The Discontinuation of TradeLens and What Can Be Learned: Cryptographic Requirements For a New Global Maritime Logistics Infrastructure

Daniel Berger, Aaron Lye and Jannis Stoppe
German Aerospace Center DLR – Institute for the Protection of Maritime Infrastructures
Bremerhaven, Germany
{daniel.berger, aaron.lye, jannis.stoppe}@dlr.de

***Abstract*—In this paper, we examine the recent discontinuation of the blockchain-based platform TradeLens developed by IBM and Maersk, where many obstacles of maritime logistics have been addressed. With the discontinuation there are lessons to be learned and there is room for new approaches. We elaborate important cryptographic properties and discuss some issues of a global maritime logistics infrastructure. In particular, we address three points: (1) Centralization, federation and power struggles within the network; (2) zero-knowledge properties and applications for maritime logistics; (3) the use of post-quantum secure cryptographic primitives.**

***Index Terms*—Maritime Logistics, Bill of Lading, Blockchain, Zero-knowledge, Post-quantum Cryptography**

I. Introduction

Maritime logistics is the backbone of global trade. Roughly 90% of goods are transferred worldwide by shipping and the worlds economy relies heavily on the respective infrastructure. The international shipping ecosystems contain a huge number of different agents like carriers, shippers, shipping agents, banks, terminal operators, freight forwarders, port authorities and customs [11]. Central processes are those related to the effective sea transport such as planning and organizing vessel operations, route planning, cargo planning and refuelling/bunkering as well as port logistics processes when a vessel arrives at a port including ship handling, terminal operations, border control and customs inspections for goods entering or leaving a country. This also requires efficient capacity management of vessel space, terminal facilities and storage capacity. The coordination of all parties involved in maritime logistics is crucial for ensuring efficient seaway operations. However, usually every operator has their own digital systems of record. There is almost no interconnection between peer companies.

Logistics IT is concerned with the transmission and documentation of data regarding the transportation of cargo, including documents such as transfer orders, shipping documents, such as the bill of lading, and customs declaration as well as the appropriate status and tracking information. Actors involved with logistics IT constitute a large and opaque network of proprietary online services. In the maritime domain, the most prominent services are *port community systems*, being communication hubs for businesses and agencies involved with a specific port and those implementing electronic customs processes. Most shipping documents have been replaced by digital counterparts and are now being handled by these systems [9].

The fact that all cargo movement through ports, i.e., a large part of all cargo entering and leaving an economic area, is controlled by logistics IT systems and documentation is almost completely digitized makes them a worthwhile target for a wide range of malicious actors, including governmental actors. Transmission, storage and processing of the appropriate data as well as the identities of their originators and participants must be protected from adverse influence.

From a technical point of view, establishing secure encryption and authentication is straightforward as there are no major limitations such as processing power, memory, storage or data rates. However, with the network operating globally and the constituting systems being implemented as proprietary closed source systems not following common standards or guidelines, the establishment of a baseline for their protection will prove challenging. Standardization is limited to low level data formats such as X12, EDIFACT or XML and network protocols such as HTTP and FTP. Moreover, many processes are primary social processes: trust and reputation plays a major role. Many companies proposing technical solutions failed.

In this paper, we examine the recent discontinuation of the blockchain-based platform TradeLens developed by IBM and Maersk, where many obstacles of maritime logistics have been addressed. With the discontinuation there are lessons to be learned and there is room for new approaches. We elaborate important cryptographic properties and discuss some issues of a global maritime logistics infrastructure. In particular, we address three points: (1) Centralization, federation and power struggles within the network; (2) zero-knowledge properties and applications for maritime logistics; (3) the use of post-quantum secure cryptographic primitives.

The paper is structured as follows. In Section II we discuss TradeLens from a high-level perspective. In order to understand the details, we give a brief overview over some technical aspects of maritime logistic processes as well as blockchains and smart contracts in Section III. In Section IV, we given an overview of cryptographic issues and system requirements. Afterwards, we discuss centralization, federation and power in Section V, zero-Knowledge in Section VI and post-quantum

cryptography in Section VII. Section VIII contains a conclusion.

II. TradeLens

The TradeLens service was officially announced in 2018 and aimed to increase the efficiency of shipping companies and logistics [1] by providing a central platform where parties such as logistics personnel, customs and customers can manage information, e.g., where a container is located, its status of the documents, etc. TradeLens had over 1.000 participants, including five of the biggest shipping companies, over 230 ports and 45 international carriers in the US, and customs in 16 countries. But this was not enough for TradeLens to be profitable. In 2023, the service was discontinued. The concrete reasons for the discontinuation of TradeLens have not been made public; officially TradeLens was discontinued because the full global industry collaboration required had not been achieved and financial expectations had not been met.

Rather than an open network of anonymous participants, IBM and Maersk proposed a permissioned network called Hyperledger [2], a blockchain-based distributed ledger which is promoted with built-in security, automatic execution of *smart contracts*, easy tracking and information exchange, with the aim of establishing trust in a network of known participants.

Faults of the chosen technology may be seen in the fact that Hyperledger is a *permissioned blockchain*, i.e., access to it is controlled by a single administrator, which also serves as the certificate authority, storing and issuing the digital certificates of all participants. Usually, Hyperledger allows the creation of *channels*, which are private "subnets" on the blockchain created by members for private transactions. In the case of Hyperledger, however, this functionality was heavily restricted. As a result, IBM and Maersk gained significant advantage over competitors by being able to withhold or revoke access at will, and analyse the market from the data stored on their servers. Furthermore, they also utilized *off-chain data storage*, where only links to data are stored on the blockchain; the actual data is stored elsewhere in private databases. Additionally, this system aimed to fully replace, instead of augment and improve, established workflows and required every participant to adopt the new system immediately. In an industry that only slowly adapts to change, this is a significant disadvantage and hinders adoption.

III. Maritime logistics

In this section, we give a brief overview over some technical aspects of maritime logistic processes as well as blockchains and smart contracts. Section III-A and Section III-B show typical maritime transport messages / processes. Afterwards, we give an introduction into blockchains and smart contracts in Section III-C and Section III-D, respectively.

A. Exchange of EDIFACT messages

Within an operation, several different computer-processable messages and documents specific to the shipping industry are exchanged. The use of standards (such as EDIFACT or X12) defining structured messages, each with a specific objective, enables the involved parties to exchange transactions in a unified notion. They are designed for automatic integration in management systems.

The following example is a booking flow based on an exchange of EDIFACT [12] messages between the freight forwarder or customs agent and consignee. It allows forwarders and shippers to book a space from shipping lines for the content to board and receive the pertinent answers.

1) The freight forwarder or customs agent asks the consignee or shipping line to book space using an IFTMBF (International Forwarding and Transport Message Firm Booking) message with its booking function.
2) The consignee confirms the booking with the forwarder and customs agent using an IFTMBC (International Forwarding and Transport Message Booking Confirmation) message.
3) The forwarder sends the booking instructions with an IFTMIN (International Forwarding and Transport Message - Instructions) message to the consignee.
4) After boarding the freight, the consignee issues a draft bill of lading to the forwarder using an IFTMCS (International Forwarding and Transport Message Contract Status)

Often, (and despite the age of EDIFACT, which has been standardised in 1988) even this process is avoided and data is directly exchanged via email in which case confidentiality and integrity cannot be guaranteed. This illustrates how slowly the industry adapts to new or overly complex systems.

B. The bill of lading process

The bill of lading is an essential document in maritime logistics, used for the shipment and transfer of goods across international borders. The document serves three purposes: (1) It confirms that the carrier has received the goods in good condition. Any damage or shortage is noted on the document. (2) It is a contract between the shipper and the carrier, defining the terms and responsibilities related to the transport of the goods. (3) It grants the holder the right to claim the goods, facilitating trade and financing during transit. The document can be negotiable (order and bearer bill of lading) or non-negotiable (straight bill of lading). The first permits that the bill can be transferred to another party, allowing the transfer of ownership of the cargo. The latter states that the goods are consigned directly to the named consignee. In the case of a negotiable bill of lading, ownership may change, even multiple times, during the shipping process.

Fig. 1 illustrates the relation based on information flow among the parties in an usual bill of lading process. The process consist of the following steps.

1) Issuance of the bill of lading:
   a) The shipper prepares the cargo and provides shipment details (e.g. cargo type, weight, consignee, destination).
   b) The carrier receives the goods and issues the bill of lading once the cargo is loaded onto the ship or handed

DOI: 10.5281/zenodo.17120601

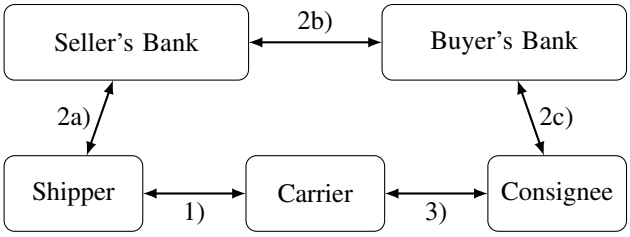

Fig. 1. Bill of lading process

over to the carrier for transport. The carrier signs the document, confirming receipt of the goods in good condition.

2) Transport of goods and transfer or endorsement (if negotiable) of the document:
   a) The shipper provides the bill of lading to the seller's bank in exchange for payment.
   b) The seller's bank then provides the bill to buyer's bank,
   c) which provides the bill to the consignee.

   During transport to the destination port, the bill of lading serves as proof that the carrier is responsible for delivering the goods in the same condition to the consignee. If the bill of lading is negotiable, the shipper can endorse it to a third party, often the buyer or a financial institution. This endorsement allows the goods to be sold or financed while in transit. The document can be transferred multiple times, depending on agreements.
3) Arrival at destination and release of goods:
   a) Upon arrival at the destination port, the consignee (or their agent) must present the original bill of lading to claim the cargo.
   b) The carrier verifies the bill of lading and ensures that the consignee is authorized to receive the goods.
   c) After verification, the carrier releases the goods to the consignee.

   If the bill of lading or cargo is lost or damaged, additional documentation may be required before the cargo can be released.
4) Final settlement:
   a) After the goods are delivered to the consignee, the bill of lading serves as a record of the transaction.
   b) It may be used to settle final payments for the shipment, especially when payment is contingent upon delivery or transfer of the bill of lading.

C. Blockchains for maritime operations

With the rise of digitalization, traditional paper-based bills of lading are being replaced by electronic equivalents, providing faster processing times, greater transparency and traceability. This opens the opportunity and need to introduce cryptography. Many studies examine the state of the art of the electronic bill of lading, as well as the impact of blockchains on specific maritime operations (cf. e.g. [7, 3, 10]). However, often it remains vague which problems are addressed and by which means they are resolved; the notions of blockchain and cryptography are often conflated. One has to distinguish different types of blockchains and their (cryptographic) properties.

Public Blockchain: Open, permissionless networks anyone can join. Examples are Bitcoin and Ethereum. Uses public-key cryptography for identity and transaction signatures, hash functions to link blocks securely, and consensus algorithms (like proof of work) to ensure trust without central authority. Proof of work consensus implies high electricity consumption.

Private Blockchain: Permissioned networks restricted to known participants, usually within an organization. Also uses public-key cryptography and hashing for data integrity, but access control is enforced through permissions and authentication. Faster consensus algorithms like Practical Byzantine Fault Tolerance are common, though electricity consumption is still high.

Consortium (Federated) Blockchain: Controlled by a group of organizations, not fully public or private. Combines public-key cryptography, hashing, and controlled consensus mechanisms, where only approved validators participate, ensuring privacy and efficiency.

Hybrid Blockchain (sidechains, crosschain or interchain): Linking of several blockchains, so that a transfer of assets, tokens or data between different blockchains is possible. Examples are Polkadot, Wanchain and Kadena. The connection can be between private or public blockchains, as well as between both blockchain types across. In this way it combines public and private blockchain features, allowing selective transparency and privacy. Hybrid blockchains enable cross-blockchain registers and calculations and public blockchains could access the restricted data of the private blockchain for certain applications.

While blockchains are cryptographically secure by design, it is possible to design a cryptographically secure system without blockchain; it is important to differentiate between this.

D. Smart Contracts

Modelling the shipping process as a protocol brings the association of implementing smart contracts, i.e., an algorithm on the ledger which automatically executes payment when certain conditions are met. These smart contracts document the business processes. The code and the agreements contained therein exist across the (distributed) blockchain network. Smart contracts have been implemented on the Hyperledger. As it is unlikely that smart contracts on a distributed public ledger is something the shipping industry will adapt to, as this implies that everyone can see the transaction including the parties involved and the value transferred, Hyperledger allows to keep transactions confidential and to share only selected data to other parties.

IV. Cryptographic issues and system requirements

In order to design the appropriate system, it is mandatory to specify the cryptographic requirements. However, as a socio-

DOI: 10.5281/zenodo.17120601

technical system it is mandatory to fulfil privacy, security and trust concerns.

A benefit of using a blockchain is the easier tracking and information exchange. All other security aspects are achieved by other cryptographic means: Encryption protects sensitive data, fraud is prevented via entity authentication, digital signature, zero-knowledge proofs and non-repudiation, data integrity is ensured by data authentication, etc. More specifically, many of the reported benefits do not stem from any specific blockchain properties but from increased digitization and information sharing as well as security properties such as protecting sensitive data, preventing fraud by offering non-repudiation and integrity of transmitted data or easily granting access to information to trusted authorities such as customs officials. These benefits are also offered by cryptography via the means of encryption, zero-knowledge proofs, digital signatures and variants of identity-based encryption, such as certificateless cryptography.

This can be achieved by a protocol built from standard cryptographic primitives; a blockchain is one possibility but not necessary. All the possible solutions we sketch in Section V can be built on top of the established EDIFACT standard or integrated into the bill of lading process outlined in Section III, ensuring that workflows have to be changed minimally. Any alternative system relying on blockchain technology has to necessarily fully replace established workflows, which will be hard in an industry that adapts to changes slowly. Moreover, not only technical issues have to be addressed. Maritime trade is governed by complex social processes and trust relations, which are hard to model appropriately. Consequentlty, we consider a decentralized or federated solution to be more likely to succeed.

V. Centralization, federation and power

A centralized system for a global market and huge and diverse ecosystem seems unfitting. A central obstacle is the centralization of power. In our view, a major issue of TradeLens was the centralization of data and power. Hyperledger is a permissioned blockchain, where access is controlled by the ledger administrator, utilizing off-chain data storage, where data is stored elsewhere and only linked to by the blocks in the chain. As such the implementation was more of a database controlled by IBM and Maersk, protected by public-key cryptography protocols. IBM and Maersk were able to decide who gets access to the network, revoke granted access and analyse the market. This is a significant dependency and disadvantage for competitors.

A decentralized/federated system is more promising. Decentralized means that each actor retains autonomy over decisions, no central authority makes decisions. Federated means that individual actors can consolidate themselves and act as one. Moreover, an approach based on the assumption that it is an anonymous network without trust is unfitting. There exist trustworthy entities in the network, not trusted by all but a selection of actors. Trust relations already exist by social experience in the shipping business or by the fact that they are state institutions and thus should be modelled by the system. A meaningful approach would be to see them as different interconnected networks with interfaces. Certificate chains can be built using the trusted entities and webs of trust can be cryptographically substantiated using digital signatures.

Possible approaches may be the following.

A. Web of trust

Public-key cryptography, as opposed to symmetric cryptography, offers the advantage that the key (used for encryption or verification) to be exchanged does not have to be transmitted via a secure channel, but is public.

One approach to transfer the key is the use a network of key servers to which anyone can upload public keys and from which anyone can retrieve the key of the person or entity with whom they wish to communicate. However, this results in the problem of untruly impersonation, i.e., that any person could publish a key with which they can impersonate someone else. Hence, there must be a mechanism to verify the authenticity of a key. One solution to this problem is to have the authenticity of a public key confirmed by a trusted authority using a digital certificate: In public key infrastructures (PKI), this is a certificate authority. This however gives huge power to the trusted authority and has been exploited in the past numerous times. Furthermore it is unclear who would play this role in the maritime trade sector, where distrust of competitors is huge. An alternative to the centralized and hierarchical trust model of a PKI is the decentralized trust model of the cryptographic concept of a web of trust. Here the participants assume the function of establishing the authenticity of the binding between a public key and its owner. In this way a web of trust can model trust relations between many different parties to share public keys without the need for a central authority.

Relating this to the bill of lading process outlined in Section III and Fig. 1, the involved parties already have established trust between each other where necessary and are able to securely exchange cryptographic keys via authenticated channels. Thus, they do not have any need for a PKI to store certificates for them, at least not in the case of a straight bill of lading. For negotiable bills of lading, however, where the consignee changes during the shipping process, trust has to be transferred between parties. When adopting a web of trust approach, each actor would store the other parties' public keys in a keyring and may elect to share them with other interested parties, which in turn may add them to their own keyring when trusting the source. This way trust can be moved transitively from one party to another, which could be used to, e.g., establish trust (via a public key exchange) between a final buyer and seller in the case ownership of a bill of lading changes during the shipping process. It could also be used to facilitate a public key exchange between parties that do not have any relations yet or no means to communicate securely directly via third parties.

We believe that this approach more closely models the reality of maritime trade, where no single authority is universally trusted and trust is instead distributed among many different

DOI: 10.5281/zenodo.17120601

parties, where some, like banks or especially large companies, are more trusted than others. Autonomy of all involved parties is preserved and they are not required to place additional trust, beyond what is already present, in a third party, possibly even a competitor.

B. Certificateless cryptography

Another approach to remove the complete reliance and thus the necessary trust in a single party to provide a PKI is certificateless cryptography, a variant of identity-based cryptography. Here the key generation process is split between two parties: a key generation centre (similar to a PKI) and the user. Thus no full trust in a PKI is necessary. Part of the final public key is provided by the key generation centre and the other part by the user, usually in form of a public string such as an email address or phone number. This also guarantees that the final public key generated by the user really belongs to the stated identity.

C. Decentralized blockchain

A truly decentralized (public) or hybrid blockchain as outlined in Section III-C could also work. The main downside to this approach, besides the high electricity consumption (which can be combated by employing zero-knowledge proofs, see Section VI), is that the whole industry would have to agree on a specific technology and adopt it at the same time. We believe that this constitutes a major challenge, that would be hard to overcome.

D. Federated smart contracts

Smart contracts don't neccessarily need a public ledger or a blockchain. A federated infrastructure agreeing on a standardized protocol of smart contracts is also possible. Contracts are then issued by a trusted instance, like a bank. In a naive way, one can think of the protocol in Fig. 1 as simple actions, e.g,. the shipper, the carrier and both banks have to sign the bill of lading specifying a specific token which later has to be provided by the consignee to obtain the goods. When the smart contract has terminated, there is no need to keep it infinitely long (only the usual time required by law).

Assuming the existence of a PKI, an established web of trust or implementation of certificateless cryptography, the process could be implemented as follows: Let pk_r be the public key of the consignee. The shipper and carrier generate a token via a cryptographic hash function, which is transferred to the consignee via the two involved banks after they confirm that the monetary transaction has succeeded. Upon arrival of the goods, the consignee now has to provide the token as well as a valid signature, which the carrier can verify using pk_r. To facilitate negotiable bills of lading, we need an update mechanism for the public key. This could be done as follows: Shipper and carrier compute a nonce (only usable once), which is transferred with the token via the seller's bank to the buyer's bank, which may in turn use it to update the public key and thus change the consignee.

VI. Zero-Knowledge

Besides strong security on the network level, the system level and in the supply chain, some services and complex freight documents require strong authentication on the application layer as well as mechanisms such as *zero-knowledge proofs* [6], e.g., to allow for signage and attestation of legally binding documents such as the bill of lading. A zero-knowledge proof is a protocol in which one party (the prover) can cryptographically convince another party (the verifier) that some statement is true, without conveying to the verifier any information beyond the fact that the statement holds.

A basic ingredient is a *commitment scheme*, i.e., a cryptographic primitive that allows one to commit to a chosen value or statement while keeping it hidden to others, with the ability to reveal the committed value later. Commitment schemes are designed to be binding, meaning that a party cannot change the value or statement after they have committed to it. They may thus be utilized to implement smart contracts for straight bills of lading. A variant, *dynamic commitment schemes*, allow updating statement provided that (a subset of) the involved parties agrees on it, which can be used to facilitate negotiable bills of lading.

To deal with large data sizes, zero-knowledge Scalable Transparent Arguments of Knowledge (zk-STARKs) [4] have been introduced, which scale sublinearly in data size. As such they may, e.g., also be used in truly decentralized blockchain approaches to increase speed by vastly decreasing data transmission rates and input sizes and enhance privacy, while also vastly decreasing electricity consumption.

VII. Post-quantum Cryptography

It is important to keep adversaries capabilities in mind, when designing (distributed) systems. Choices of cryptographic primitives to matter and logistics IT systems should use long-term secure schemes. In this section, we discuss post-quantum cryptography.

In recent years, there has been a substantial amount of research on quantum computers. If this research succeeds in the construction of a large-scale universal quantum computer, this computer will break many of the public-key cryptographic systems that are currently considered secure [8]. When the encryption scheme is broken, a decryption attack can reveal confidential information; when the signature scheme is broken, an attacker can forge signatures corrupting the integrity of the system. To provide protection against an attacker having access to a quantum computer, a cryptographic system has to be post-quantum secure. Moreover, as the set of potential threat actors in the maritime domain includes foreign governmental agencies and organized crime, i.e., actors with substantial resources, the adaptation of post-quantum cryptography should be addressed in a timely manner.

The US' National Institute of Standard and Technology (NIST) standardized the key encapsulation mechanism (KEM) CRYSTALS-Kyber (now called ML-KEM) and the digital signature schemes CRYSTALS-Dilithium (now called ML-DSA) and SPHINCS$^+$ (now called SLH-DSA). The digital

DOI: 10.5281/zenodo.17120601

signature scheme FALCON was also selected for standardization.

Cryptographic attacks raise awareness of the fact that not only parameter sets, but also cryptographic primitives of deployed implementations may need to be changed in the future, if attacks are found. The ability to easily make such an adjustment in a protocol is called *cryptographic agility* and it is especially important for systems that are rarely replaced or hard to upgrade. Post-quantum secure logistics IT systems should implement schemes on the highest security level. Moreover, until enough confidence is established, hybrid (pre- and post-quantum) encryption is recommended. Unfortunately, proprietary software, a large number of stakeholders and a lack of regulation will presumably impede efforts aimed at the introduction of strong post-quantum cryptography to the field. In [5], we have started the research on deploying post-quantum cryptography in maritime systems.

VIII. Conclusion and future work

In this paper, we analysed the discontinuation of the TradeLens platform and discussed some cryptographic issues for new approaches to a global bill of lading infrastructure. We stress three points.

1) Networks have to deal with trust issues. Decentralized blockchain-based networks have high (electricity) cost and large data transmission overhead. Suitable solutions have to be worked out according to existing (social) processes and trust relations. In other words, we deal with complex system with many different actors, varying levels of trust, which is hard to model. For widespread success a decentralized/federated solution is necessary.
2) Confidentiality and integrity are central. We are convinced that zero-knowledge properties can be used to improve security and performance and can be used to create protocols for maritime trade.
3) Due to the risk of universal quantum computers breaking today's established cryptographic schemes, we propose that the used primitives are post-quantum secure. Post-quantum cryptography and cryptographic agility is needed to ensure long-term security.

In the future we want to develop and implement more concrete prototypes of secure protocols utilizing zero-knowledge proofs, that can be integrated into existing IT systems for maritime logistics for further testing.

Acknowledgements: We are grateful to the anonymous reviewers for their valuable comments that led to various improvements.

References

[1] IBM United States Software Announcement 218-524. *TradeLens, a Maersk and IBM solution, delivers a blockchain-enabled visibility and document management solution for container shipping that promotes more efficient and secure global trade*. 2018.

[2] Shubhani Aggarwal and Neeraj Kumar. "Hyperledger". In: *Advances in Computers*. Ed. by Shubhani Aggarwal, Neeraj Kumar, and Pethuru Raj. Vol. 121. The Blockchain Technology for Secure and Smart Applications across Industry Verticals. Elsevier, Jan. 1, 2021, pp. 323–343. DOI: 10.1016/bs.adcom.2020.08.016.

[3] Clarissa Amico and Roberto Cigolini. "Improving port supply chain through blockchain-based bills of lading: a quantitative approach and a case study". In: *Maritime Economics & Logistics* 26.1 (2024), pp. 74–104. ISSN: 1479-294X. DOI: 10.1057/s41278-023-00256-y.

[4] Eli Ben-Sasson et al. *Scalable, transparent, and post-quantum secure computational integrity*. Publication info: Preprint. MINOR revision. 2018. URL: https://eprint.iacr.org/2018/046 (visited on 03/10/2025).

[5] Daniel Berger et al. "Post-Quantum Cryptography for Maritime Systems". In: *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*. Aug. 2025, pp. 660–665. DOI: 10.1109/CSR64739.2025.11129991. URL: https://ieeexplore.ieee.org/document/11129991.

[6] Oded Goldreich and Yair Oren. "Definitions and properties of zero-knowledge proof systems". In: *Journal of Cryptology* 7.1 (Dec. 1, 1994), pp. 1–32. ISSN: 1432-1378. DOI: 10.1007/BF00195207.

[7] Kunpeng Li, Jun-Yeon Lee, and Amir Gharehgozli. "Blockchain implementation in the maritime industry: a literature review and synthesis analysis of benefits and challenges". In: *Maritime Economics & Logistics* 26.4 (2024), pp. 630–657. ISSN: 1479-294X. DOI: 10.1057/s41278-023-00280-y.

[8] Vasileios Mavroeidis et al. "The Impact of Quantum Computing on Present Cryptography". In: *International Journal of Advanced Computer Science and Applications (ijacsa)* 9.3 (2018). Number: 3 Publisher: The Science and Information (SAI) Organization Limited. ISSN: 2156-5570. DOI: 10.14569/IJACSA.2018.090354.

[9] Francisco Petronilho, Hugo Fonseca, and André Zúquete. "The state of the art of the electronic bill of lading". In: *F1000Research* (2022). DOI: 10.12688/f1000research.123856.1.

[10] Sunil Tiwari et al. "Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap". In: *Transportation Research Part E: Logistics and Transportation Review* 170 (Feb. 1, 2023), p. 103012. ISSN: 1366-5545. DOI: 10.1016/j.tre.2022.103012.

[11] UNCTAD. "Review of maritime transport 2024: Navigating maritime chokepoints". In: *Review of maritime transport* (2024).

[12] United Nations Economic Commission for Europe. *EDIFACT*. en. Standard E/ECE/DEC/I(43). United Nations Economic Commission for Europe, 1988. URL: https://digitallibrary.un.org/record/47333.