Maritime Blockchain Labs Topic Brief

Misdeclaration of Dangerous Goods

Blockchain for real.

wearebloc.io

Bloc. Labs

Contents

Introduction to Maritime Blockchain Labs

In 2018, Bloc, with the support of Lloyd's Register Foundation, launched the Maritime Blockchain Labs (MBL) initiative to investigate and assess the applicability of blockchain technology for addressing business challenges, and in particular safety, in the maritime sector. The vision of the labs was to bridge the physical/digital and industry/technical divides by designing, developing and deploying technical solutions in close partnership with the maritime industry. The objective was to increase the likelihood of creating impactful and scalable technology for the maritime sector focussing on the safety of engineered systems. Between April 2018 and December 2019, MBL took the lead on openly and collaboratively creating solutions and sharing them with the maritime community.

This MBL brief covers the third lab, focused upon the issue of misdeclaration of dangerous goods. Bloc had received multiple requests and comments from several industry actors that pointed to the challenge of misdeclaration of dangerous goods as a major issue with costly consequences for safety and life at sea. The following briefing provides an in-depth review of the topic context, problem area challenges and obstacles, the lab consortium, solution prototype design, development and testing, as well as results and findings. Further information on MBL can be found in a separate main report and other lab briefs.

Problem: The Misdeclaration of Dangerous Goods

Problem Background

Dangerous goods and hazardous substances are items that pose a risk to crew health and safety, to ships or pollution of the marine environment. The nature of these substances means that they need to be handled with special care and caution, for fear of adverse consequences to personnel, damage to property or environment. Some common substances that fall under this classification include fireworks, propane, gasoline, lighters, bleach, paint, aerosols, rat poison, and lithium batteries[1].

To address risks associated with the transportation of these materials, the International Maritime Organization (IMO) and its Convention of the Safety of Life at Sea (SOLAS)[2] as well as its Convention for the Prevention of Pollution from Ships (MARPOL 73/78)[3] mandated the use of the International Maritime Dangerous Goods (IMDG) Code. This code was developed by the IMO as the international guideline on the safe transportation or shipment of dangerous goods and hazardous materials by sea. The code provides "detailed recommendations for individual substances, materials and articles, and a number of recommendations for good operational practice, including advice

1 Worksafe (2019), Commonly used dangerous goods. https://www.worksafe.vic.gov.au/commonly-used-dangerous-goods

2 IMO (2020), International Convention for the Safety of Life at Sea (SOLAS), 1974. http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

3 IMO (2020), International Convention for the Prevention of Pollution from Ships (MARPOL). http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-(MARPOL).aspx

on terminology, packing, labelling, stowage, segregation and handling, and emergency response action"[4]. It aims to protect crew members and prevent marine pollution in the safe transportation of hazardous materials. Furthermore, its use is intended to extend beyond seafarers to all those involved in industries and services connected with shipping.

Handling and transporting dangerous goods is a complex task involving multiple actors and cross-jurisdictions. Continuously tracking and monitoring the contents of containers demands cooperation with a high level of data interoperability and information sharing. Misdeclaration of dangerous goods occurs when these goods have been incorrectly described, weighed, measured, and/or counted[5]. An estimated 6 million shipping containers contain dangerous goods, nearly 1.3 million (22%) of which are not properly packed or are incorrectly identified. If misdeclaration occurs and results in another individual or organisation shipping dangerous goods without knowing it, the risks of detrimental situations arising increase substantially; for example, explosive or heat-sensitive cargo must be stowed well away from crew quarters and kept away from hot areas like fuel bunkers and engines[6]. Should proper handling and storage protocols not be followed, ship operators take on increased risks associated with unknown chemical contamination, fire, poisoning, and additional personal health and safety issues.

Widely referred to as the 'iceberg' risk in the maritime industry, this is a large and growing concern for all industry stakeholders with a 65% increase in misdeclared dangerous goods in 2015[7]. According to the Cargo Incident Notification System, up to 25% of all serious incidents and fires on board containerships are attributable to misdeclared cargo. A serious fire occurs every 30 days at sea, with the number of reported incidents trending upwards. In 2018, there were 174 reported fire incidents, an increase from the previous year.

---

4 IMO (2018), IMDG Code, 2018 Edition (Publishing Brief). http://www.imo.org/en/Publications/Documents/IMDG%20Code/IMDG%20Code,%202018%20Edition/IL200E.PDF

5 OOCL (2020), Rule 24 - Misdeclaration of Cargo. https://www.oocl.com/eng/ourservices/eservices/tariffandrates/globalrule/Pages/rule24.aspx

6 Allianz Global Corporate & Specialty (2019), Safety and Shipping Review 2019. https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/AGCS_shipping_review_2019.pdf

7 Allianz Global Corporate & Specialty (2018), Safety and Shipping Review 2018. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2018.pdf

The cost range associated with a fire onboard a vessel, or worse a total loss of a vessel, could amount to approximately 4 billion USD[8], while packing failures alone result in an estimated annual supply chain loss of 500 million USD[9]. For example, the 2018 Mærsk Honam fire resulted in the loss of five crewmen and an estimated financial loss of 430 million USD, with reconstruction costs alone amounting to 30 million USD[10]. Though not confirmed as the cause, Mærsk believed that dangerous goods were implicated in the severity of the fire onboard[11]. Indeed, an estimated 66% of cargo damage across freight modes, including container fires, is attributable to poor packing and labelling of dangerous materials[12]. Even if no physical loss or damage occurs, the non- or mis- declaration of goods can cause delays or result in the confiscation of the goods, invalidate an export licence, or result in customs fines, duty payments, and regulatory investigations, all of which have adverse financial implications.

In response, multiple shipping lines (including Evergreen, Maersk Line, Hapag-Lloyd, Hyundai Merchant Marine and OOCL[13]) have declared their intent to impose high fines between 15,000 to 35,000 USD per container[14] for shippers and the strengthening of inspection procedures. Hapag-Lloyd stated that failure to properly declare such cargoes is a violation that may be subject to monetary fines and/or criminal prosecution under applicable law: “To ensure the safety of our crew, ships and other cargo onboard, Hapag-Lloyd holds the Shipper liable and responsible for all costs and consequences related to violations, fines, damages, incidents, claims and corrective measures resulting from cases of undeclared or misdeclared cargoes”[15].

---

8 Allianz Global Corporate & Specialty (2019), Ibid.

9 Allianz Global Corporate & Specialty (2018), Ibid.

10 Insurance Marine News (2018), Reconstruction bill for Maersk Honam to exceed $30m. https://insurancemarinenews.com/insurance-marine-news/reconstruction-bill-for-maersk-honam-to-exceed-30m/

11 The Maritime Executive (2019), Rebuilt Maersk Honam Returns to Service as Maersk Halifax. https://www.maritime-executive.com/article/rebuilt-maersk-honam-enters-service-as-maersk-halifax

12 Allianz Global Corporate & Specialty (2019), Ibid.

13 Shipping and Freight Resource (2019), Shipping lines get tough on dangerous goods misdeclaration. https://shippingandfreightresource.com/dangerous-goods-misdeclaration/#

14 ForwarderLaw (2019), Carriers Levy Large Fines for Misdeclared Cargo. http://forwarderlaw.com/2019/10/28/carriers-levy-large-fines-for-misdeclared-cargo/

15 Ibid.

Marine insurers are also heavily impacted by the damages caused by the misdeclaration of dangerous goods. The International Union of Marine Insurance (IUMI) estimated that between 2000 and 2015, 56 containership fires damaged 8,252 containers, resulting in insurance payouts of over 1 billion USD. Furthermore, between 2000 and 2019, hull insurers paid out roughly 189 million USD for hull claims related to containership fires, most of which were believed to be caused by misdeclared goods. Speculations state that the increasing size of the containership industry is also expected to see an increase to the cost to insurers[16].

Problem Definition

Even with the introduction of fines and deterrents against misdeclaration, there are ongoing issues with large container ships, fires and misdeclared cargo. Some solutions exist that support sharing of information, but antitrust laws impede container lines from alerting competitors about rogue shippers or shipments. Despite innovation and technology advancements, industry stakeholders have voiced that these efforts are "not a panacea if the root cause of incidents and losses is not addressed"[17]. Some of these possible root causes, also expressed through this lab, include[18] [19]: (1) lack of adequate enforcement and adherence to regulations and guidelines for dangerous cargo; (2) avoidance of additional freight charges, or to circumvent rules and requirements on carriage of certain dangerous goods; (3) a lack of adequate training or awareness regarding how to properly package containers, or the compatibility of different cargo types in holds; and (4) the complexity and number of forms for dangerous goods documentation are difficult to fill out properly, and can vary drastically depending on IMDG Code and jurisdiction.

16 TradeWinds (2020), IUMI sounds alarm as cost of boxship blazes exceeds $1bn. https://www.tradewinds-news.com/casualties/iumi-sounds-alarm-as-cost-of-boxship-blazes-exceeds-1bn/2-1-755331

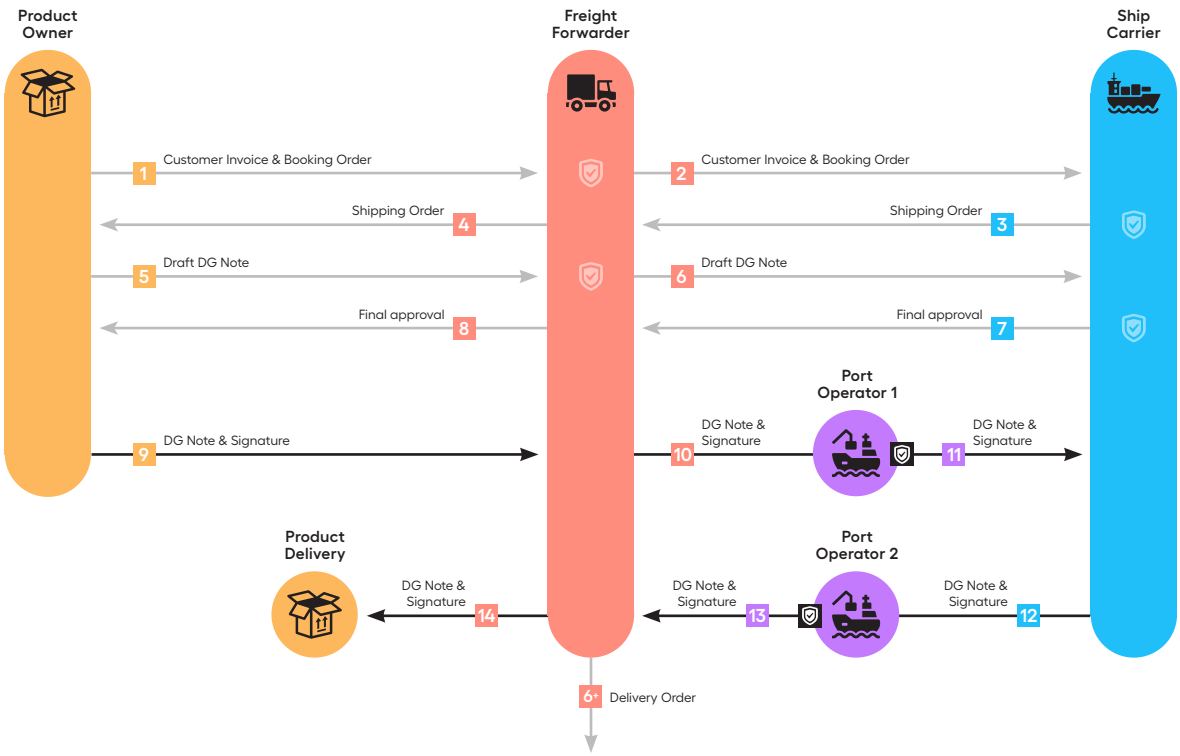
17 Allianz Global Corporate & Specialty (2019), Ibid.

18 Ibid.

19 Lloyd's List Maritime Intelligence (2019), Misdeclared cargoes accounting for more container fires. https://lloydslist.maritimeintelligence.informa.com/LL1129974/Misdeclared-cargoes-accounting-for-more-container-fires

Efforts to further define the problem area highlighted how the current process for declaring and transporting dangerous goods (see figure 1) is largely paper and email-based, requiring different actors to manually extract and input data into their separate systems, adding the risk of human errors. In some cases, additional information is required from the shipper or freight forwarder, which can cause delays and an unnecessary amount of interaction between supply-chain stakeholders. Furthermore, there often is a lack of oversight between what is declared on paper versus what is actually packed in the container to be shipped. Some ports and shipping lines are pushing for additional surveyor spot checks for suspicious containers and cargo, though others argue that this is not a feasible and practical solution to this problem.

Figure 1: Process Tracing for Misdeclaration of Dangerous Goods



Solution: End-to-End Digital Traceability of a Dangerous Good

Scope

Using the process tracing information, the vision of this lab was to utilise blockchain technology to create a prototype that traces the transportation of one dangerous good from end-to-end and registers all respective declarations for the dangerous good to focus on minimising misdeclaration and enable trust and efficiency gains regarding documentation handling.

The decision was made to exclude non-declaration (i.e. when shippers fail to declare their goods as dangerous or hazardous), as this was not something that could be addressed within the scope of the lab. An online consortium workshop conducted in June 2019 provided input that focused the scope towards the design of a prototype that:

1. Demonstrates an end-to-end delivery of a dangerous good and records all declarations, approvals and receivals along the way (which forms the basis of the chain of custody for insurance and trust); and

2. Investigates value propositions to all stakeholders in the supply chain to make shippers of dangerous cargo use such a prototype (which forms the basis of the feasibility of such a solution).

Prototype Design

The lab working group envisioned a solution that would discourage misdeclaration and support the proper documentation and declaration of dangerous goods. The resulting solution was foreseen to include the following elements:

- The prototype would require an electronic Dangerous Goods Note[20] to be filled out at point of origin and shared between supply chain actors to reduce human errors relating to documentation and updated as it was transferred with the cargo.

- This electronic Dangerous Goods Note would need to be electronically signed for and validated and verified through a cross-check of container contents (IMDG Codes) and packaging (UN Packaging Codes), and the customer invoice. This would eradicate the need for multiple QA checks throughout the supply chain.

- However, to cross-check and send and receive this information, many software applications would be necessary as each of these processes are currently handled in isolation. Therefore, some type of data adapter would be needed as an integration tool to connect various applications together, manage data flows to create a standardisation of data and connect to distributed ledgers (or blockchains). This would also automatise transactions between different parties, reducing the need to manually extract and input data into separate the data systems of each supply chain actor.

- The application of blockchain would provide an immutable chain of provenance for the shipment of a dangerous good. Hashed records of booking procedure, documentation, and signing off of handover between transport points for dangerous goods would be stored on a blockchain.

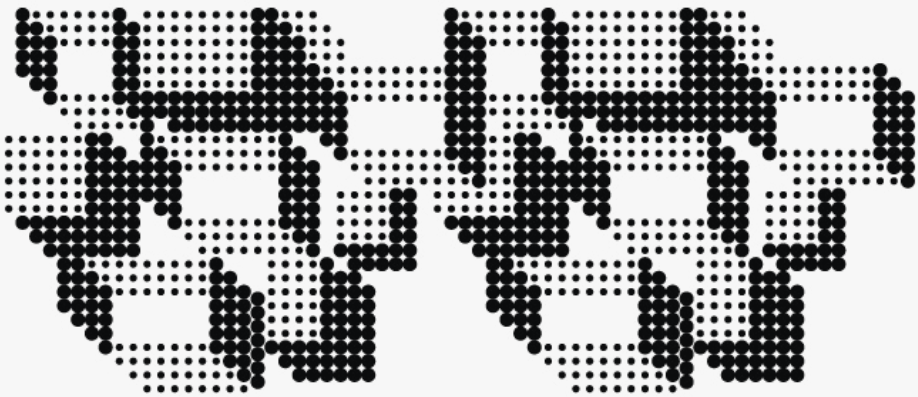
20 A Dangerous Goods (DG) Note is a form completed by individuals or companies who are exporting dangerous goods. It contains all the hazardous information required to be able to transport the goods in a safe manner.

What is a data adapter?

A **data adapter** is a tool that allows for integration and communication between multiple systems. It has two primary functions: (1) gathers and standardises data from multiple sources into one combined output dataset, and (2) writes changed data from the dataset back to the data source. A data adapter is configurable to allow specification of what data to move into and out of the dataset[21].

In practice, and for the purpose of demonstrating this end solution, the prototype had four primary features:

1. User roles for a dangerous goods supplier, a freight forwarder, a port operator, shipping container line, and technology providers;
2. Permissions, rights and actions associated to each user in the shipment process;
3. A digital signing feature before passing the dangerous goods to the next user; and
4. A timestamped hashed record of user actions.



21 ADO.NET Data Adapters (n.d.). http://diranieh.com/Netado/DataAdapters.htm

What are timestamps and hashes?

Timestamps are records of the time and date of a transaction. Timestamping is a technique used to prove the existence of certain digital data prior to a specific point in time. The advent of cryptocurrencies and blockchain enables some level of secure timestamp accuracy in a decentralised and tamper-proof manner[22].

Hashing is the function of mapping data to tables of data. The values are used to index a fixed-size table called a hash table[23]. Digital data can thus be hashed and the hash can be incorporated into a transaction stored in the blockchain, which serves as evidence of the time at which that data existed[24].

Demonstration and Testing

We then demonstrated the prototype with consortium members to simulate an end-to-end documentation and shipment of a dangerous good, recording relevant document details, receivals and handoff digital signatures. The foreseen process flow with the prototype when aggregating the above features can be seen on the following page.

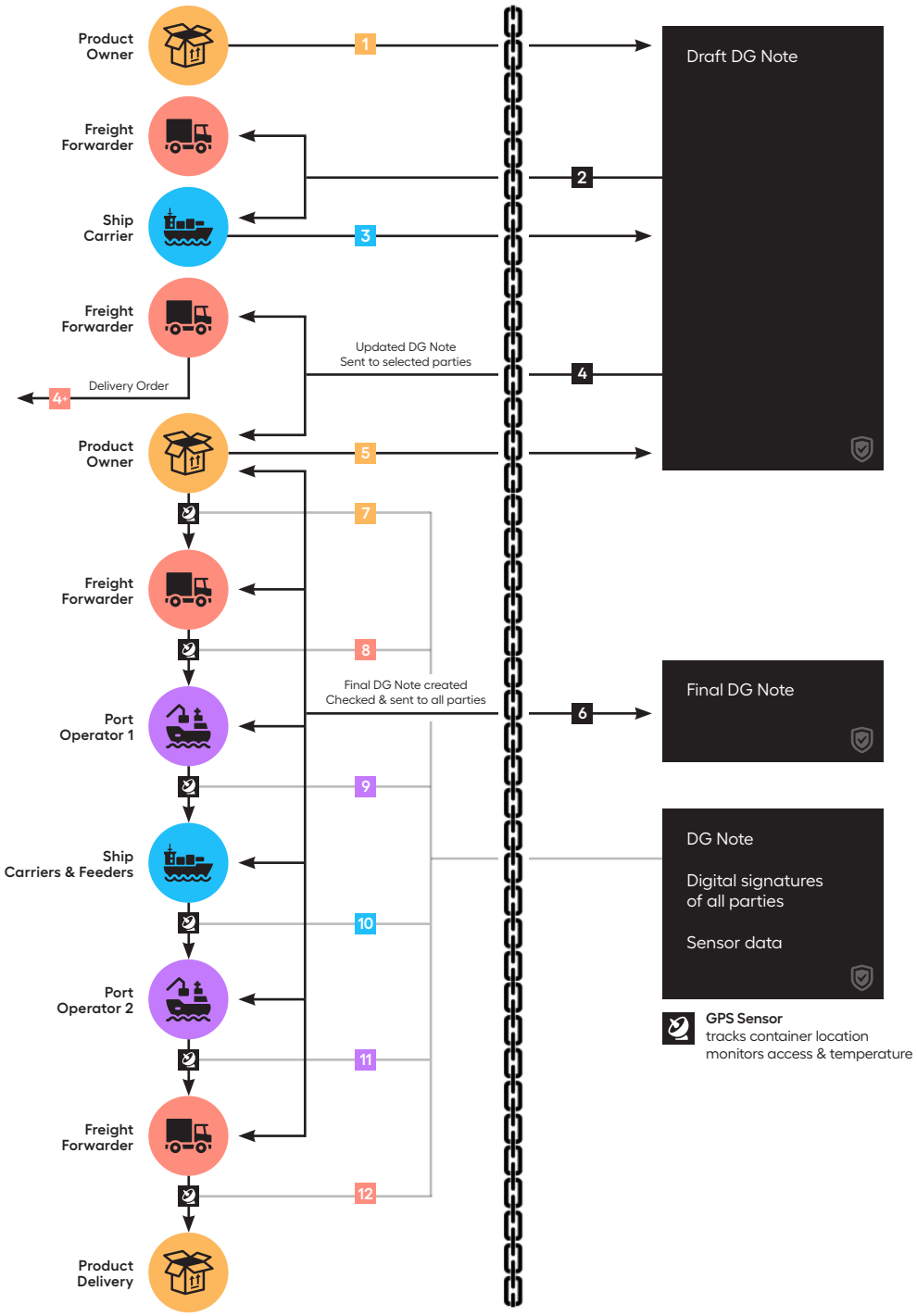
22 Kolydas, T. (2019), Timestamping Metadata Using Blockchain: A Practical Approach. In: Garoufallou E., Fallucchi F., William De Luca E. (eds) Metadata and Semantic Research. MTSR 2019. Communications in Computer and Information Science, vol 1057. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-36599-8_42

23 BlockGeeks (n.d.), What is Hashing? [Step-by-Step Guide-Under Hood Of Blockchain]. https://blockgeeks.com/guides/what-is-hashing/

24 Gipp, B., Meuschke, N. and Gernandt, A. (2015), Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. In Proceedings of the iConference 2015. March 2015, Newport Beach, California. https://arxiv.org/abs/1502.04015#

Step	Action	Hash Record to Blockchain
1	Product owner (i.e. shipper) sends request to a selected freight forwarder with a customer invoice and booking order (CI & BO). • Documents are internally checked and automatically pushed and validated through Hazcheck. • Once verified, the documents are sent to the freight forwarder.	Customer invoice Booking order Shipper digital signature Hazcheck verification Timestamp of event
2	Freight forwarder receives pre-checked docs, accepts order and pushes the documents to a selected carrier.	Freight forwarder digital signature Timestamp of event
3	Carrier gets pre-checked docs, accepts order and sends back shipping order (SO).	Shipping order Carrier digital signature Timestamp of event
4	Forwarder and product owner receive SO, and forwarder gets automatic generation of Delivery Order (DO) for truck driver.	Delivery order Timestamp of event
5	Product owner back last details for order, which auto-populates the final dangerous good note. • Documents are automatically pushed and validated through Hazcheck. • Once verified, the documents are sent to all parties.	Final dangerous goods note Hazcheck verification Digital signatures of all parties to confirm receipt Timestamp of event
6	Freight forwarder records sign off at transfer of DG cargo from product owner.	Product owner digital signature Freight forwarder digital signature Timestamp of event
7	Port authority (loading) records sign off at transfer of DG cargo from freight forwarder.	Port authority digital signature Timestamp of event
8	Carrier records sign off at transfer of DG cargo from port authority.	Carrier digital signature Timestamp of event
9	Port authority (unloading) records sign off at transfer of DG cargo from carrier.	Port authority digital signature Timestamp of event
10	Freight forwarder records sign off at transfer of DG cargo from port authority and confirms delivery of cargo at destination.	Freight forwarder digital signature Digital signature of receiver at delivery point Timestamp of event

Figure 2: Prototype Solution for Misdeclaration of Dangerous Goods



Value Propositions and Business Model

After the demonstration we gathered feedback from the consortium as to the value they perceived the application would have. These value propositions would be shared across the dangerous goods supply chain and included:

- **Product owner or shipper** (i.e. dangerous goods supplier), using the trusted application would offer a form of credibility. They can avoid delays for shipping cargo to their buyers, due to mistakes in documentation, as well as have faster booking and documentation processes overall. In addition, the application would provide the shipper with the ability to showcase product and supply chain provenance.

- **Freight forwarders**, they could be whitelisted as a trusted intermediary and offer faster processing via the auto-population of legal documentation and booking forms. The solution also would allow the freight forwarder the ability to showcase supply chain provenance.

- **Shipping Liners and Carriers** would have peace of mind knowing for certain what they are transporting and can take appropriate measures for handling. The audit trail for shipments would allow for whitelisting and building reputations for trusted stakeholders in the supply chain, making it easier to identify potentially rogue shippers. The early sharing of dangerous goods information would help to avoid delays for cargo and can support faster processing via the auto-population of legal documentation and booking forms. Importantly, the solution would provide the carrier with the ability to showcase supply chain provenance.

- **Port authorities** would have peace of mind knowing for certain that dangerous cargo is being handled appropriately within their jurisdiction. They would also benefit from faster administrative processes, which enables the port to operate efficiently and safely, as well as provide full transparency towards state authorities for inspections.

Digitalisation of the dangerous goods information and its exchange between supply chain actors via the data platform would help to reduce human error, save time on documentation and correspondence, support efficiency gains,

save working hours, avoid fines for misdeclaration and delays, and avoid costly incidents onboard.

The business model for the prototype was envisioned as a software as a service (SaaS) application for actors within the dangerous goods supply chain. Monthly fees could be applied to different actors along the supply chain for API integration, and/or transaction fees could be based on individual container shipments. The underlying blockchain element of the solution is open source but the application built on top of it and the data generated would be private and commercially operated. To scale the solution, an offer was made to the consortium as first mover users and investors. These first movers would benefit from reduced fees and were offered equity in the proposed venture. Over time, the solution would be able to provide transparency regarding the historical actions of all actors, creating a whitelist of trusted suppliers, freight forwarders, shipping lines, and ports that can competently and securely handle the transport of dangerous goods. With this information, additional business models could evolve into other applications, to better enable insurance of dangerous goods cargo, handle incident claims and charges, and support enforcement of trade restrictions and bans.

Key Findings

Multiple consortium members voiced their support for the joint effort to tackle the upstream issues and root causes of misdeclaration of dangerous goods.

Required Participation from Carrier

Multiple lab members identified the absence of a carrier or shipping line in the consortium as a key challenge and weakness as it limited the holistic perspective needed to address this complex problem. While significant efforts were made to fill this role during the formation of the consortium, they were ultimately unsuccessful. This absence negatively impacted the overall problem definition, solution validation, and business model scoping as shipping lines and container carriers play an essential role in the transport of these goods and their documentation flow (see figure 1).

Verification of Physical Goods Needed

Another challenge was that the solution prototype did not have a means to securely and concretely verify what and how a product is packed into a container. Existing practices rely on trust in product owners and their ability to pack, fill and document a container correctly. It was suggested a surveyor could attend at the point of origin to confirm and sign off on the quality assurance for packing and labelling of the dangerous goods shipment; however, the practicality of this was challenged and members suggested alternatives such as assessing whether the supplier was ISO certified or if an employee overseeing this task had certification or training experience in the handling of dangerous goods. It was agreed that this should be a topic to be decided upon in the next phase of product development.

Defining Data Security and Permissions

Data security and permissions would need to be clearly defined for this solution to be trusted and adopted by the market. Not all parties may want to or can share their data, let alone have it displayed or pushed through the solution and recorded on the blockchain. Though the Dangerous Goods Note that gets passed through the supply chain currently has specific information that all parties can and need to see, there may be additional details that each actor along this supply chain may need in addition to what's provided in the document. It became clear that identifying key data points required by various stakeholders, as well as data privacy and agreements on data exchange would also need to be discussed and addressed.

Successful Combination of Technology

Regarding the technical development of the prototype, we successfully combined technology providers and their respective technologies (i.e. MTI Adapter, Exis Technologies HazCheck and SecureSystem container sensors) together to create a prototype solution. This combination demonstrated the ability to increase transparency and smooth the communication of important dangerous goods information between previously separated parties.

Collaboration Leads to Efficiency Gains

Recognising that dangerous goods represent over 10% of all goods shipped globally, one of the key opportunities identified and explored during this lab is the potential to achieve efficiency gains by utilising such solutions. As the prototype and the MTI Adapter supports agnostic integration (so a platform can interface with any type of operating system and database), it effectively acts as a complementary rather than competitive addition to existing technology solutions, such as HazCheck and SecureSystem sensor technology. It also enables various forms of integration (API/EDI) between different data systems, using algorithms to offer a flexible approach towards connecting the various stakeholders onto one data exchange platform.

Discussion

Without actually performing the integrations between these technologies, we developed a prototype that mimicked system integrations to showcase what a new process for data sharing of dangerous goods information could look like. Having requested example documentation from consortium members, we also imitated sending and digitalisating these documents in an attempt to showcase how the solution would look and act in practice. The documentation examples also served to provide a better understanding of how diverse dangerous goods documentation is and how the proposed solution would benefit particular stakeholders.

Additional benefits identified through the demonstration of the solution prototype highlighted the possibility to avoid delays and high carrier fines, mainly through automated transmission and updating of dangerous goods information and data to individual supply chain actors. This also enables such stakeholders to prepare well in advance of the shipment arriving in their jurisdiction or work area. Critically, such preparations help to increase safety across the supply chain, on land, at port, and onboard vessels at sea.

In addition, such a solution was seen to offer the opportunity to develop a trusted certification of properly documented dangerous goods with possible insurance applications. By taking appropriate measures to increase safety and security, as well as improve traceability across the supply chain via active participation in electronic documentation processes, there is the opportunity to reduce burdens for insurers with respect to costly claims management. Furthermore, if more goods are correctly labelled and, therefore, properly handled during shipment, this could lead to reductions in insurance premiums on the shipment and transport of dangerous goods. The latter would also make such insurance coverage more affordable and attractive for those currently operating without insurance.

Conclusion

Overall, this lab showcased how the design and development of a prototype solution can reimagine existing processes and propose new methods for supply chain communication and cooperation. The active participation between industry stakeholders saw the implementation of a collaborative approach to solving network-wide problems, as well as the design and validation for a proof-of-concept. We managed to incorporate and represent a diverse set of industry perspectives covering the majority of the supply chain. The resulting solution prototype provided a case for increased transparency and efficiency gains. More information regarding the next steps of this lab and efforts for further development are described in the main report.

Appendix: Industry Consortium

The process tracing exercise for bunkering helped to identify the type of stakeholders that should be included in the consortium. After reaching out and garnering interest in MBL, a consortium was brought together to (1) bring industry expertise and process knowledge; (2) design an initial prototype to demonstrate proof of compliance with requirements (technical, operational, human) in a simulated setting; and (3) provide feedback while assessing the value propositions to their operations.

Representatives from the following organisations took part in the MBL lab:

Agility Global Integrated Logistics offers ocean, air and road freight, warehousing and distribution, and integrated supply chain services in more than 100 countries. Agility represented the perspectives and insights of transporters of dangerous goods, and helped to assess potential impacts on operations and ability to ship dangerous goods.

Port+ is a business partner for companies serving ships and terminals in the port communities of Belgium and Zeeland. Port+ provided early insights, including knowledge into the process of declaring dangerous goods to Port Authorities.

Flexport is a digital freight forwarding and customs brokerage company. Flexport provided insight into the process of shipping and documenting dangerous goods, and helped to assess potential impacts on operations and ability to ship dangerous goods.

Marine Transport International (MTI) specialises in moving cargo around the world, bringing technology and logistics together. Their Adapter solution is an open modular integration tool that allows teams to create, connect and manage distributed ledgers, enterprise DLT networks, smart contracts, data mapping and data flows. MTI provided technical expertise and knowledge relating to the transport of dangerous goods.

Exis Technologies is the leading supplier of compliance systems for the management of dangerous goods in sea transport. Exis Technologies and their solution HazCheck provided knowledge and input on the declaration of dangerous goods and required documentation verification processes.

SecureSystem and their sensor technology delivers an IoT-enabled supply chain intelligence solution for the security and integrity of shipments. SecureSystem provided technical expertise and support relating to active monitoring of dangerous goods container shipments.

Copenhagen-Malmö Port (CMP) is a full service port, and offers transport and logistics services as one of the largest port and terminal operators in the European Nordic region. CMP provided insights into how ports manage and monitor shipments of dangerous goods.

DSV is a global supplier of transport and logistics services and provides and manages supply chain solutions. DSV provided insight into the process of shipping and documenting dangerous goods, and helped to assess potential impacts on operations and ability to ship dangerous goods.

X-Press Feeders is the largest independent common carrier in the world, providing transportation services to container operators. X-Press Feeders provided knowledge and information relating to the shipment of dangerous goods between shipping liners.

Lloyd's Register Group (LRG) is a marine classification society and provides independent assurance, consulting, and advisory services. LRG participated as an advisor and advocacy partner.

Date
December 2020

Authors
Katrina Abhold and Deanna MacDonald (Bloc)
and Gary Pogson (Lloyd's Register Foundation)

Bloc and Lloyd's Register Foundation (2020).
"Misdeclaration of Dangerous Goods"
Maritime Blockchain Labs Topic Brief under grant no. XXXXX

Bloc. Labs

Lloyd's Register