A Systematic Literature Review of Blockchain Interoperability Analysis for Authorized Economic Operator (AEO) System

Article history

Received:
4 May 2025

Received in revised form:
10 May 2025

Accepted:
20 May 2025

Published online:
27 June 2025

*Corresponding author
izdihar.sahalan@mimos.my

Muhammad Izdihar Sahalan[1], Mohd Nazri Mohd Warip[2], Normaizeerah Mohd Noor[3]

Business Management & Subsidiary Monitoring, MIMOS Berhad
Wilayah Persekutuan Kuala Lumpur, Malaysia

[1]*izdihar.sahalan@mimos.my*, [2]*nazri.warip@mimos.my*, [3]*normaizeerah.mohd@mimos.my*

Abstract

The Authorized Economic Operator (AEO) system plays a vital role in global trade by ensuring secure and efficient supply chain operations. Blockchain technology offers transformative potential for AEO systems by enhancing transparency, traceability, and operational efficiency. This study employs a systematic literature review (SLR) methodology to analyse blockchain applications in AEO systems, focusing on standardisation challenges such as interoperability, regulatory compliance, and integration. A total of 222 studies were initially identified, with 53 passing the screening process. After further analysis, 23 studies were selected for final evaluation based on relevance and quality criteria. Findings indicate that blockchain facilitates the mutual recognition of AEO certifications, simplifies customs clearance processes, and improves data security. However, standardisation gaps, scalability limitations, and data privacy concerns persist. Recommendations include developing standardised interoperability frameworks, integrating blockchain with existing AEO processes, and adopting cost-efficient, scalable blockchain models. This review offers researchers, policymakers, and practitioners actionable insights to advance blockchain-enabled AEO systems.

Keywords: Blockchain, Authorized Economic Operator, Interoperability, Supply Chain Security, Trade Facilitation, Systematic Literature Review, Standardisation Challenges

1. Introduction

The Authorized Economic Operator (AEO) system ensures security, efficiency, and trust among trade stakeholders in an increasingly complex global supply chain era. As international trade faces challenges like regulatory misalignment, fraud, and inefficiencies, the need for transformative technologies has never been greater. Digital ledger stores transactions in blocks linked in a chronological chain within the blockchain environment. Each block contains a cryptographic hash of the previous block and timestamped transaction data distributed across a network of nodes. The decentralised nature of blockchain ensures that no single entity controls the technology, giving the technology autonomy to enhance transparency and reduce fraud or manipulation [1]. Blockchain technology revolutionises various

**Corresponding author izdihar.sahalan@mimos.my*
DOI: 10.11113/oiji2025.13n1.323

industries by enabling secure, transparent, and decentralised digital transactions [2]. With its inherent transparency, traceability, and decentralisation features, blockchain technology offers a unique opportunity to revolutionise AEO systems. Blockchain addresses long-standing inefficiencies in customs processes and compliance mechanisms by providing tamper-proof records and real-time data sharing.

Despite its potential, blockchain integration with AEO systems is hindered by significant challenges, including platform interoperability, a lack of standardisation, and data privacy and scalability concerns. These barriers have limited the widespread adoption of blockchain, creating a pressing need for focused research to address these gaps. This study systematically reviews the applications and challenges of blockchain in AEO systems, focusing on interoperability, regulatory alignment, and integration with legacy processes. Using a systematic literature review (SLR) methodology, the research identifies key issues, highlights successful use cases, and provides actionable recommendations for advancing blockchain-enabled AEO systems.

The remainder of this paper is organised as follows: Section 2 reviews related works, providing an overview of blockchain applications in AEO systems. Section 3 details the methodology of the SLR process. Section 4 discusses the findings, including key use cases and challenges. Finally, Section 5 offers recommendations and outlines future research directions.

2. Related Works

Beyond cryptocurrency functions, blockchain technology is being explored and implemented across various industries, such as supply chain management. These businesses leverage blockchain accountability to streamline operations, reduce costs, and improve efficiency. The technology's ability to provide secure and verifiable records has applications in supply chain traceability, digital identity management, and smart contracts [3]. There is a potential demand for interoperability between blockchain platforms, especially in AEO for the supply chain system.

2.1 Overview of Blockchain Interoperability

Blockchain technology has demonstrated transformative potential across industries, including supply chain management, healthcare, and financial services. Features like immutability and decentralisation make blockchain particularly suited for enhancing transparency and trust in multi-stakeholder ecosystems. Standards like ISO/TR 23455:2019 ensure interoperability and compliance in blockchain systems, which are critical for AEO applications.

As technology rapidly grows, ISO/TR 23455:2019 standardisation for smart contracts facilitates interactions and transactions between integrated blockchain systems and ensures they comply with security and operational guidelines. These also provide the interoperability of a seamless process for automation transactions, ensuring efficiency and reducing manual intervention.

A project hosted by the Linux Foundation created an open-source innovation project called Hyperledger [2]. The Hyperledger project, one of the prominent projects called Hyperledger Fabric, provides a more specific viewpoint on blockchain technology tailored for enterprise use cases.

Ethereum allows developers to build and deploy decentralised applications (dApps) by executing smart contracts on a decentralised platform. The Ethereum Virtual Machine (EVM) function allows developers to process and verify transactions across multiple nodes securely, and its flexibility for coding complex applications makes it a cornerstone of the Ethereum ecosystem.

Based on the ISO T/R 3242, the most applied blockchain platforms are Hyperledger and Ethereum. Ethereum is the highest use case, accounting for 31.8 % of blockchain implementation platforms [4]. Second is the Hyperledger private blockchain, which accounts for 27.3%. The Ethereum platform is divided into public, hybrid, and private blockchains, which account for 13.6%, 9.1%, and 9.1%, respectively. These two blockchains, Ethereum and Hyperledger, became the highest example platforms among other blockchains internationally [4].

All blockchain platforms have diverse applications. Hence, developing interoperability standards between two prominent blockchain platforms, Hyperledger Fabric and Ethereum, ensures seamless inter-blockchain platform demand. The research approach helps enable the broader adoption of blockchain solutions for future use cases and prevents business fragmentation.

3. Blockchain in Supply Chain Management

Blockchain's application in supply chain management has focused on addressing fraud, inefficiencies, and a lack of transparency. For instance, the Fast Corridor system [5] leverages blockchain to streamline customs clearance, reducing delays and costs in international logistics. Similarly, smart contracts automate stakeholder interactions, enhancing efficiency and trust in supply chain networks.

Blockchain demonstrates the potential to revolutionise AEO systems by improving transparency, efficiency, and collaboration in supply chain management. For example, the CADENA project [6] employs blockchain to facilitate mutual recognition of AEO certifications, enabling real-time data sharing and reducing compliance burdens across jurisdictions.

Despite its potential, blockchain adoption in AEO systems faces significant challenges, particularly interoperability. Studies highlight the difficulty of integrating blockchain with legacy systems and ensuring seamless data exchange between diverse platforms.

A study shows that privacy and regulatory concerns remain critical barriers to blockchain adoption, even in data sharing [7]. Studies emphasise the need for advanced encryption techniques and regulatory alignment to balance transparency with data protection in AEO systems.

While previous studies have explored blockchain's potential in supply chains and customs, limited attention has been given to interoperability challenges and blockchain integration into AEO-specific frameworks. This study addresses these gaps by systematically reviewing relevant literature and providing actionable recommendations.

4. Methodology

This study searched the literature and identified several challenges to blockchain interoperability, including a lack of standardisation and complexity in integration processes. Data collection aims to identify issues relating to blockchain technology and medical data. This section uses a Systematic Literature Review (SLR) [8]. The SLR method offers insight into the related research issues that enable the information for further research on the selected topics [8]. In addition, SLR results are more reliable and likely to be unbiased than unstructured methods such as the simple literature review [8]. The SLR process consists of eight distinct phases, as illustrated in Figure 1.

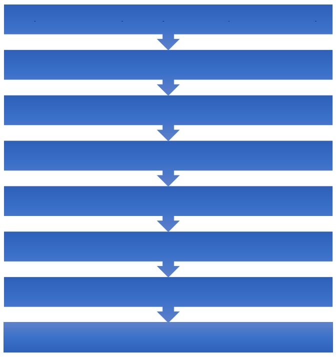

Figure 1 SLR Phase

This review process includes eight phases: (1) Planning and Protocol, (2) Literature Search, (3) Initial Screening, (4) Data Extraction, (5) Quality Assessment, (6) Final Screening, (7) Data Synthesis, (8) Reporting. The phases collect various aspects to understand the interoperability analysis between blockchain applications for AEO systems.

Phase (1) shall define the research questions to address the specific topics. The first research question was crucial to understanding the current challenges for blockchain applications in AEO systems: What are the potential issues for blockchain applications in AEO systems?

Phase (2) is to develop a protocol for a search strategy on each source. The keywords "blockchain" and “AEO systems” and “Standardisation challenges” were selected based on the appropriate research keywords for the study objective. In this study, synonymous keywords for “Authorized Economic Operator” such as “Customs Security Program”, “Trade Facilitation Programs”, “Customs Trade Partnership”, “Supply Chain Security Programs”, “Customs Compliance Programs”, “Global Trade Compliance”, “AEO Certification”, “Customs Risk Management”, “International Supply Chain Security”, “AEO Mutual Recognition Agreements”, “Secure Trade Partnership”, “Trusted Trader Programs”, “Authorized Operator Programs”, “Customs and Border Security Initiatives” were identified.

Phase (3) is to conduct the literature search using the proposed protocol that has been developed. The search is performed manually using various databases, which have been collected from 222 articles on blockchains for AEO system Primary Databases (IEEE, ACM Digital Library, Scopus, Web of Science), Supplementary

Databases (Google Scholar, Google Patent, ScienceDirect, SpringerLink, ProQuest), and Specialized Databases (Emerald, TRB, EBSCOHost).

Phase (4) screens and selects related studies that address the topic of interest. After reading the abstract and title of the papers, the initial screening is done. During the screening process, duplicate records identified across databases were removed using Mendeley and manual verification. This ensured that each study was considered only once during the abstract and full-text screening phases. 46 selected studies are summarised and reviewed using qualitative assessment.

For challenges and negative findings, Phase (5) performed data extraction and mapping of the results from the literature search. Each study was assessed against 10 predefined quality criteria (Q1–Q10), covering aspects such as clarity of objectives, methodological rigour, relevance, depth of analysis, and reporting challenges or limitations. A scoring system was applied: Yes = 1, Partially = 0.5, No = 0.

Phase (6) synthesised the initial data. Each of the 46 initially selected studies was evaluated against a predefined set of quality criteria to ensure methodological rigour and relevance to the research questions. Studies that scored below 6/10 (60%) were excluded from the final synthesis.

Phase (7) reported the final data results synthesised. However, some selected studies are excluded based on the results of the criteria for finding negative issues and challenges in blockchain applications for AEO systems. These exclusions are either the topic not directly addressed on blockchain applications or the studies not discussing negative findings of the study, resulting in a total of 23 studies analysing the findings included in the final assessment.

The revised quality assessment was included in Table 1, and Table 2 shows the questions used for review. Overall, the highest-rated study was [14], which achieved a perfect 10 (100%) score, demonstrating full alignment with all assessment criteria. In contrast, the lowest-scoring study was [12], with a total score of 6.5 (65%), primarily due to a partial score on technical aspects coverage.

Table 1 Quality Assessment

Ref	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Total (10)	% Max S
[5]	1	1	1	0.5	1	1	1	1	1	1	9.5	95%
[6]	1	1	1	0.5	0.5	1	0.5	1	1	1	8.5	85%
[9]	1	1	1	0.5	1	1	1	1	1	1	9.5	95%
[10]	1	1	1	0.5	0.5	1	1	1	1	1	9	90%
[11]	1	1	1	0.5	1	1	1	1	1	1	9.5	95%
[12]	1	0.5	0.5	0.5	0.5	0.5	0.5	1	1	0.5	6.5	65%
[13]	1	1	1	0.5	0.5	1	1	1	1	1	9	90%
[14]	1	1	1	1	1	1	1	1	1	1	10	100%
[15]	1	1	0	0.5	0.5	1	1	1	1	1	8	80%
[16]	1	1	0.5	0.5	1	1	1	1	1	1	9	90%
[17]	1	0.5	0.5	0.5	0.5	1	0.5	1	1	0.5	7	70%
[18]	1	0.5	1	0.5	0.5	0.5	0.5	1	1	0.5	7	70%
[19]	1	1	0.5	0.5	0.5	0.5	0.5	1	1	1	7.5	75%
[20]	1	1	0.5	0.5	1	1	1	1	1	1	9	90%
[21]	1	1	1	0.5	1	1	1	0	1	0.5	8	80%
[22]	1	1	0.5	0.5	0.5	1	0.5	1	1	0.5	7.5	75%
[23]	1	1	1	0.5	1	1	1	1	1	1	9.5	95%
[24]	1	1	0.5	0.5	0.5	0.5	0.5	1	1	0.5	7	70%
[25]	1	1	0.5	0.5	1	1	0.5	1	1	0.5	8	80%

[26]	1	1	1	0.5	0.5	1	0.5	1	1	1	8.5	85%
[27]	1	0.5	0.5	0.5	1	1	1	1	1	0.5	8	80%
[28]	1	1	0.5	0.5	0.5	0	0.5	1	1	1	7	70%
[29]	1	1	1	0.5	1	0.5	0.5	1	1	1	8.5	85%

Table 2 Questions and score

No.	Question	Answer
Q1	Are the study objectives clearly defined?	Yes/No/Partially
Q2	Is the article's chosen research design suitable for addressing the complexities and technical aspects?	Yes/No/Partially
Q3	Does the research adequately describe the operational and regulatory contexts?	Yes/No/Partially
Q4	Are there specific ethical issues addressed within the study?	Yes/No/Partially
Q5	Are the methods used for collecting data robust and appropriate for capturing detailed insights?	Yes/No/Partially
Q6	Does the study thoroughly explore and demonstrate the analysis?	Yes/No/Partially
Q7	Does the study provide credible interpretations for validation?	Yes/No/Partially
Q8	Does the study discuss any negative findings or potential drawbacks?	Yes/No/Partially
Q9	Do the results provide new insights or extend existing knowledge?	Yes/No/Partially
Q10	Does the study propose actionable strategies or policy recommendations?	Yes/No/Partially

5. Results and Discussion

In extracting related articles, keywords were identified based on specific terms such as “Blockchain” and “Authorized Economic Operator” and “Standardisation challenges”. The total number of articles searched resulted in 222 articles being screened at the first exclusion. However, these outcome articles show that essential information on blockchain applications related to the AEO system is still unidentifiable. The screening process involved reviewing the titles and abstracts to determine relevance to the study topic. After applying the screening process, 46 selected studies were summarised and reviewed with a critical assessment to evaluate the issues of blockchain implementation for the AEO system. The selected studies are based on the exclusion criteria based on the results of issues addressed in blockchain applications. These exclusions are either the topic not directly addressed in blockchain applications or the studies that do not discuss negative findings. As a result, a total of 23 studies analysing the findings included in the final assessment as shown in Table 3.

Table 3 Selected Studies

Study ref	Title
[5]	Fast Corridors: Innovative customs processes and technology to increase supply chain competitiveness. The case of IKEA Italy
[6]	Blockchain in international e-government processes: Opportunities for recognition of foreign qualifications
[9]	Managing food security using a blockchain-enabled traceability system
[10]	Blockchain Revolution: A New Horizon for Supply Chain Management in Hotel Industry
[11]	Examining the Factors That Facilitate or Hinder the Use of Blockchain Technology to Enhance the Resilience of Supply Chains
[12]	Blockchain and its Integration with IoT Security
[13]	RMF-GPT — OpenAI GPT-3.5 LLM, Blockchain, NFT, Model Cards and OpenScap Enabled Intelligent RMF Automation System

[14]	Securing Supply Chain - Blockchain: Leveraging ICC for Product Verification and Validation
[15]	Designing an integrated blockchain-enabled supply chain network under uncertainty
[16]	Application of blockchain in enterprise financing: literature review and knowledge framework
[17]	Green Supply Chains and Digital Supply Chains: Identifying Overlapping Areas
[18]	A Distributed Ledger-Based Automated Marketplace for the Decentralized Trading of Renewable Energy in Smart Grids
[19]	Practice of Trade Facilitation in China Free Trade Zone and Its Enlightenment to Heilongjiang Free Trade Zone: Basic Principal Component Analysis Method
[20]	An ISM Modelling of Success Factors for Blockchain Adoption in a Cyber Secure Supply Chain
[21]	Blockchain technology in the energy sector: From basic research to real-world applications
[22]	Blockchain for electronic voting system—review and open research challenges
[23]	Establishing a security control framework for blockchain technology
[24]	Blockchain: a brief review of Agri-Food Supply Chain Solutions and Opportunities
[25]	Blockchain Technology Open Problems and Impact on Supply Chain Management in the Automotive Component Industry
[26]	Enhancing E-Commerce through Blockchain (DLTs): The Regulatory Paradox for Digital Governance
[27]	Blockchain and supply chain management integration: A systematic review of the literature
[28]	Comparing blockchain standards and recommendations
[29]	Roadmap for National Adoption of Blockchain Technology Towards Securing the Food System of Qatar

Table 4 shows the study's exclusion and the reason for exclusion. The findings are to find all the blockchain issues and challenges that address the same theme of complexity and standardisation for blockchain interoperability, which requires a holistic, integrated framework to facilitate the future AEO system.

Table 4 Excluded Studies

Study ref	Reason
[30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49]	The study has not shown challenges and negative findings related to blockchain applications.
[50], [51]	The study has not shown relevance to blockchain applications.

As a result, standardisation and complexity themes are labelled as the main issues for blockchain interoperability for AEO systems. Table 5 shows the data synthesis from selected studies with more explanation on each topic addressed.

Table 5 Studies Category with Issue

Theme	Challenges
Standardisation	
- Privacy	[5], [9], [22], [28], [29]
- Regulatory Compliance	[6], [9], [11], [12], [17], [19], [20], [21], [23], [27], [28], [29]
- Education	[6], [9], [22], [29]
- System adoption	[5], [9], [11], [14], [23], [24], [25]
Complexity	
- Financial	[6], [10], [11], [14], [15], [18], [20], [29]
- Security	[10], [16], [22], [27], [29]
- Scalability	[5], [6], [11]

5.1 Standardisation challenges

a. Education

The perception of data exposure raised by [29] shows a fear of using blockchain applications. The blockchain does not inherently expose data due to its encryption, pseudonymity, and access control; however, the poor design of smart contracts, storing data directly on the blockchain, and weak access control implementation in private blockchains may allow unauthorised access. Therefore, addressing these concerns requires increased knowledge of robust privacy mechanisms, encryption, and careful system design.

Other perceptions of institutional inertia create resistance to change in individuals', organisations', or systems' ways of working [6]. The fear of the unknown about how the blockchain works impacts the stakeholders. Since people and organisations are familiar with the status quo, they prefer to stay even if they have inefficient roles and processes. The institutional inertia mentioned [6], [22] is deeply ingrained in bureaucratic and larger entities that may slow the adoption and resist disruption due to uncertainty.

Therefore, addressing a strategic approach prioritises clear communication to highlight the benefits of change in blockchain applications, active engagement with stakeholders and targeted training programs to build necessary skills and confidence. Structurally implementing changes with incrementally phased approaches paves the way for trust and smoother transitions on blockchain applications [6], [22], [29].

b. **Privacy**

The study [29] points out the reluctance to join blockchain decentralised networks due to the transparency of the blockchain solutions. Some organisations may be hesitant to join blockchain networks due to concerns about resource availability and the desire to maintain privacy over certain information. This reluctance could result in incomplete data sharing and reduced transparency across the supply chain, undermining the effectiveness of blockchain technology.

Although not extensively discussed, the study [9] implicitly recognises the importance of data privacy in implementing blockchain technology. It suggests that policy recommendations should include guidelines for protecting sensitive information, ensuring the system improves transparency and safeguarding all participants' privacy.

The study [5] raises concerns about public information and data within the AEO system, often held by private entities rather than customs and port authorities. This could lead to fears of data control, security, and potential interruptions in the flow of information.

Another issue related to privacy is the voting identification [22]. The study [22] discusses the challenges of maintaining voter privacy while ensuring transparency in the voting process. While blockchain provides transparency, it cannot be easy to balance this with the need for privacy, as all transactions on a public blockchain are visible to everyone. This creates a potential drawback, as inadequate privacy protections could lead to voter identification, undermining the secrecy of the ballot.

Lastly, privacy concerns must be addressed to meet the requirements of existing laws [28]. The study [28] mentions the difficulties in aligning blockchain technology with existing regulations, such as the GDPR, which could pose challenges for implementation.

c. **System Adoption**

Existing systems may differ from the blockchain system due to the nature of compatibility. The study [14] shows incompatibility with legacy systems. Many businesses, especially those with established supply chain operations, rely on legacy systems that may not be compatible with blockchain technology or QR code implementations. Integrating blockchain with these existing systems often requires significant effort, including custom middleware, which increases the complexity and cost of adoption. The study [5] also concerns legacy systems: Many customs and logistics operations still rely on legacy systems that may not easily integrate with blockchain technology [5].

Developing middleware or APIs to connect these systems to a blockchain can be technically challenging, leading to potential inefficiencies [11]. Another study [25] Integrating blockchain into the AEO system presents challenges due to legacy systems and diverse stakeholders. However, smart contracts can simplify the process by automating interactions and enabling seamless communication.

Supporting study [5] Data Exchange: Blockchain technology may not always be compatible with existing systems' data formats and communication protocols. Without proper standardisation, blockchain might not work harmoniously with other digital systems, causing delays in data flow or errors in processing.

The study [14] challenges diverse blockchain platforms that may have different standards. Different blockchain platforms like Hyperledger Fabric, Ethereum, and others use varying consensus mechanisms, data structures, and protocols. These differences can create difficulties when businesses integrate multiple platforms within a single supply chain system [14]. Ensuring these platforms can communicate and share data seamlessly becomes a significant challenge without standardisation.

The study [23] mentioned cross-chain interoperability, smart contracts interoperability, and the establishment of secure communication protocols between different blockchain platforms. The study [23] discusses the challenges associated with the lack of standardisation in blockchain technology, particularly regarding interoperability between different blockchain platforms. These challenges [23] are significant drawbacks because they complicate implementing secure, interoperable blockchain systems.

The study [24] highlights challenges related to the interoperability of blockchain systems. Since there is no single standard for blockchain implementation, integrating different blockchain platforms or integrating blockchain with existing systems can be complex and problematic. This fragmentation can hinder the seamless operation of supply chains that rely on multiple systems [24]. By discussing the integration of blockchain with IoT devices and using specific blockchain platforms like Hyperledger, the study indirectly suggests strategies for implementing blockchain in the supply chain. However, these are not formalised as explicit, step-by-step strategy.

An example study [9] proposed a comprehensive framework that includes a delivery system, an enabling system, and a criteria system for achieving food security for India's Public Distribution System (PDS). This framework is designed to guide the implementation of the blockchain-enabled traceability system and other innovations. It outlines the roles and responsibilities of various stakeholders and provides a roadmap for ensuring that the proposed changes are effectively integrated into the existing system. Develop middleware and APIs to integrate blockchain with existing supply chain management systems. To minimise disruptions, this should be accompanied by thorough testing and phased implementation [11].

d. **Regulatory Compliance**

Blockchain technology has not yet fully matured in terms of governance. There are concerns selected that lead to legal and regulatory challenges, such as cross countries' regulations, insufficient privacy law, the company certification process for blockchain adoption, insufficient law for privacy, security, and smart contract codifiability (the ability of smart contracts to incorporate all necessary nuances)

i. Smart Contract Codifiability

The study [29] points out that blockchain technology has not yet fully matured in terms of governance aspects, such as modifiability (the ability of smart contracts to incorporate all necessary nuances). This immaturity can lead to legal and operational challenges, reducing trust in the technology.

The study [19] ensures that the company understands the smart contract requirements and can handle digital assets and smart contracts with established frameworks and protocols, such as platforms like Hyperledger Fabric or Ethereum.

ii. Insufficient security standards

The study [23] highlights that existing international and national information security standards, such as ISO 27001, do not fully cover the specific security risks associated with blockchain technology. This gap necessitates the development of additional security controls, which the study proposes. However, the need for these additional controls indicates that current standards are insufficient, a drawback in the broader context of blockchain security.

While the study [23] proposes new security controls to mitigate blockchain-specific risks, it stresses the importance of not over-relying on blockchain's inherent security features, as significant risks still need to be managed proactively.

iii. Insufficient privacy regulatory

Often, devices involve sending data to central servers, which can compromise user privacy. Even with blockchain integration, ensuring complete privacy is challenging, as all transactions are recorded on a distributed ledger. The study [12] points out that the transparency inherent in blockchain could lead to privacy concerns if sensitive data is not adequately protected, creating ethical and regulatory challenges.

The study [28] points out insufficient data privacy regulations like the GDPR. Blockchain's immutability conflicts with GDPR requirements, such as the right to be forgotten. These challenges in handling personal data in a decentralised and immutable system are also the difficulties in identifying legal responsibility for data protection in decentralised blockchain networks.

iv. Cross-Country Regulations

The study [6] acknowledges that different countries have legal frameworks and administrative practices, which can challenge standardising recognition processes.

Also, the study [28] mentions that cross-country data flow challenges arise when blockchain networks span multiple jurisdictions with different legal requirements.

The study [6] discusses the importance of harmonising regulations and developing collaborative frameworks to enable seamless cross-border recognition of qualifications. To improve efficiency in global supply chains, collaborate with international trade bodies to establish standardised cross-border blockchain protocols and promote their adoption in customs and trade facilitation [11].

v. Insufficient regulations and standards

The issue reflects the current state, in which comprehensive, universally accepted regulatory frameworks for blockchain are either incomplete or non-existent in many regions or industries. This lack of regulations creates uncertainty for businesses and hinders widespread adoption.

The study [28] mentions that a lack of clear legal definitions for blockchain terms and functions complicates regulatory compliance. The absence of universally accepted standards creates uncertainty about what regulatory frameworks blockchain technologies should follow.

The study [27] identified the lack of regulatory frameworks as a significant challenge for blockchain adoption. By identifying this gap, the research brings attention to the need for regulatory development, which is a crucial first step for action.

The study [17] emphasises the lack of alignment between blockchain technology and environmental goals, indirectly touching on the challenge of technological standardisation and the need for clear regulatory frameworks to guide blockchain adoption in sustainable practices

vi. Policy Reforms

The study [9] emphasises the need for policy reforms to support adopting blockchain technology in governance systems. Clear policies and regulations governing blockchain use in public systems are often missing. Governments must create frameworks for data ownership, privacy, and accountability. The study [27] implies that establishing clear and comprehensive regulations is critical for enabling blockchain adoption, fostering innovation, and addressing stakeholder concerns regarding security, privacy, and operational integrity.

The study's research agenda includes exploring governance disruption caused by blockchain adoption. This could provide insights into how regulations can be shaped to facilitate innovation while addressing legal and operational concerns [27].

Some countries and institutions show limited collaboration in blockchain research, hindering the sharing of knowledge and best practices [21]. Engage with policymakers to draft blockchain-encouraging regulations that ensure data protection and privacy compliance while offering financial incentives, such as tax benefits or grants, for organisations adopting the technology [11]. Promote investment in blockchain applications in underrepresented regions through international collaborations, grants, and public-private partnerships. This can help bridge the gap between research and implementation [21].

vii. Company certification for blockchain adoption

The study [19] mentions a concept requiring companies to prepare and align with the blockchain ecosystem the certification of company capability and preparation for AEO blockchain adoption. The preparation shall include verification of identity and credentials, proof of adherence to transparency and traceability practices, and demonstration of IT capabilities and cybersecurity compliance.

Also, companies' capability to manage blockchain systems requires securely handling digital documentation, deploying and managing smart contracts for automation, and ensuring compliance with blockchain governance rules [19].

Companies must have the technical infrastructure to interface successfully with blockchain systems, understand smart contract requirements, and adhere to the blockchain network's technical and operational guidelines [19].

Blockchain adoption requires companies to collaborate with stakeholders such as customs authorities, banks, logistics providers, and regulatory bodies, ensuring they align internal systems with blockchain processes, securely share data within interoperable networks, and meet ethical and legal standards for ecosystem participation [19].

viii. Environmental Impact

The study [5] imposes a blockchain environmental impact that poses regulatory challenges for blockchain adoption arising from the need to balance technological innovation with sustainability goals.

The study [17] acknowledges the significant energy consumption of blockchain technology, especially Proof-of-Work (PoW) systems, and highlights how this energy demand creates environmental concerns. This directly aligns with the challenge of meeting energy efficiency standards.

The environmental burden caused by blockchain's high energy usage is a potential drawback that could counteract its benefits in green supply chains. This reflects concerns about carbon emissions regulations and the need to align with international climate goals like the Paris Agreement [17].

The study [17] discusses how operational trade-offs, such as energy consumption required for data storage and blockchain validation, may diminish the environmental benefits of blockchain adoption. This resonates with challenges like sustainability vs. functionality in blockchain implementation.

5.2 Complexity challenges

a. Financial

Studies [11], [14], [15], [20], [29] mentioned that organisations with insufficient budgets, especially small and medium-sized enterprises (SMEs) and low-margin industries, often lack the necessary budget to implement and maintain blockchain systems. This financial limitation can impede the adoption of the technology. It emphasises the need for a win-win situation where costs and benefits are shared fairly across the supply chain. Supply chain managers are encouraged to collaborate with partners and stakeholders to share the benefits of blockchain adoption, making the technology more cost-effective and scalable.

Studies [6], [10], [11], [12], [20], [29] discuss the cost of technical expertise. The specialised skills required to implement and maintain blockchain systems add to the overall cost. Hiring or training personnel with expertise in blockchain technology can be costly, especially for smaller organisations that may struggle to afford the necessary talent [20]. The study [10] points out that the initial setup and ongoing maintenance of a blockchain-based system require significant resources, both in terms of technology and skilled personnel. This resource intensity may limit the accessibility of blockchain solutions for smaller companies or those with limited budgets [10], [12].

Studies [6], [11], [18], [20] mention that the investment requirement for blockchain infrastructure, including hardware, software, and network infrastructure, can be substantial. Organisations may find it challenging to allocate funds for these resources compared to their existing systems [20]. Although the system [18] is designed to integrate with existing grid infrastructure, some upfront investment in compatible sensors, communication devices, or nodes may still be required. This could pose a barrier, especially in regions where utilities or governments are unwilling or unable to invest [18]. The study [6] recommends that governments invest in capacity building and technological infrastructure to support the adoption of blockchain, including training personnel, developing the necessary technical expertise, and ensuring that the infrastructure is in place to support blockchain applications. The study [11] suggested financial assistance to SMEs to help them adopt blockchain technology with low-interest loans and low individual costs.

b. **Scalability**

Studies [5], [11], [13] faces a high volume of transactions, and blockchain networks may struggle to handle large transactions efficiently. In the AEO system, customs, and logistics processes, thousands of data points are often processed simultaneously (e.g., shipment tracking and customs documentation). If the blockchain network cannot scale efficiently, it may lead to delays or bottlenecks. The performance evaluation highlights issues with block generation time, which increases as the number of blockchain peers grows [13].

The study [6] recommends a private blockchain optimised for specific use cases and offers better performance and scalability for the administrative processes involved in recognition procedures. The study [13] proposes innovative and actionable solutions that leverage a mix of blockchain, AI, and compliance management tools to automate and enhance the Risk Management Framework (RMF) process that is designed to address the complexities and challenges of traditional RMF implementation, offering a scalable, transparent, and efficient alternative.

The study [11] proposes exploration for research and development efforts focused on developing scalable blockchain models that can handle large transaction volumes. In contrast, exploring hybrid blockchain solutions that combine the benefits of public and private blockchains for better efficiency [11].

c. **Security**

While blockchain technology is praised for its enhanced security features, concerns include selfish mining, 51% majority attacks, smart contract vulnerability, denial-of-service (DoS), complexity of access control and insufficient security standards.

i. Selfish mining

The study [29] concerns the risk of selfish mining, which seriously threatens blockchain networks, especially those using Proof of Work (PoW) as their consensus mechanism. The challenge behaviour is where the fairness of rewards is manipulated, increasing double-spending risk and collusion among large mining entities. Addressing this issue requires technical protocol adjustments and ongoing research into robust consensus mechanisms.

ii. Access control on data privacy

Studies [9], [10], [27], [29] mention that policy recommendations should include guidelines for access control to protect sensitive information. While a decentralised blockchain system accessible to multiple parties offers benefits like transparency, traceability, and immutability, it also introduces challenges that need careful planning and mitigation [10]. By addressing concerns about privacy, security, governance, and operational efficiency, organisations can maximise the advantages of blockchain while minimising its risks [10].

iii. Smart contract

The study [27] concerns a vulnerability in smart contracts, which could potentially compromise data privacy involving sensitive information. The studies [16] also concern the potential for security breaches in smart contracts, which automate transactions by being susceptible to programming errors or bugs. Attackers can exploit these vulnerabilities to manipulate the contract's functionality, leading to financial losses or unauthorised access to sensitive data [16].

iv. Majority attacks

Studies [22], [29] concern 51% of most attacks, highlighting areas requiring specific attention and enhancement as the technology evolves. The possibility of 51% majority attacks on certain blockchain networks, where malicious actors control most of the network's hashing power, could compromise the integrity of the voting process [22]. Additionally, the study [22] notes that existing blockchain voting systems may still be vulnerable to denial-of-service (DoS) attacks, which could disrupt the voting process. Figure 2 refers to the specific issues arising from the publication, and Table 3 categorises the related issues.

As shown in Figure 2, a summary of the issues resembles the themes to address.

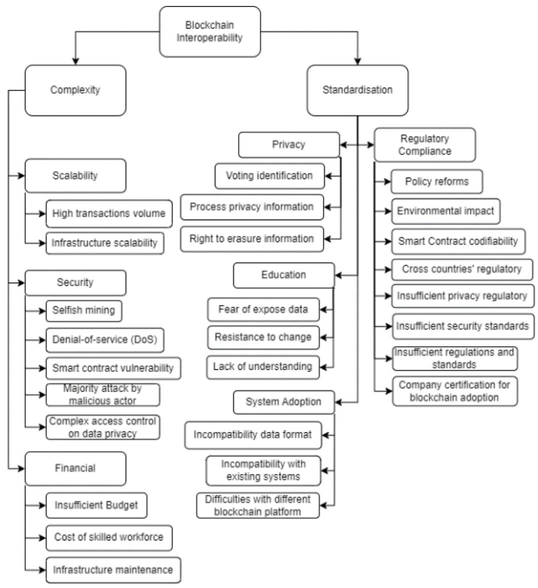

Figure 2 List of Issues

2. Future Works

Blockchain technology presents significant opportunities for transforming the AEO system by addressing the challenges of complexity and standardisation. However, integrating blockchain into the AEO system is not without its obstacles. Regulatory misalignment, scalability, and privacy concerns continue to limit widespread adoption. Further research and development are needed to realise blockchain's full potential in enhancing the AEO system. These proposals focus on complexity and standardisation to bridge current gaps and unlock new opportunities for the AEO system.

Table 6 Recommendations

Future Work Area	Proposed Focus	Rationale
Enhanced Interoperability	Develop standardised protocols and frameworks for cross-platform integration.	Current interoperability challenges hinder seamless communication between blockchain platforms and legacy systems.
Regulatory Alignment	Collaborate with policymakers to create unified global trade laws for blockchain.	Addressing discrepancies in international regulations is critical for enabling smooth blockchain integration in AEO systems.
Scalable Blockchain Models	Research scalable solutions like Layer 2 technologies, sharding, and hybrid models.	High transaction volumes in AEO systems demand scalable blockchain frameworks to avoid bottlenecks and delays.
Advanced Privacy-Preserving Mechanisms	Investigate techniques like zero-knowledge proofs and differential privacy.	Balancing blockchain transparency with data privacy concerns is essential for stakeholder trust and regulatory compliance.
Cost-Efficient Solutions	Design lightweight and modular blockchain models tailored for SMEs.	High blockchain implementation and maintenance costs can exclude small and medium enterprises from adoption.
Stakeholder Engagement and Training	Research resistance to adoption and develop targeted training programs.	Lack of stakeholder understanding and acceptance is a major barrier to blockchain adoption in AEO systems.
Sustainability	Explore energy-efficient consensus mechanisms like proof-of-stake or proof-of-authority.	Energy-intensive blockchain models conflict with global sustainability goals, such as reducing carbon footprints.
Integration of Emerging Technologies	Combine blockchain with IoT, AI, and big data analytics for AEO systems.	Integration with complementary technologies can enhance real-time tracking, predictive analytics, and automation in supply chain operations.
Impact Assessment Studies	Conduct longitudinal studies to measure blockchain adoption's economic, operational, and environmental effects.	Empirical data is needed to evaluate the long-term benefits and challenges of blockchain implementation in AEO systems.
Pilot Programs and Case Studies	Implement blockchain pilots in diverse regulatory and economic environments.	Real-world pilots provide actionable insights for scaling blockchain in AEO operations while documenting lessons learned.

Enhanced interoperability frameworks, scalable blockchain models, and privacy-preserving mechanisms are essential for ensuring the seamless integration of blockchain into existing AEO systems. Additionally, aligning blockchain solutions with international regulations and exploring cost-efficient and sustainable models will facilitate broader adoption across diverse industries and stakeholders.

Integrating emerging technologies like IoT and AI, along with empirical impact assessment studies, can further refine the implementation and efficacy of blockchain in AEO systems.

These proposed future works serve as a roadmap for researchers, policymakers, and practitioners to collaboratively shape a secure, efficient, and globally compliant AEO ecosystem powered by blockchain technology. By addressing these priorities, the transformative potential of blockchain for global trade can be fully realised.

3. Conclusion

In summary, the key takeaway revolves around the complexity and standardisation of blockchain. This highlights the challenges associated with technology, particularly blockchain, which requires in-depth knowledge and expertise. Understanding how the system operates and addressing issues like security, scalability, and interoperability are critical [7].

Addressing market or community needs requires an understanding of standardisation and complexity requirements. Achieving valuable dependency necessitates an interoperability between technical skills and diplomatic/political abilities to ensure critical demands are met effectively.

Acknowledgements

This work is supported by MIMOS Berhad and Ministry of Science, Technology and Innovation (MOSTI) under Grant No. SRF PG3-P, titled “Blockchain System for Customs AEO and OGA”. The authors gratefully acknowledge their financial and technical support, which was instrumental in conducting this research.

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this paper.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” [Online]. Available: https://ssrn.com/abstract=3440802

[2] Linux Foundation, “Writing Your First Chaincode — Hyperledger Fabric Docs main documentation.” Accessed: Jul. 19, 2024. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/chaincode4ade.html

[3] World Economic Forum, “Community Paper Reimagining Digital Identity: A Strategic Imperative,” 2020. [Online]. Available: www.weforum.org

[4] ISO, “ISO T/R 3242 Blockchain and distributed ledger technologies-Use cases,” 2022. [Online]. Available: www.iso.org

[5] C. Caballini and M. Benzi, “[25] Fast Corridors: innovative customs processes and technology to increase supply chain competitiveness. The case of IKEA Italy,” *Transp Res Interdiscip Perspect*, vol. 21, p. 100909, 2023, doi: https://doi.org/10.1016/j.trip.2023.100909.

[6] C. Pauletto, “[37] Blockchain in international e-government processes: Opportunities for recognition of foreign qualifications,” *Research in Globalization*, vol. 3, p. 100034, 2021, doi: https://doi.org/10.1016/j.resglo.2020.100034.

[7] M. I. Sahalan, F. Yusof, and H. Abas, “The challenges of using blockchain technology for medical data in public hospitals in Malaysia Article history,” 2023.

[8] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering–a systematic literature review,” *Inf Softw Technol*, vol. 51, no. 1, pp. 7–15, 2009.

[9] R. Gupta and R. Shankar, “[3] Managing food security using blockchain-enabled traceability system,” *BENCHMARKING-AN INTERNATIONAL JOURNAL*, vol. 31, no. 1, pp. 53–74, 2024, doi: 10.1108/BIJ-01-2022-0029.

[10] S. Kadam, R. Senta, R. K. Sah, A. Sawant, and S. Jain, “[4] Blockchain Revolution: A New Horizon for Supply Chain Management in Hotel Industry,” in *2024 International Conference on Emerging Smart Computing and Informatics (ESCI)*, Mar. 2024, pp. 1–8. doi: 10.1109/ESCI59607.2024.10497236.

[11] R. Manzoor, B. S. Sahay, and S. K. Singh, “[5] Examining the Factors That Facilitate or Hinder the Use of Blockchain Technology to Enhance the Resilience of Supply Chains,” *IEEE Trans Eng Manag*, vol. 71, pp. 10626–10649, Jun. 2024, doi: 10.1109/TEM.2024.3358722.

[12] H. Abu-tarboush, J. H. Lee, M. Al-shrouf, N. O. Maaitah, and N. A. Al-Dmour, “[6] Blockchain and its Integration with IoT Security,” in *2024 2nd International Conference on Cyber Resilience (ICCR)*, Feb. 2024, pp. 1–4. doi: 10.1109/ICCR61006.2024.10533114.

[13] E. Bandara, S. Shetty, A. Rahman, R. Mukkamala, P. Foytik, and X. Liang, “[8] RMF-GPT — OpenAI GPT-3.5 LLM, Blockchain, NFT, Model Cards and OpenScap Enabled Intelligent RMF Automation System,” in *2024 International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2024, pp. 653–658. doi: 10.1109/ICNC59896.2024.10555963.

[14] M. S. Faiyaz, N. Dhanda, A. Srivastava, G. D. Singh, and R. Verma, “[9] Securing Supply Chain - Blockchain: Leveraging ICC for Product Verification and Validation,” in *2024 2nd International Conference on Disruptive Technologies (ICDT)*, Mar. 2024, pp. 1691–1698. doi: 10.1109/ICDT61202.2024.10489614.

[15] A. Babaei, M. Khedmati, M. R. A. Jokar, and E. B. Tirkolaee, “[14] Designing an integrated blockchain-enabled supply chain network under uncertainty,” *Sci Rep*, vol. 13, no. 1, 2023, doi: 10.1038/s41598-023-30439-9.

[16] H. Song, Y. Yang, and Z. Tao, “[23] Application of blockchain in enterprise financing: literature review and knowledge framework,” *Nankai Business Review International*, vol. 14, no. 3, pp. 373 – 399, 2023, doi: 10.1108/NBRI-08-2022-0080.

[17] V. D’Angelo and V. Belvedere, “[26] Green Supply Chains and Digital Supply Chains: Identifying Overlapping Areas,” Jun. 01, 2023, *MDPI*. doi: 10.3390/su15129828.

[18] D. B. Gajić *et al.*, “[33] A Distributed Ledger-Based Automated Marketplace for the Decentralized Trading of Renewable Energy in Smart Grids,” *Energies (Basel)*, vol. 15, no. 6, Mar. 2022, doi: 10.3390/en15062121.

[19] H. Yang and Y. Wang, “[34] Practice of Trade Facilitation in China Free Trade Zone and Its Enlightenment to Heilongjiang Free Trade Zone: Basic Principal Component Analysis Method,” in *Proceedings of the 2021 1st International Conference on Control and Intelligent Robotics*, in ICCIR ’21. New York, NY,

USA: Association for Computing Machinery, 2021, pp. 459–463. doi: 10.1145/3473714.3473793.

[20] N. Etemadi, F. Strozzi, P. Van Gelder, and T. Etemadi, "[36] An ISM Modelling of Success Factors for Blockchain Adoption in a Cyber Secure Supply Chain," in *Proceedings of the 2021 4th International Conference on Computers in Management and Business*, in ICCMB '21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 65–72. doi: 10.1145/3450588.3450600.

[21] Q. Wang, R. Li, and L. Zhan, "[38] Blockchain technology in the energy sector: From basic research to real world applications," Feb. 01, 2021, *Elsevier Ireland Ltd*. doi: 10.1016/j.cosrev.2021.100362.

[22] U. Jafar, M. J. A. Aziz, and Z. Shukur, "[39] Blockchain for electronic voting system—review and open research challenges," Sep. 01, 2021, *MDPI*. doi: 10.3390/s21175874.

[23] M. Al Ketbi, K. Shuaib, E. Barka, and M. Gergely, "[40] Establishing a security control framework for blockchain technology," *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 16, pp. 307–330, 2021, doi: 10.28945/4837.

[24] P. Roseiro and J. Parra-Domínguez, "[41] Blockchain: a brief review of Agri-Food Supply Chain Solutions and Opportunities," *ADCAIJ-ADVANCES IN DISTRIBUTED COMPUTING AND ARTIFICIAL INTELLIGENCE JOURNAL*, vol. 9, no. 4, pp. 95–106, 2020, doi: 10.14201/ADCAIJ20209495106.

[25] Surjandy, Meyliana, H. L. H. Spits Warnars, and E. Abdurachman, "[43] Blockchain Technology Open Problems and Impact to Supply Chain Management in Automotive Component Industry," in *2020 6th International Conference on Computing Engineering and Design (ICCED)*, Oct. 2020, pp. 1–4. doi: 10.1109/ICCED51276.2020.9415836.

[26] G. Guarín Duque and J. D. Zuluaga Torres, "[44] Enhancing E-Commerce through Blockchain (DLTs): The Regulatory Paradox for Digital Governance," *Global Jurist*, vol. 20, no. 2, 2020, doi: 10.1515/gj-2019-0049.

[27] M. M. Queiroz, R. Telles, and S. H. Bonilla, "[45] Blockchain and supply chain management integration: a systematic review of the literature," Feb. 24, 2020, *Emerald Group Holdings Ltd.* doi: 10.1108/SCM-03-2018-0143.

[28] L. König, Y. Korobeinikova, S. Tjoa, and P. Kieseberg, "[46] Comparing blockchain standards and recommendations," *Future Internet*, vol. 12, no. 12, pp. 1–17, Dec. 2020, doi: 10.3390/fi12120222.

[29] W. George and T. Al-Ansari, "[2] Roadmap for National Adoption of Blockchain Technology Towards Securing the Food System of Qatar," *Sustainability*, vol. 16, no. 7, 2024, doi: 10.3390/su16072956.

[30] H. Xu, H. Zheng, D. Sun, M. Wang, and C. Ye, "[1] An Integrated Framework for Enablers in Supply Chain Resilience: Model Development and Analysis," *IEEE Access*, vol. 12, pp. 42490–42508, 2024, doi: 10.1109/ACCESS.2024.3379212.

[31] F. T. Adebusoye *et al.*, "[10] Terrorism's impact on low and middle-income countries' healthcare services: A perspective," *J Public Health Res*, vol. 13, no. 1, 2024, doi: 10.1177/22799036241231544.

[32] P. E. Mora Lozano and J. R. Montoya-Torres, "[11] Global Supply Chains Made Visible through Logistics Security Management," *Logistics*, vol. 8, no. 1, p. 6, 2024, doi: https://doi.org/10.3390/logistics8010006.

[33] S. Porkodi and D. Kesavaraja, “[15] Smart contract: a survey towards extortionate vulnerability detection and security enhancement,” *WIRELESS NETWORKS*, 2023, doi: 10.1007/s11276-023-03587-z.

[34] C. P. Mohammed and S. R. Chopra, “[16] Blockchain Security Implementation using Python with NB-IoT deployment in Food Supply Chain,” in *2023 International Conference on Emerging Smart Computing and Informatics (ESCI)*, Mar. 2023, pp. 1–5. doi: 10.1109/ESCI56872.2023.10100139.

[35] F. Golshani, “[17] Feasting on Technology: The Art of Computer-Enhanced Serving,” in *2023 IEEE 39th International Conference on Data Engineering Workshops (ICDEW)*, Apr. 2023, pp. 218–219. doi: 10.1109/ICDEW58674.2023.00042.

[36] I. M. Musthafa Sheriff and D. J. Aravindhar, “[18] Blockchain Integration for Enhanced Agri-Food Supply Chain Security and Efficiency,” in *2023 6th International Conference on Recent Trends in Advance Computing (ICRTAC)*, Dec. 2023, pp. 27–32. doi: 10.1109/ICRTAC59277.2023.10480814.

[37] N. Rameshkumar, E. Kalaivani, A. Bhope, R. Sobti, K. Subhashini, and M. L. B, “[19] Blockchain Technology: Revolutionizing Sectors and Defining Digital Transactions’ Future,” in *2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, Dec. 2023, pp. 1738–1742. doi: 10.1109/UPCON59197.2023.10434406.

[38] A. Alahbabi, K. Alshehhi, A. Albloushi, and K. Shuaib, “[20] Establishing Security Controls For Blockchain Technology In P2P Energy Trading,” in *2023 IEEE PES Conference on Innovative Smart Grid Technologies - Middle East (ISGT Middle East)*, Mar. 2023, pp. 1–6. doi: 10.1109/ISGTMiddleEast56437.2023.10078508.

[39] Q. Wang and Y. Liu, “[21] Enhancing Collaborative Emergency Management: Leveraging Blockchain Distributed Ledger for Inter-Agency Data Sharing,” in *EM-GIS 2023 - Proceedings of the 8th ACM SIGSPATIAL International Workshop on Security Response using GIS 2023*, H. Y., T. J.-C., Z. H., G. D., L. Y., X. W., and C. B., Eds., Association for Computing Machinery, Inc, 2023, pp. 13 – 17. doi: 10.1145/3615884.3629423.

[40] B. Aljabhan and M. A. Obaidat, “[22] Privacy-Preserving Blockchain Framework for Supply Chain Management: Perceptive Craving Game Search Optimization (PCGSO),” *Sustainability (Switzerland)*, vol. 15, no. 8, 2023, doi: 10.3390/su15086905.

[41] N. K. Dewangan and P. Chandrakar, “[24] Patient-Centric Token-Based Healthcare Blockchain Implementation Using Secure Internet of Medical Things,” *IEEE Trans Comput Soc Syst*, vol. 10, no. 6, pp. 3109–3119, 2023, doi: 10.1109/TCSS.2022.3194872.

[42] L. F. Huang, L. Zhen, J. B. Wang, and X. Zhang, “[27] Blockchain implementation for circular supply chain management: Evaluating critical success factors,” *INDUSTRIAL MARKETING MANAGEMENT*, vol. 102, pp. 451–464, 2022, doi: 10.1016/j.indmarman.2022.02.009.

[43] S. Yadav and S. P. Singh, “[28] Modelling procurement problems in the environment of blockchain technology,” *Comput Ind Eng*, vol. 172, 2022, doi: 10.1016/j.cie.2022.108546.

[44] D. Prajapati, S. K. Jauhar, A. Gunasekaran, S. S. Kamble, and S. Pratap, “[29] Blockchain and IoT embedded sustainable virtual closed-loop supply chain in E-commerce towards the circular economy,” *Comput Ind Eng*, vol. 172, 2022, doi: 10.1016/j.cie.2022.108530.

[45] H. Niavis and K. Loupos, “[30] ConSenseIoT: A Consensus Algorithm for Secure and Scalable Blockchain in the IoT context,” in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, in ARES ’22. New York, NY, USA: Association for Computing Machinery, 2022. doi: 10.1145/3538969.3543811.

[46] F. K. Elmay, K. Salah, R. Jayaraman, and I. A. Omar, “[31] Using NFTs and Blockchain for Traceability and Auctioning of Shipping Containers and Cargo in Maritime Industry,” *IEEE ACCESS*, vol. 10, pp. 124507–124522, 2022, doi: 10.1109/ACCESS.2022.3225000.

[47] A. Mettler and J. S. Lobo, “[32] The Future of the Logistics Industry in the European Union: An Outlook to 2032 Supported by Current and Upcoming Market Trends,” Portugal, 2022. [Online]. Available: https://vpn.utm.my/dissertations-theses/future-logistics-industry-european-union-outlook/docview/3059436896/se-2?accountid=41678

[48] P. Kumar, M. Kumar, K. B. Singh, A. R. Tripathi, and A. Kumar, “[35] Blockchain Security Detection Condition Light Module,” in *2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART)*, Dec. 2021, pp. 363–367. doi: 10.1109/SMART52563.2021.9676302.

[49] P. Saindane, Y. Jethani, P. Mahtani, C. Rohra, and P. Lund, “[42] Blockchain: A Solution for Improved Traceability with Reduced Counterfeits in Supply Chain of Drugs,” in *2020 International Conference on Electrotechnical Complexes and Systems (ICOECS)*, Oct. 2020, pp. 1–5. doi: 10.1109/ICOECS50468.2020.9278412.

[50] S. A. Kalaiselvan, J. S. Prasanna Venkatesh, A. M. Vasanth Kumar, and K. Raghul Karthik, “[7] Blockchain Powered Carbon Credit Marketplace,” in *2024 10th International Conference on Communication and Signal Processing (ICCSP)*, Apr. 2024, pp. 582–585. doi: 10.1109/ICCSP60870.2024.10543794.

[51] M. Oudani, A. Sebbar, K. Zkik, I. El Harraki, and A. Belhadi, “[13] Green Blockchain based IoT for secured supply chain of hazardous materials,” *Comput Ind Eng*, vol. 175, 2023, doi: 10.1016/j.cie.2022.108814.