A Novel Integrated Freight Forwarding Information System Based on Block-Chain Technology

[1]CHENGLIAN LIU, [2]SONIA C-I CHEN
[1]School of Computing, Neusoft Institute of Guangdong, Foshan 528225, CHINA
[2]School of Economics, Qingdao University, Qingdao 266061, CHINA

Abstract: As an emerging foreign trade model, crossborder E-commerce is booming. This foreign trade model shortens the distance between products from manufacturers to foreign consumers and reshapes the value chain of foreign trade. However, because buyers and sellers use virtualization. Negotiations and consultations on the platform may also involve the participation of freight forwarders and the services of shipping companies, which increases the uncertainty of the transaction process and results. How to efficiently and confidentially transfer information to each other is the main idea and goal of this paper. Foreign buyers, domestic sellers, shipping companies, and freight forwarding companies are independent entities. Due to common transaction events, the interaction between the four parties has been promoted. However, independent information systems cannot exchange information (or content) with other entities. Based on this point, our goal has formulated an integrated freight forwarding program.

Keywords: ElGamal Algorithm, Anonymity, Double- Blind Mechanism

Received: April 28, 2021. Revised: July 18, 2022. Accepted: August 14, 2022. Published: September 14, 2022.

1. Introduction

In today's society with highly competitive business, no matter which company or seller is concerned, partners are afraid of digging into each other's corners. The current freight forwarding operation system focuses on freight calculation, customs declaration and shortest path optimization. Especially when it comes to commercial activities between import and export trade, the considerations are more complicated; whether it is a freight forwarding company at home and abroad, it is most afraid of partners to dig each other's corners. Therefore, how to prevent these situations from happening is a difficult problem for everyone. This research intends to use Partial Information in the theory of Knowledge Management to try to deal with and solve corner-cutting incidents. Corresponding research at home and abroad is currently at the initial stage, and there are very few similar subjects. At the same time, our team proposed this system in the context of research. It will improve trade security and enhance the feasibility of transactions between the two parties, thereby promoting the development of cross-border e-commerce. As an emerging foreign trade model, cross-border e-commerce is booming. This foreign trade model has shortened the distance between products from manufacturers to foreign consumers, and has reshaped the value chain of foreign trade. However, because buyers and sellers use virtualization Negotiations and consultations on the platform may also involve the participation of freight forwarders and the services of shipping companies, which increases the uncertainty of the transaction process and results. How to efficiently and confidentially transfer information to each other is the main idea and goal of this project. The main highlight and contribution of this research is that the integrated cross-border e-commerce information leakage prevention system of this program can be used as a part of the management information system (MIS, Management Information System) system of the cross-border e-commerce platform. This system is proposed optimize the information security of both parties to the transaction, thereby improving the security of cross-border e-commerce transactions, protecting the rights and interests of buyers and sellers, and freight forwarders can trade safely. Therefore, this scheme has a high degree of commercial value and can be practically applied in commercial trade. With the construction of China's "One Belt One Road' policies and the increase of import and export trade, I am more convinced of the research value of this research.

2. Literature Review

In 2007, Zhang et al. [1] used the game theory method to explore the process of freight information exchange network promotion. Wei [2] mentioned the formulation of port of loading and unloading in the bill of lading in 2008. In the same year, Deng and Zhang [3] proposed

the design of electronic customer relationship management system for freight forwarding industry. Yang and Luo [4] also proposed a management information system for freight forwarding business of small enterprises; Zheng [5] mentioned that computerization is an important way for China's international freight forwarders to improve their competitiveness. Hu et al. [6] studied the integration of supply chain information resources to promote the development of freight forwarding industry. The application of blockchain technology in supply chain management literatures such as Jabbari and Kaminsk [7], and Jabbar et al. [8]. The application of blockchain technology in logistics includes Issaouia et al. [9], Tijan et al. [10], Irannezhad [11], and Koh et al. [12]. The related research of freight agency in other aspects are listed in Table 1.

Table 1
RELATED LITERATURES

Year	SCM	CRM	Logistics	Others
2007				Zhang et al. [1]
2008				Wei [2]
2008		Deng & Zhang [3]		
2009				Yang & Luo [4]
2010				Zheng & Xu [5]
2010			Poon & Choy [13]	
2015	Hu & Liu [6]			
2016			Huang [14]	
2017				Hopkins [15]
2018	Jabbari & Kaminsky [7]			
2019			Issaouia et al. [9]	
2019			Tijan et al. [10]	
2019			Irannezhad [11]	
2019				Hackius et al. [16]
2019				Elbert & Gleser [17]
2020				Tsiulin et al. [18]
2020	Jabbar et al. [8]			
2020			Koh et al. [12]	
2021				Tan & Sundarakani [19]

3. Our Research Methodology

This article extends the concept of information security technology and management, and specifically introduces cryptography and information security mechanisms into the securities regulatory system review system, combined with the ElGamal algorithm, to meet the requirements of the securities regulatory process. In the process of submitting materials, the supervisory system can set to know or not know the identity of the investor (double-blind mechanism). Based on this design concept, the handler passively knows or does not know the identity of the investor. This article is a conditional anonymity plan. During the submission process, investors and brokers have registered and issued accounts and order confirmations, and investors, brokers, and regulators are anonymous to each other. The system processes the investor has no direct dealings with the stock exchange, stock exchange can not know the true identity of the investor; the Commission is entitled to the role of supervision and inspection of the contents of investor transactions, and exchanges of information inquiry ; and SEC The securities firm is responsible for reporting the business to the Securities Regulatory Commission; the securities dealers need transaction returns to the Stock Exchange. The core of this algorithm has 8 stages, namely: registration stage, account issuance stage, order placement stage, order confirmation stage, transaction return stage, report business stage, data inquiry and supervision and inspection stage. The detailed process of each stage is as follows description:

Step 1. The purchaser orders something by merchant.
Step 2. The merchant receives an order, he then authorizes the freight forwarder to process Shipments.
Step 3. The freight forwarder books compartment with shipping company (may be airline).
Step 4. The shipping company sends back the bill of lading to the freight forwarder. 5
Step 5. The freight forwarder sends back the bill of lading information to the merchant.
Step 6. The merchant provides shipping information to the purchaser.
Step 7. The shipping company informs the purchaser to pick up the cargoes.
Step 8. Purchaser pick up his cargoes.
Step 9. The shipping company informs the freight forwarder of the delivery result.

Notation and **Significant**:
p: is a prime number, usually more than 1024 bits length.
g: is the primitive root of prime number p.
x_i: is a private key in ElGamal like algorithm.
y_i: is a public key in ElGamal like algorithm.
m: digitized message.
Purchaser: mean to foreign buyer, we usually use 'purchaser' instead of buyer in this paper.
Merchant: mean to domestic seller, we usually use 'merchant' in this article.
Freight Forwarder: is sometimes called cargo agent.
Shipping Company: express the transportation company such as railway, shipping or airline. It depends on the contract content of the transaction.

3.1. System Initialization Phase

3.1 In the system initialization phase, all users such as purchaser, merchant, freight forwarders and the shipping company set their own account numbers and passwords, and share primitive parameters g and a large prime numbers p through the system.
The merchant randomly selects a number x_a, as its

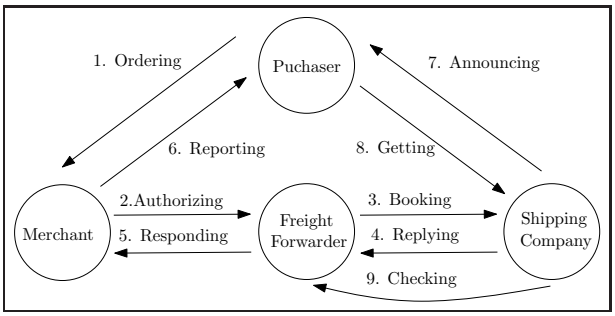

Figure 1. The Idea of Conception.

private key and satisfies $\gcd(x_a, p-1)$, then calculates his public key

$$y_a \equiv g^{x_a} \pmod{p} \tag{1}$$

The freight forwarder (or agent) randomly selects its own private key x_b to calculates its own public key y_b, and then announces

$$y_b \equiv g^{x_b} \pmod{p} \tag{2}$$

The purchaser randomly selects its own private key x_c to calculates its own public key y_c, and publishes it

$$y_c \equiv g^{x_c} \pmod{p} \tag{3}$$

Shipping company will randomly select its own private key x_d to calculate his public key y_d, and then publishes

$$y_d \equiv g^{x_d} \pmod{p}. \tag{4}$$

Please see Figure 2.

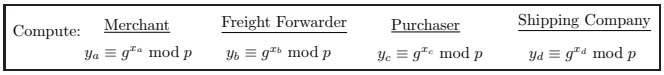

Figure 2. The System Initializing Phase.

3.2. Ordering Phase

3.2 The purchaser uses his private key x_c, nonce key k_c and merchant's public key y_a to produce an order S_c where

$$S_c \equiv y_a^{x_c} \cdot r_a^{k_c} \bmod p. \tag{5}$$

and sends these two parameters $\{S_c, r_c\}$ to the merchant, see Figure 3.

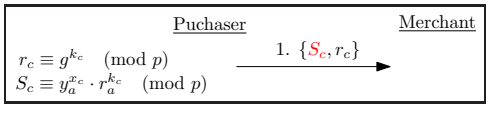

Figure 3. The Ordering Phase.

3.3. Authorizing Phase

3.3 When the merchant receives $\{S_c, r_c\}$ from purchaser, he then authorizes the freight forwarder to delegate shipments, see Equation 6 and Figure 4.

$$W_c \equiv s_c \cdot r_c^{-k_a} \cdot y_b^{r_c} \bmod p. \tag{6}$$

And sends $\{W_c, r_c\}$ to freight forwarder, see Figure 4.

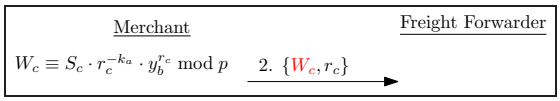

Figure 4. The Authorizing Phase.

3.4. Booking Phase

3.4 The freight forwarder obtains a valid delegation and after books some cabins according to the contract information by shipping company, see Equation 7 and Figure 5.

$$T_c \equiv (w_c)^{x_b} \cdot y_b^{-r_c x_b} \bmod p, \tag{7}$$

see Figure 5.

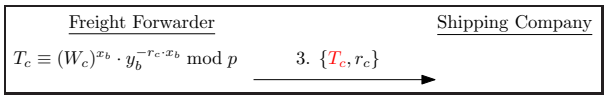

Figure 5. The Booking Phase.

3.5. Replying Phase

3.5 The shipping company uses his private key x_d to sign the bill of lading before he returned $\{V_c, r_d\}$ to freight forwarder, see Equation 8 and Figure 6.

$$V_c \equiv (t_c)^{x_d} \bmod p. \tag{8}$$

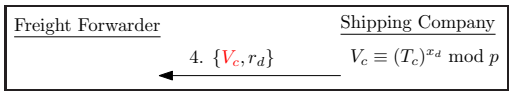

Figure 6. The Replying Phase.

3.6. Responding Phase

3.6 Freight forwarder received a valid bill of lading from shipping company, freight forwarder uses his private key x_b^{-1} to endorse it, and then forward partially information to merchant, see Equation (9) and Figure 7.

$$z_c \equiv (v_c)^{x_b^{-1}} \bmod p. \tag{9}$$

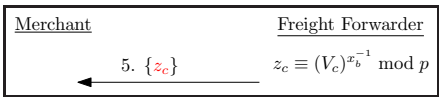

Figure 7. The Responding Phase.

3.7. Reporting Phase

3.7 The merchant reported the cargoes progress to purchaser before merchant endorsed the bill of lading, see Equation (10) and Figure 8.

$$\eta_c \equiv (z_c)^{x_a^{-1}} \bmod p, \tag{10}$$

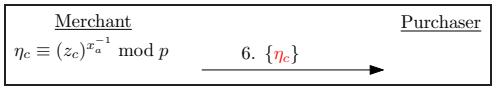

Figure 8. The Report Business Phase.

3.8. Announcing Phase

3.8 In the same time, the shipping company will also announce cargoes information such as arrival date, time and place of port, see Equation (11) and Figure 9.

$$\beta_c \equiv r_c^{k_d} \bmod p. \tag{11}$$

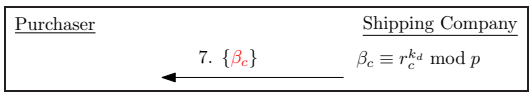

Figure 9. The Information Inquiry Phase.

3.9. Getting Phase

3.9 When purchaser got an announcement from shipping company, the purchaser will ready to fetch these cargoes, see Equation (12) and Figure10.

$$\psi_c \equiv (\beta_c)^{k_c^{-1}} \bmod p. \tag{12}$$

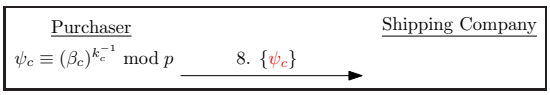

Figure 10. The Supervision and Inspection Phase.

Proof. Omitted. □

123243

3.10. Checking Phase

3.10 In finally phase, the shipping company will result the useful information after purchaser finished to picked it up all cargoes, see Equation (13) and Figure11.

$$\rho_b \equiv y_b^{k_d} \bmod p. \tag{13}$$

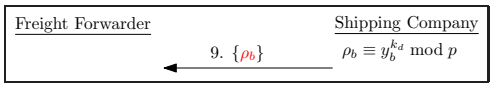

Figure 11. The Checking Phase.

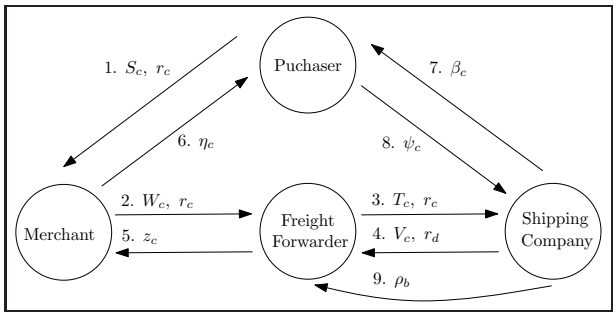

Figure 12. The protocol of this scheme.

4. Security Analysis

1312321

Definition 1. *Discrete Logarithm Problem (DLP)*
When the calculation formula $y_i \equiv g^{x_i} \pmod p$*, and as known parameters* $\{p,\ g,\ y_i\}$*, to find the private key* x_i *while prime approaching infinite, it is very difficult to calculate* x_i*; it is impossible computation, in which case the condition is called Solving the discrete logarithm problem (Solving Discrete Logarithm Problem) [?]. The current public key cryptosystem based on discrete logarithm has value parameters that are greater than 1024 bit length or 2048 bit length.*

Definition 2. *Computation Diffie-Hellman Problem (CDHP)*
The Computation Diffie-Hellman Problem [?]is derived on the Diffie-Hellman key exchange principle (Diffie Hellman Key Exchange) [?]. The main ideas are described as follows: Given $\{g,\ g^x,\ g^y\}$ *to find* g^{xy}*. Here,* g *is known parameter, the* x *and* y *are unknown parameters.*

Definition 3. *Decisional Diffie-Hellman Problem (DDHP)*
The Decisional Diffie-Hellman Problem [?] is a variant of the Diffie-Hellman computation problem. Given $\{g,\ g^x,\ g^y,\ g^z\}$*, to find the* $\mathbb{Z}_p$ *is satisfied* $z = xy$*.*

Given $\{g,\ g^x,\ g^y\}$*, to find* g^{xy}*. Here the parameter* g *is known, and the parameters* $\{x,\ y,\ z\}$ *are all unknown.*

4.1. Theoretical Security Level Analysis

Theoretical Security Level Analysis Analysis security of theoretical level

Lemma 1. *If Purchaser is honest, then the Equation (5) holds, that is, the broker verified the user.*

Proof. As known the Equation (5) S_c calculated by purchaser, if purchaser honestly use his private key x_c and nonce key k_c to sign the Merchant's public key y_a and semi public key r_c since

$$S_c \equiv y_a^{x_c} \cdot r_a^{k_c} \pmod{p}. \tag{14}$$

The merchant can re-express the Equation (7) to

$$S_c \stackrel{?}{\equiv} y_c^{x_a} \cdot r_c^{k_a} \pmod{p}. \tag{15}$$

If merchant honestly uses his private key x_a and nonce key r_a, the Equation (7) and (30) are equal to pass the verification. Otherwise, it is a contradiction. □

Lemma 2. *If Merchant is honest, then the Equation (6) holds, that is, the broker verified the user.*

Proof. As known the Equation (8) W_c calculated by merchant, the merchant honestly uses his semi key k_a to sign in the contract, there include the freight forwarder's public key y_b, and the purchaser's semi key r_c. Thus, we can rewrite the the Equation (8) to

$$\begin{aligned} W_c &\stackrel{?}{\equiv} S_c \cdot r_c^{-k_a} \cdot y_b^{r_c} \pmod{p} \\ &\equiv y_a^{x_c} \cdot y_b^{r_c} \pmod{p} \\ &\equiv y_c^{x_a} \cdot y_b^{r_c} \pmod{p} \end{aligned} \tag{16}$$

Therefore, the purchaser and merchant verify each other through equation (30), they can also verify each other by Equation (31). □

Lemma 3. *If Shipping Company is honest, then the Equation (6) and Equation (6) holds, that is, the broker verified the user.*

Proof. As known the Equation (8), the shipping company announces β_c to purchaser, the purchaser can verify whether the shipping company is honest, as shown in Equation (32).

$$\beta_c \stackrel{?}{\equiv} r_d^{k_c} \pmod{p}, \tag{17}$$

and purchaser used k_c^{-1} to sign in ψ_c where

$$\psi_c \equiv r_d. \tag{18}$$

On the other hand, the freight forwarder can also check whether shipping company is honest or dishonest; the freight forwarder used x_b^{-1} to recover r_d by τ_b, namely

$$\tau_b \equiv r_d. \tag{19}$$

In summary, the purchaser and the freight forwarder can verify the identity of the shipping company. □

Lemma 4. *If Freight Forwarder is honest, then the Equation (6) and Equation (6) holds, that is, the broker verified the user.*

Proof. Because the merchant sent W_c and r_c to the freight forwarder, and then the freight forwarder returned z_c to merchant. Consequently, the freight forward produce T_c before he used $y_b^{-r_c x_b}$ to sign the message. Based on this point, shipping company can verify the identity of freight forwarder. When V_c is generated by the shipping company, it means that the four party agreement has been generated, The freight forwarder generated z_c and transmitted it to the merchant, he also used x_b^{-1} before decoding. It fully proves the freight forwarder honesty. Therefore, it is impossible for the freight forwarder to cheat only one side and be honest with the another sides, or cheat both sides"merchant–shipping company", it is a contradiction with our assumption. Thus, the freight forwarder have to honest in the stage "3-5" of phases "2-3-4-5"; otherwise, from Lemma 1 to Lemma 3 became contradictions. □

4.2. Analysis of Practical Safety Levels

Analysis security of practical levels

User identity leak concerns: investors to brokerage orders, the identity with anonymity, Stock Exchange even by Equation (16) to obtain the original content m, stock exchange still does not know the original user's identity. The Securities Regulatory Commission obtains the content m through equation (13), which does not mean that the Securities Regulatory Commission knows the identity of the investor. Therefore, the identity of the investor is anonymous to the stock exchange and the China Securities Regulatory Commission. To a certain extent, the identity of the investor is prevented from leaking in this link.

Leakage of the contents of risk: If the broker (system) invaded, hacked-off attempt by the brokerage has made investors under a single content is in vain. Only Stock Exchange and the SFC in after signing, can the number of bits of content is reduced to m, brokerage in before the transaction return phase , such as the Equation (8) and (9), are powerless to encrypted number of bits content reduced to m. If the hacker colludes with the

stock exchange or with any party of the China Securities Regulatory Commission, since the stock exchange or the China Securities Regulatory Commission can only obtain at most, there is no way to obtain the identity, and there is still no need to worry about the exposure of the identity under the risk of the original content being leaked problem.

Key theft issue: Investors, brokerage firms, stock exchanges, and the China Securities Regulatory Commission each keep their own keys. Although their public keys are public, hackers cannot use known public keys to calculate the corresponding keys, a discrete logarithm problem of the Definition 1, has been charged part narrative. Unless any party who owns the key reveals the key held by himself, this research does not consider this assumption.

5. Conclusion

This research is mainly about the four-party supervision and management plan of investors, securities firms, stock exchanges, and the China Securities Regulatory Commission. The improved ElGamal algorithm is used in the application of the securities industry regulatory information system. This information system is anonymous and the identity of any investor is strictly controlled. Keep it secret. If the brokerage (system) is invaded, hackers cannot obtain investor transaction content through the brokerage. If the hacker colludes with any of the regulatory agencies to deceive, he still does not have to worry about identity exposure. If the investor has breached the contract, the manager and the system center can track the anonymous identity under certain conditions, and finally restore the anonymous identity to the real-name user identity. In this way, the investor's security can be protected. The identity is protected from exposure, and on the other hand, it can deter investors from maliciously defaulting on transactions. This program has the best of both worlds. This research plan puts forward 6 lemmas, 3 definitions and 19 equations to run through the full text, provide a strong theoretical support for the thesis, and finally put this idea into reality. The real system proposes a securities industry supervision system with anonymity, non-modification, security, and double-blind mechanism to achieve a combination of theory and practice.

Acknowledgments

The authors would like to thank the anonymous reviewers for their useful comments. This work is partially supported from university project under the number NUIT2020-001. This work also partially supported by Guandong province special funds to foster the student's science and technology innovation under the number PDJH2020B0689 (Climbing program funds).

References

[1] L. Zhang, Z. Fu, and Z. Juan, "Study on the popularizing process of freight information exchange network based on evolutionary game theory," in *2007 International Conference on Wireless Communications, Networking and Mobile Computing*, 2007, pp. 6187–6190.

[2] R. Wei, "A critical issue of making out loading port and unloading port in the bill of lading for marine transportation," in *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, 2008, pp. 1–4.

[3] S. Deng and F. Zhang, "Design of a knowledge-based e-crm system: A case of freight forwarding industry," in *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, 2008, pp. 1–4.

[4] X. Yang and J. Luo, "Design and realization of management information system for the freight forwarding agency business of mini-enterprise," in *2009 International Symposium on Computer Network and Multimedia Technology*, 2009, pp. 1–4.

[5] J. Zheng and M. Xu, "Computerization, an important way for china's international freight forwarders to improve competitiveness," in *2010 International Conference on E-Business and E-Government*, 2010, pp. 3836–3839, in Chinese.

[6] X.-L. Hu and D. Liu, "Information resource integration of the supply chain to promote freight forwarding industry," in *2015 Third International Conference on Robot, Vision and Signal Processing (RVSP)*, 2015, pp. 117–120.

[7] A. Jabbari and P. Kaminsky, "Blockchain and supply chain management," https://www.mhi.org/downloads/learning/cicmhe/blockchain-and-supply-chain-management.pdf, January 2018.

[8] S. Jabbar, H. Lloyd, M. Hammoudeh, B. Adebisi, and U. Raza, "Blockchain-enabled supply chain: analysis, challenges, and future directions," *Multimedia Systems*, Nov 2020. [Online]. Available: https://doi.org/10.1007/s00530-020-00687-0

[9] Y. Issaoui, A. Khiat, A. Bahnasse, and H. Ouajji, "Smart logistics: Study of the application of blockchain technology," *Procedia Computer Science*, vol. 160, pp. 266–271, 2019, the 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2019) / The 9th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2019) / Affiliated Workshops. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919316825

[10] E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, "Blockchain technology implementation in logistics," *Sustainability*, vol. 11, no. 4, 2019. [Online]. Available: https://www.mdpi.com/2071-1050/11/4/1185

[11] E. Irannezhad, "Is blockchain a solution for logistics and freight transportation problems?" *Transportation Research Procedia*, vol. 48, pp. 290–306, 2020, recent Advances and Emerging Issues in Transport Research – An Editorial Note for the Selected Proceedings of WCTR 2019 Mumbai. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352146520304397

[12] L. Koh, A. Dolgui, and J. Sarkis, "Blockchain in transport and logistics – paradigms and transitions," *International Journal of Production Research*, vol. 58, no. 7, pp. 2054–2062, 2020.

[13] T. C. Poon and K. L. Choy, "Design of a logistics costs analyzer to formulate distribution routes for freight forwarders," in *2010 8th International Conference on Supply Chain Management and Information*, 2010, pp. 1–6.

[14] H. H. Huang, "Authorized economic operator in taiwan - an example of international freight forwarders," in *2016 IEEE International Conference on Management of Innovation and Technology (ICMIT)*, 2016, pp. 172–176.

[15] R. A. Hopkins, *Making the Sale: Proposals, Shipping, Payment, and Trade Finance*. Berkeley, CA: Apress, 2017, pp. 115–142. [Online]. Available: https://doi.org/10.1007/978-1-4842-3114-2_8

[16] N. Hackius, S. Reimers, and W. Kersten, "The privacy barrier for blockchain in logistics: First lessons from the port of hamburg," in *Logistics Management*, C. Bierwirth, T. Kirschstein, and D. Sackmann, Eds. Cham: Springer International Publishing, 2019, pp. 45–61.

[17] R. Elbert and M. Gleser, "Digital forwarders," in *Logistics Management*, C. Bierwirth, T. Kirschstein, and D. Sackmann, Eds. Cham: Springer International Publishing, 2019, pp. 19–31.

[18] S. Tsiulin, K. H. Reinau, O.-P. Hilmola, N. Goryaev, and A. Karam, "Blockchain-based applications in shipping and port management: a literature review towards defining key conceptual frameworks," *Review of International Business and Strategy*, vol. 30, no. 2, pp. 201–224, Jan 2020. [Online]. Available: https://doi.org/10.1108/RIBS-04-2019-0051

[19] W. K. A. Tan and B. Sundarakani, "Assessing blockchain technology application for freight booking business" a case study from technology acceptance model perspective," *Journal of Global Operations and Strategic Sourcing*, vol. 14, no. 1, pp. 202–223, 2021.