the dynamics of cybercrime quickly and transparently. On the other hand, companies and regulators need to develop comprehensive mitigation strategies, including harmonizing cross-border compliance policies, enhancing law enforcement's capacity to understand blockchain technology, and implementing digital audits

that enable real-time transaction monitoring. With this collaborative and flexible approach, the integrity, security, and sustainability of the global food supply chain can be maintained amidst the ever-evolving and increasingly complex threat of cybercrime (Garg et al., 2020).

Regulatory differences across countries present complex challenges in cybercrime law enforcement, particularly regarding the management of private blockchains in global food supply chains. Variations in legal standards, regulatory priorities, and regulatory focus are often inconsistent. For example, some countries emphasize consumer data protection through strict regulations on privacy, information access control, and user rights, while others focus more on network security, system audits, or product traceability within the supply chain. This discrepancy not only slows down investigations and enforcement but also creates legal loopholes that cybercriminals can exploit, increasing risks to the integrity, accuracy, and security of supply chains. This aligns with Greenberg's (2018) findings, which emphasize that cross-jurisdictional regulatory conflicts are a major obstacle to international legal coordination, as cybercrime often involves parties from countries with different legal frameworks. Therefore, companies and regulators need to design adaptive and flexible compliance mechanisms, including aligning operational procedures with the legal requirements of various jurisdictions, developing internal policies responsive to regulatory changes, and establishing cross-country collaborative frameworks to support effective information exchange, law enforcement coordination, and risk mitigation. This integrated approach not only strengthens legal risk management, but also maintains the integrity, transparency, and accountability of the entire supply chain, enabling companies to conduct global operations safely, legally, and sustainably amidst the complexity of ever-changing international regulations (X. Yang et al., 2021).

Delays in the extradition process add significant complexity to law enforcement against cross-jurisdictional cybercrime, particularly for companies managing the global food supply chain. In this study, several companies reported that investigations into cyber incidents are often hampered by differences in legal procedures, administrative requirements, and bureaucracy across countries, delaying swift and effective prosecution of perpetrators. This finding is consistent with a study by (Bera et al., 2021), which stated that extradition procedures in cybercrime cases often do not align with the demands of international law enforcement, which demand a swift response, given that cyberattacks can cross national borders in a short time. This situation highlights the limited effectiveness of international law in addressing cyber threats, prompting companies and regulators to proactively design additional mitigation strategies. These strategies include intensive coordination with legal authorities in various countries, strengthening internal oversight mechanisms, and implementing risk mitigation procedures that ensure the security, integrity, and traceability of data throughout the supply chain. Therefore, the integration of these legal and technical measures is key to minimizing the impact of investigation delays on company operations while maintaining the resilience of the global food supply chain in the face of increasingly complex and dynamic cyber threats.

Furthermore, the complexity of cross-jurisdictional laws directly impacts the formulation of cyber risk mitigation strategies by companies, particularly in the context of managing private blockchains in the global food supply chain. Differences in regulations between countries and overlapping jurisdictions pose challenges that require companies to proactively coordinate with regulators at both the national and international levels. These efforts include conducting regular legal consultations, adjusting internal operational procedures, and updating compliance policies to align with cross-jurisdictional legal standards. Through this approach, companies are able to anticipate potential legal conflicts, expedite responses to cyber incidents, while maintaining product integrity, security, and

traceability throughout the global supply chain. This finding aligns with literature emphasizing the importance of international legal collaboration as a key strategy in mitigating cross-border cyber risks, as stated by (Lin et al., 2021), who highlights that multinational cooperation, information exchange, and regulatory coordination are key factors in addressing the legal and operational challenges of cross-jurisdictional digital transactions. This collaborative approach serves as a critical foundation for implementing effective, adaptive, and sustainable risk mitigation mechanisms.

In conclusion, this study confirms that the complexities of cross-jurisdictional laws related to cybercrime in global supply chains require the implementation of a comprehensive, integrated, and multi-layered mitigation strategy. This strategy includes harmonizing regulations across countries to reduce the potential for legal conflicts while providing legal certainty for companies operating internationally and promoting uniform compliance standards that support the implementation of blockchain technology, particularly private blockchains. Furthermore, international cooperation between regulators, law enforcement authorities, and stakeholders is crucial for accelerating the handling of cyber incidents, exchanging intelligence, and strengthening cross-border law enforcement capacity. Internally, the implementation of robust risk management mechanisms, including data security protocols, regular audits, role-based access controls, and regular employee training, are essential tools for preventing information manipulation, maintaining system integrity, and ensuring product accuracy and traceability throughout the supply chain. This integrative approach not only ensures data security and product traceability but also enhances consumer trust, corporate reputation, and operational credibility globally. Thus, the combination of regulatory harmonization, international coordination, and strengthening internal practices forms a vital strategic foundation for companies to address complex cyber risks, ensure supply chain sustainability, and maintain legal compliance and operational reliability in an increasingly dynamic digital era (Latif et al., 2022).

Regulatory Compliance Evaluation of Private Blockchain

The research findings indicate that while national regulations provide a relatively clear legal framework, rules specifically governing blockchain implementation, particularly private blockchains, remain limited and do not fully reflect the operational complexities of the food industry. This limitation has prompted companies to develop additional standard operating procedures (SOPs) aimed at ensuring compliance with existing regulations while maintaining data security, integrity, and traceability of transactions throughout the supply chain. Furthermore, harmonization with international law remains suboptimal, requiring companies operating across borders to adapt their internal practices to comply with legal requirements in various jurisdictions, including in the context of cyber risk mitigation. These findings align with (Lohmer & Lasch, 2020), who emphasized that blockchain regulations in many countries are still general and do not explicitly address the implementation of this technology in operational practices. Therefore, companies are required to adopt an adaptive and proactive approach by integrating technical mechanisms, internal procedures, and regulatory compliance, ensuring the safe, effective, and reliable implementation of private blockchains, while minimizing the risk of legal violations and maintaining the integrity of the global food supply chain.

The legal gap across jurisdictions is evident in the challenges companies and law enforcement authorities face in coordinating across countries, particularly in addressing data security incidents involving the use of private blockchains in global supply chains. Differing regulations across countries, ranging from data protection standards to applicable legal authorities, create barriers to information exchange, investigation, and enforcement of cyber

breaches. This situation not only slows incident response but also increases legal risks for companies that must comply with multiple legal frameworks simultaneously. This finding aligns with research by Zyskind et al. (2015), which shows that regulatory disharmony across countries can reduce the effectiveness of cyber law enforcement and pose significant challenges for companies operating globally. Therefore, effective mitigation strategies require systematic legal coordination, cross-jurisdictional cooperation mechanisms, and adjustments to internal company practices to align with national and international regulations, to ensure legal compliance while maintaining data security and integrity in global supply chains (Uddin, 2021).

Furthermore, existing regulations emphasize the importance of consumer protection and data privacy, encouraging companies to implement more comprehensive security mechanisms in private blockchain systems, including the use of double encryption and role-based access controls for each user. These measures not only ensure compliance with national and international laws but also maintain the integrity, accuracy, and traceability of transaction data, while increasing consumer confidence in the transparency and security of the food supply chain. This aligns with the findings of Casino et al. (2019), who emphasized that private blockchain implementations require additional security protocols to ensure full compliance with regulatory standards, while minimizing the risk of data breaches and strengthening accountability in global supply chain management. Therefore, a security strategy that combines layered encryption and strict access controls is a crucial element in cyber risk mitigation, as it protects systems from internal and external threats while strengthening companies' ability to respond to evolving regulatory dynamics and compliance demands, thus supporting secure, transparent, and reliable food supply chain operations (França et al., 2020).

Research findings indicate that companies are not only focused on compliance with applicable regulations but are also actively developing internal mechanisms to anticipate cross-jurisdictional legal risks associated with the implementation of private blockchain in global supply chains. Mitigation strategies implemented include regular internal audits to ensure compliance and data integrity, the development of additional standard operating procedures (SOPs) that align operational practices with legal requirements in various jurisdictions, and employee training programs designed to increase awareness and competency in addressing legal and cyber risks. This proactive approach enables companies to maintain smooth, secure and efficient operations while reducing the likelihood of legal violations or errors in data management, despite the continued development of blockchain and cybersecurity regulations at the national and international levels. Furthermore, effective synergy between regulatory compliance, strengthening internal mechanisms, and enhancing human resource capacity not only supports transaction security and traceability but also builds a solid foundation for maintaining the company's reputation and enhancing stakeholder trust. Thus, the implemented risk mitigation strategies are adaptive, comprehensive, and capable of addressing the complexities of cross-jurisdictional law in the context of an increasingly digitalized global food supply chain (Ayub Khan et al., 2022).

In conclusion, the regulatory compliance evaluation demonstrates that maintaining security and traceability in private blockchain implementations is not sufficient by simply complying with existing legal requirements. A combination of regulatory compliance and internal company innovation is required, including the development of additional standard operating procedures (SOPs), regular audits to ensure data integrity and accuracy, strengthening technical security protocols, and employee training programs to enhance preparedness for cyber risks and cross-jurisdictional legal challenges. This comprehensive approach confirms that effective risk mitigation depends on a balanced synergy between

regulations, operational practices, and blockchain security mechanisms, enabling companies to maintain product security, accuracy, transparency, and traceability throughout the global supply chain. Furthermore, these adaptive mitigation mechanisms not only support legal compliance but also strengthen stakeholder trust, enhance company reputation, and ensure the sustainability of the food supply chain in a complex digital era where cyber threats and regulatory differences across jurisdictions pose significant challenges to global operations (Liang et al., 2021).

Technology and Legal Mitigation and Governance Practices

The research findings indicate that the company implemented a comprehensive risk mitigation strategy by combining internal security enhancements, cross-border collaboration, and the implementation of advanced blockchain security protocols to address various cyber threats in the private blockchain ecosystem. Internal security enhancements include systematic routine audits and the implementation of role-based access controls, which have proven effective in mitigating the risk of insider threats while ensuring the accuracy, integrity, and traceability of transaction data. This approach emphasizes that access rights management and internal oversight are not merely administrative procedures but vital components for maintaining the operational stability and reliability of private blockchain systems, aligning with the findings of Xu et al. (2019) who emphasized that internal controls are a key element in risk mitigation and improving operational reliability. Furthermore, cross-border collaboration plays a strategic role in addressing cross-jurisdictional legal challenges, expediting the handling of cyber incidents, and enhancing transparency and traceability in complex global supply chains. Therefore, the company's mitigation strategy reflects the simultaneous integration of technical, regulatory, and human resource aspects, forming a holistic, adaptive, and effective risk management framework in addressing the dynamics of cybersecurity and international law in the digital era (Cerchione et al., 2023).

Cross-border collaboration is a crucial risk mitigation strategy and a key element in managing private blockchains in the complex global food supply chain. Companies are actively collaborating with national regulators, international legal institutions, and cross-jurisdictional authorities to support investigations, expedite information exchange, and coordinate law enforcement in response to cyber incidents. This approach enables companies to respond more quickly to threats, minimize operational impact, and ensure compliance with differing legal frameworks across countries. The findings of this study align with those of Kshetri & Voas (2019), who emphasized that cross-jurisdictional collaboration can strengthen global legal mechanisms, increase transparency and accountability, and close legal loopholes potentially exploited by cybercriminals. Furthermore, this collaboration enables companies to adopt international best practices in internal procedures, establish operational standards that are flexible to regulatory changes, and strengthen data traceability and integrity across the supply chain. Thus, a cross-border collaborative approach not only addresses legal and technical challenges but also serves as a strategic foundation for mitigating cyber risks while strengthening stakeholder trust in the private blockchain ecosystem (He et al., 2021).

The implementation of security protocols in blockchain systems, including the use of securely designed smart contracts and strong data encryption, plays a crucial role in maintaining information integrity and ensuring the traceability of food products throughout the supply chain. These protocols enable companies to accurately record every transaction and product movement, protect it from manipulation, and ensure it can be verified by all relevant stakeholders. These findings align with Saberi et al. (2019), who emphasized that implementing additional security protocols on blockchains is essential for improving operational efficiency and building trust in global supply chains. Furthermore, secure smart

contracts not only automate transaction processes but also reduce the potential for human error, while data encryption safeguards sensitive information from internal and external threats. Therefore, the integration of these technical protocols is a key component of cyber risk mitigation strategies, while strengthening the transparency, accountability, and credibility of companies' operations in the context of an increasingly digitalized food supply chain (Han et al., 2022).

Furthermore, the implementation of a mitigation strategy that combines technological and regulatory aspects forms a comprehensive governance framework for managing private blockchains in the global food supply chain. Within this framework, companies not only rely on technical mechanisms such as smart contracts designed with high security and layered data encryption to maintain transaction integrity and traceability, but also proactively adjust internal operational procedures to align with regulations at both the national and international levels. This holistic approach includes strengthening internal controls through monitoring access rights and regular audits, developing additional standard operating procedures (SOPs) that align with legal requirements in various jurisdictions, and employing training programs to enhance cyber risk preparedness while ensuring compliance with cross-border laws. The research findings confirm that effective risk mitigation cannot be achieved in isolation between technical and regulatory aspects; rather, it requires synergy between technological innovation, internal policies, and legal compliance to ensure data security, transaction accuracy and traceability, and build stakeholder trust. This integrated approach also plays a role in minimizing the potential for operational disruptions or legal violations that could damage the reputation and threaten the sustainability of the food supply chain, emphasizing the importance of adaptive, responsive, and strategic governance in addressing the complexities of cybersecurity and the dynamics of global regulation (Wylde et al., 2022).

In conclusion, risk mitigation in managing cybercrime on private blockchains emphasizes the need for a comprehensive strategy that synergistically integrates technology, regulations, and internal company procedures. From a technological perspective, the company implements security-tested smart contracts, double data encryption, and additional security protocols to ensure the integrity, accuracy, and traceability of every transaction in the global food supply chain. Meanwhile, compliance with national and international regulations is strengthened through the development of internal standard operating procedures (SOPs) tailored to the requirements of different jurisdictions, regular audits to detect potential legal or technical weaknesses, and employee training programs to increase awareness and preparedness for cross-border cyber risks and compliance. This integrated approach enables the company to proactively respond to cyber threats, minimize opportunities for data manipulation, and maintain transparency, accountability, and stakeholder trust throughout the supply chain. Furthermore, the synergy between technological innovation, regulatory compliance, and strengthened internal mechanisms not only builds a strategic foundation for the security and sustainability of the private blockchain ecosystem but also creates an adaptive framework capable of adapting to regulatory dynamics and cyber threats in the digital era, ensuring food supply chain operations remain reliable, legally compliant, and sustainable (Ahl et al., 2020).

Conclusions

This study reveals that the implementation of private blockchain in the global food supply chain offers significant benefits in terms of traceability, transparency, and operational efficiency, but remains vulnerable to complex cybercrime risks, including insider threats, malware attacks, phishing, and system vulnerabilities. From a legal perspective, this study highlights serious challenges in cross-jurisdictional law enforcement, such as the existence of

multiple jurisdictions, differences in national and international regulations, and slow and complex extradition procedures. The strength of this study lies in its in-depth understanding of the interplay between technology, cybersecurity, and cross-jurisdictional law through a concrete case study approach, providing practical insights for companies and regulators. However, limitations include the study's limited scope to a select number of companies and regulators, requiring caution in generalizing the results, and the use of qualitative data that may be influenced by informant perceptions. Implications of this study include the development of integrated risk mitigation strategies, including strengthening internal controls, implementing blockchain security protocols, and effective cross-jurisdictional legal coordination. It can also serve as a basis for developing regulations that are more adaptive to new technologies. Furthermore, this research opens up opportunities for further studies to explore public and hybrid blockchains in other industrial contexts, as well as expanding the analysis related to the harmonization of international law to address cybercrime globally, so that its contribution is not only academic, but also provides practical value in managing a safe, sustainable, and legally compliant food supply chain.

Acknowledgement

The author expresses sincere gratitude to all individuals and institutions who contributed to the completion of this study. Appreciation is extended to legal scholars, blockchain and supply chain practitioners, and industry experts who provided valuable insights related to the use of private blockchain in combating cybercrime within global food supply chains. The author also thanks academic advisors and colleagues for their guidance and constructive feedback. It is hoped that this research contributes to the development of effective cross-jurisdictional legal frameworks in the food industry.

References

Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O.-Y., Bashir, A. K., & El-Latif, A. A. A. (2020). DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. IEEE Access, 8, 111223–111238. https://doi.org/10.1109/ACCESS.2020.2999468

Ahl, A., Yarime, M., Goto, M., Chopra, S. S., Kumar, N. M., Tanaka, K., & Sagawa, D. (2020). Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan. Renewable and Sustainable Energy Reviews, 117, 109488. https://doi.org/10.1016/j.rser.2019.109488

Ali, M., Karimipour, H., & Tariq, M. (2021). Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges. Computers & Security, 108, 102355. https://doi.org/10.1016/j.cose.2021.102355

Ayub Khan, A., Laghari, A. A., Shaikh, Z. A., Dacko-Pikiewicz, Z., & Kot, S. (2022). Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review. IEEE Access, 10, 122679–122695. https://doi.org/10.1109/ACCESS.2022.3223370

Bera, B., Saha, S., Das, A. K., & Vasilakos, A. V. (2021). Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System. IEEE Internet of Things Journal, 8(7), 5744–5761. https://doi.org/10.1109/JIOT.2020.3030308

Cao, B., Wang, X., Zhang, W., Song, H., & Lv, Z. (2020). A Many-Objective Optimization Model of Industrial Internet of Things Based on Private Blockchain. IEEE Network, 34(5), 78–83. https://doi.org/10.1109/MNET.011.1900536

Casino, F., Kanakaris, V., Dasaklis, T. K., Moschuris, S., Stachtiaris, S., Pagoni, M., & Rachaniotis, N. P. (2021). Blockchain-based food supply chain traceability: a case study

in the dairy sector. International Journal of Production Research, 59(19), 5758–5770. https://doi.org/10.1080/00207543.2020.1789238

Centobelli, P., Cerchione, R., Vecchio, P. Del, Oropallo, E., & Secundo, G. (2022). Blockchain technology for bridging trust, traceability and transparency in circular supply chain. Information & Management, 59(7), 103508. https://doi.org/10.1016/j.im.2021.103508

Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., & Oropallo, E. (2023). Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. Technovation, 120, 102480. https://doi.org/10.1016/j.technovation.2022.102480

Chang, Y., Iakovou, E., & Shi, W. (2020). Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities. International Journal of Production Research, 58(7), 2082–2099. https://doi.org/10.1080/00207543.2019.1651946

França, A. S. L., Amato Neto, J., Gonçalves, R. F., & Almeida, C. M. V. B. (2020). Proposing the use of blockchain to improve the solid waste management in small municipalities. Journal of Cleaner Production, 244, 118529. https://doi.org/10.1016/j.jclepro.2019.118529

Garg, N., Wazid, M., Das, A. K., Singh, D. P., Rodrigues, J. J. P. C., & Park, Y. (2020). BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment. IEEE Access, 8, 95956–95977. https://doi.org/10.1109/ACCESS.2020.2995917

Han, D., Zhang, C., Ping, J., & Yan, Z. (2020). Smart contract architecture for decentralized energy trading and management based on blockchains. Energy, 199, 117417. https://doi.org/10.1016/j.energy.2020.117417

Han, D., Zhu, Y., Li, D., Liang, W., Souri, A., & Li, K.-C. (2022). A Blockchain-Based Auditable Access Control System for Private Data in Service-Centric IoT Environments. IEEE Transactions on Industrial Informatics, 18(5), 3530–3540. https://doi.org/10.1109/TII.2021.3114621

He, Y., Wang, Y., Qiu, C., Lin, Q., Li, J., & Ming, Z. (2021). Blockchain-Based Edge Computing Resource Allocation in IoT: A Deep Reinforcement Learning Approach. IEEE Internet of Things Journal, 8(4), 2226–2237. https://doi.org/10.1109/JIOT.2020.3035437

Huang, D., Ma, X., & Zhang, S. (2020). Performance Analysis of the Raft Consensus Algorithm for Private Blockchains. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 172–181. https://doi.org/10.1109/TSMC.2019.2895471

Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic Literature Review of Challenges in Blockchain Scalability. Applied Sciences, 11(20), 9372. https://doi.org/10.3390/app11209372

Latif, S. A., Wen, F. B. X., Iwendi, C., Wang, L. F., Mohsin, S. M., Han, Z., & Band, S. S. (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. Computer Communications, 181, 274–283. https://doi.org/10.1016/j.comcom.2021.09.029

Li, Y., Chen, C., Liu, N., Huang, H., Zheng, Z., & Yan, Q. (2021). A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus. IEEE Network, 35(1), 234–241. https://doi.org/10.1109/MNET.011.2000263

Liang, W., Zhang, D., Lei, X., Tang, M., Li, K.-C., & Zomaya, A. Y. (2021). Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection. IEEE Transactions on Emerging Topics in Computing, 9(3), 1410–1420. https://doi.org/10.1109/TETC.2020.2993032

Lin, C., He, D., Huang, X., Kumar, N., & Choo, K.-K. R. (2021). BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems, 22(12), 7408–7420. https://doi.org/10.1109/TITS.2020.3002096

Lohmer, J., & Lasch, R. (2020). Blockchain in operations management and manufacturing: Potential and barriers. Computers & Industrial Engineering, 149, 106789. https://doi.org/10.1016/j.cie.2020.106789

Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. IEEE Transactions on Industrial Informatics, 16(6), 4177–4186. https://doi.org/10.1109/TII.2019.2942190

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88, 101653. https://doi.org/10.1016/j.cose.2019.101653

Mazlan, A. A., Mohd Daud, S., Mohd Sam, S., Abas, H., Abdul Rasid, S. Z., & Yusof, M. F. (2020). Scalability Challenges in Healthcare Blockchain System—A Systematic Review. IEEE Access, 8, 23663–23673. https://doi.org/10.1109/ACCESS.2020.2969230

Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. ICT Express, 7(2), 229–233. https://doi.org/10.1016/j.icte.2020.09.002

Rahman, M. A., Hossain, M. S., Islam, M. S., Alrajeh, N. A., & Muhammad, G. (2020). Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. IEEE Access, 8, 205071–205087. https://doi.org/10.1109/ACCESS.2020.3037474

Raja Santhi, A., & Muthuswamy, P. (2022). Influence of Blockchain Technology in Manufacturing Supply Chain and Logistics. Logistics, 6(1), 15. https://doi.org/10.3390/logistics6010015

Ramanan, P., & Nakayama, K. (2020). BAFFLE : Blockchain Based Aggregator Free Federated Learning. 2020 IEEE International Conference on Blockchain (Blockchain), 72–81. https://doi.org/10.1109/Blockchain50366.2020.00017

Shamshad, S., Minahil, Mahmood, K., Kumari, S., & Chen, C.-M. (2020). A secure blockchain-based e-health records storage and sharing scheme. Journal of Information Security and Applications, 55, 102590. https://doi.org/10.1016/j.jisa.2020.102590

Shayan, M., Fung, C., Yoon, C. J. M., & Beschastnikh, I. (2021). Biscotti: A Blockchain System for Private and Secure Federated Learning. IEEE Transactions on Parallel and Distributed Systems, 32(7), 1513–1525. https://doi.org/10.1109/TPDS.2020.3044223

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A Survey on Zero-Knowledge Proof in Blockchain. IEEE Network, 35(4), 198–205. https://doi.org/10.1109/MNET.011.2000473

Toufaily, E., Zalan, T., & Dhaou, S. Ben. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. Information & Management, 58(3), 103444. https://doi.org/10.1016/j.im.2021.103444

Uddin, M. (2021). Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. International Journal of Pharmaceutics, 597, 120235. https://doi.org/10.1016/j.ijpharm.2021.120235

Ul Hassan, M., Rehmani, M. H., & Chen, J. (2019). DEAL: Differentially Private Auction for Blockchain based Microgrids Energy Trading. IEEE Transactions on Services Computing, 1–1. https://doi.org/10.1109/TSC.2019.2947471

Wang, Y., Su, Z., Zhang, N., Chen, J., Sun, X., Ye, Z., & Zhou, Z. (2021). SPDS: A Secure and Auditable Private Data Sharing Scheme for Smart Grid Based on Blockchain. IEEE

Transactions on Industrial Informatics, 17(11), 7688–7699. https://doi.org/10.1109/TII.2020.3040171

Wenhua, Z., Qamar, F., Abdali, T.-A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. Electronics, 12(3), 546. https://doi.org/10.3390/electronics12030546

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. SN Computer Science, 3(2), 127. https://doi.org/10.1007/s42979-022-01020-4

Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., Yang, X., Amarasinghe, G., & Chen, S. (2020). Public and private blockchain in construction business process and information integration. Automation in Construction, 118, 103276. https://doi.org/10.1016/j.autcon.2020.103276

Yang, X., Li, M., Yu, H., Wang, M., Xu, D., & Sun, C. (2021). A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products. IEEE Access, 9, 36282–36293. https://doi.org/10.1109/ACCESS.2021.3062845

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Zhang, Q., & Choo, K.-K. R. (2020). An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security. IEEE Transactions on Services Computing, 13(4), 625–638. https://doi.org/10.1109/TSC.2020.2966970

Yu, K., Tan, L., Aloqaily, M., Yang, H., & Jararweh, Y. (2021). Blockchain-Enhanced Data Sharing With Traceable and Direct Revocation in IIoT. IEEE Transactions on Industrial Informatics, 17(11), 7669–7678. https://doi.org/10.1109/TII.2021.3049141