TU Delft TNO

Design of a blockchain-based platform to support the availability of Entry Summary Declarations to European Customs

Matteo Di Benedetto

Page intentionally left blank

The design of a blockchain-based platform to support the availability of Entry Summary Declarations to European Customs

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Management of Technology**

Faculty of Technology, Policy and Management

by

Matteo Di Benedetto

Student number: 4848764

To be defended in public on August 24th, 2020

Graduation committee

Chairperson:	Prof. Dr. Y. (Yao-Hua) Tan, Information and Communication Technology
First Supervisor:	Drs. J. (Jolien) Ubacht, Information and Communication Technology
Second Supervisor:	Dr. M.Y. (Yousef) Maknoon, Transport and Logistics
External Supervisor:	Dr. B.D. (Boriana) Rukanova, Information and Communication Technology
External Supervisor:	Dr. Ir. W. (Wout) Hofman, TNO

Page intentionally left blank

Acknowledgments

This master thesis concludes my two-year experience as a student in the Management of Technology programme at Delft University of Technology. Leaving my home country and moving abroad was a challenging experience, but also a memorable journey. Therefore, I feel the need to thank who supported me during this adventure.

I want to start by expressing my gratitude to TNO for the big opportunity given to me to take part in such a project. The acknowledgements go in particular to Dr. Ir. Wout Hofman, who consistently monitored me and assisted me with getting the expertise I needed to carry out my research work. My appreciation also goes to Dr. Ir. Jok Tang, who helped me with settling up and continuously showed his support despite the unprecedented circumstances. A big thank goes to the colleagues from the Data Science department: being surrounded by such smart people was inspiring. Thank you also to Marteen Sies from IBM NL for reviewing my thesis report with such short notice.

This project would not have been possible without the support of my graduation committee. I want to thank Dr. Yousef Maknoon for his contribution, which helped me clarify the research structure. Likewise, the long-standing expertise of Prof. Dr. Yao-Hua Tan and Dr. Boriana Rukanova were crucial to deliver this comprehensive project. Lastly, I would not have been able to progress week by week without the constant and patient guidance of Drs. Jolien Ubacht who from the first day we met showed motivation and excitement: thanks to her supportive supervision, I gained the confidence and the skills I needed to complete this research.

My academic journey has come to an end. Thank you to all the people who supported me during the last five years: the memorable moments we shared shaped my identity. I want to conclude with a quote which best represents my feelings at the moment:

“Time flies and never returns. Memory stays and never departs”

Matteo Di Benedetto

Pratola Peligna, August 2020

Summary

To ensure the safety and security of imported goods, customs authorities perform risk assessment on goods arriving in Europe. A successful risk assessment is based on two pillars: good quality of data, and good availability of this data to customs. While the former is widely addressed in the literature (e.g., data pipeline, Digital Trade Infrastructure), the latter still has room for research. The primary document used during risk analysis is the Entry Summary Declaration (ENS): this document is submitted to the customs office of first entry (COFE) 24 hours before loading the cargo onto the vessel. On average, the customs office of first entry cannot correctly assess 60% of the incoming vessels because of missing ENS.

Several projects and technologies have been proposed to address the availability issue, among which blockchain technology (BCT). BCT is based on a decentralised network that performs transactions and stores them in blocks linked via cryptography. The potential advantages of this technology are the immutability of transactions, confidentiality, and availability. Insights from the literature show that BCT's application in the shipping industry has several problems: on the one hand, there are technological concerns towards a still new-born technology; on the other hand, the governance of a decentralised system raises organizational concerns. The research gap identified is missing empirical research on BCT, which requires design-oriented research. This brings to the MRQ:

> *"Which design of a* blockchain-*based platform can be developed to support the availability of Entry Summary Declarations to customs authorities for incoming cargo flows into the EU?"*

The research is conducted using the design science research methodology (DSRM), which is divided into several steps, from problem definition and design, to evaluation and communication. This framework was enriched with an additional sub-step that addressed organizational issues to obviate the framework's high technical focus.

During the first step of the DSRM, the AS-IS process has been analysed: the main result from this analysis was that deviations in the vessel's itinerary could lead to missing data. In the TO-BE process description, where a blockchain-based platform is used to support the Business-to-government (B2G) interactions between carriers and customs, the upload and update of

itineraries are proposed as a solution to give access permission to customs authorities to the correct ENS data. In the next step, the design requirements have been elicited using the TO-BE process description and literature on the data pipeline concept. This resulted in several requirements that addressed both functional aspects and security, integrity, and scalability constraints. The blockchain components had to be identified to design the architecture: through a literature review on blockchain taxonomy, several components were identified, namely network topology, data storage, consensus mechanism, and application. Each of these components had sub-components which provided design options.

The architecture has been defined using the sub-components. Carriers and customs authorities compose the peer-to-peer network. Carriers store the ENS document in an off-chain repository, encrypted using a symmetric key, and publish a reference on-chain, which contains a hash for integrity, and a Unified Resource Identifier (URI), to access the document. Carriers also upload and update their itinerary by publishing events on-chain, which will update the state of a smart itinerary contract. When customs want to access the ENS data, they will query the blockchain ledger, where their role in the itinerary will be assessed, and, eventually, the decryption key will be provided.

The platform was then evaluated by comparison with TradeLens, which is a blockchain-based platform supporting shipping processes. The result is that the ENS platform theoretically scores better than TradeLens in terms of scalability, security, trust, and immutability, identified in the literature as hindering factors. Nevertheless, the two platforms have different functionalities; thus, the main differences could be explained by the different underlying scope. From a governance perspective, the main result was that the governance structure does not influence technical choices, which are instead closely related to the business process.

This research contributes to several research areas. The first contribution is to the new Import Control System (ICS2) implementation: the blockchain-based platform provides technical improvements to the common repository by including a dynamic access control mechanism, such that only authorised parties can access relevant data, as well as technical immutability, since no parties would be able to tamper information once it is stored on the blockchain ledger. The second contribution is on research on blockchain: this research described how a

blockchain-based platform can be designed, providing insights for future design frameworks, defining network topology, data storage, consensus mechanism and application as key components, with their relative design choices. An important contribution is made to research on governance in blockchain contexts, where the relationships between governance and design are not clear: this research describes why the governance structure does not impact technical choices; instead technical choices are driven by the business process to be supported. Finally, this research contributes to research on B2G data sharing in blockchain contexts: the result is that the voluntary sharing of data from private firms to governmental organizations can be achieved only by aligning stakeholder interests.

The societal contribution of this research is mainly to customs risk assessment: with increased data availability, customs might improve risk assessment procedures, which would result in better identification of threats as well as higher facilitation of trade. This has two implications: on the one hand, better identification of risks would improve safety and security of the EU territory and decrease fraud cases; on the other hand, facilitating cross-border activities could boost global trade, with benefits for the economy as a whole. Additionally, this research can increase the awareness towards blockchain technology, which has the potential to improve several business areas as well as daily tasks, but as of today is not yet implemented at large scale.

Table of Contents

List of figures

List of Tables

Glossary

Architecture	Underlying components of the software and relations among them
Blockchain-based platform	Software based on blockchain technology
Carrier	Trade actor who performs the transport of goods by sea
Consensus mechanism	Procedure which regulates the validation of new transactions, before they are stored in the blockchain ledger
Consignee	Receiver of the goods
Consignor	Initial owner of the goods, who send the shipment
Cryptographic key	A parameter used to encrypt/decrypt information
Customs Authority	Authority responsible for controlling the import/export of goods and collect duties
Customs office of first entry	The customs office in Europe where the incoming vessel will stop first
Digital twin	A digital representation of a real-world object

Entry Summary Declaration	Document containing information on the cargo, buyer and seller
Event	An occurrence which represents a physical activity
Freight Forwarder	Actor who organises the shipment of goods
Governance structure	Which actors make up the organizational network around a platform, and their role
Member State	State member of the European Union
Node	A device which contains a copy of the blockchain ledger
Risk assessment	The process of identifying threats from traded goods
Smart Contract	A code which is executed if some predefined conditions are met
Trader	General term which refers to consignor, consignee, freight forwarder or carrier
Transaction	An operation executed on a blockchain ledger
Union Customs Code	Regulatory framework on customs procedures
Vessel itinerary:	The sequence of ports touched upon by a vessel, and the container loaded/unloaded in each port

List of abbreviations

BCT Blockchain Technology

CA Certificate Authority

CBM Coordinated Border Management

COFE Customs office of First Entry

COU Customs office at Unloading

CSSP Cross-sectorial social partnership

EC European Commission

ENS Entry Summary Declaration

ESB Enterprise service bus

EU European Union

FF Freight Forwarder

GUI Graphic User Interface

ICS (2) Import Control System (2)

IoT Internet of things

IS Information System

MoT Management of Technology

MS Member State

PBFT Practical Byzantine Fault Tolerance

PKI Public Key Infrastructure

PoA Proof of Authority

PAP Policy administration point

PDP Policy decision point

PEP Policy enforcement point

PIP Policy information point

PR Private Key

PU Public Key

RA Risk assessment

UCC Union Customs Code

UN United Nations

1. Problem statement

The European Union (EU) represents the major trading player worldwide, with a 15% share in the global trade and 4.5 thousand tonnes of goods imported and exported every minute (European Commission, 2018; DG TAXUD, 2018). To protect the Members States (MS) from risks linked with the transportation of goods and to check the compliance of traders with international requirements, the EU entrusts national Custom Authorities to execute risk assessment. The goal is twofold: customs should protect the European territory from terrorism, environment, economic and health threats, while at the same time facilitating international trade (Elmane-Helmane & Ketners, 2012; European Commission, 2010, 2018; Iordache, 2007).

The role of customs has evolved into an authority responsible for implementing policies which span from duties collection to the control of harmful products (Iordache, 2007; Widdowson, 2007). Globalization and changing economic landscape, together with revolutionary factors such as 9/11, have been significant factors towards the modernization of customs. After the Revised Kyoto Convention, in force since 2006, highly facilitated trading contexts have been promoted, producing an increment in global commerce, which eventually resulted in a higher workload for customs (Widdowson, 2007).

To achieve its objectives, customs perform risk assessment analyses to identify hazards and inspect goods (Iordache, 2007; Widdowson, 2007). In 2010, following the steps of US customs, the European Commission (EC) conducted a feasibility study on whether 100% scanning of imported goods would be beneficial (European Commission, 2010). The results showed that the financial burden to implement such framework on a global level would impact the worldwide economy in terms of €150 billion annually, while not substantially improving global security and disrupting trade (European Commission, 2010). The EU thus focused on improving risk management by introducing new technologies and management systems, by collecting information before arrival to and departure from the EU, and by improving the coordination of customs authorities within the community (European Commission, 2010).

1.1. Issues within risk assessment and document flow

The success of the risk assessment process is based on declarations data and the exchange of this information among customs. Goods moving within the supply chain are accompanied by several documents containing details related to the cargo: import and export declarations, for instance, include information such as buyer and seller, description and origin of the goods (Hesketh, 2010). According to IBM (2017), over 200 separate interactions and 30 organizations are involved for an average cargo from East Africa to Europe, producing a stack of paperwork close to 25 centimetres in heights (Allison, 2016). Given the amount of information exchanged during each communication, data can be altered, voluntarily or not, resulting in incorrect figures.

Considering the Import Control System (ICS), which manages and regulates the security declarations of goods imported in the European Union customs territory, low data quality and low data availability of Entry Summary Declarations (ENS), currently hinder proper risk management (DG TAXUD, 2017c). For instance, ENS contains information aggregated from other documents, which in turn contain information from other documents, undermining the quality of data provided to authorities (Hesketh, 2010). Another example is missing ENS documents: taking into account shipping traffic, which covers 90% of global trade in terms of volumes (International Chamber of Shipping, 2017), the ENS is sent for deep-sea containerized cargo[1] to the Customs office of First Entry (COFE) 24 hours before arrival; in case the itinerary changes and the cargo arrives first in a different customs, the latter will not have the ENS document to perform risk assessment. A 2012 study revealed that current operational methodologies do not provide enough information sharing among customs: in a

[1] General cargo – packages, boxes or pallets with particular products or other packages. Postal items and eCommerce shipments are considered as general cargo; Bulk cargo – cargo like edible oils, grains, sand, coals, that is transported without any added packaging materials; Containerised cargo – general – or bulk cargo transport in containers.

12-month period, over 36 million ENS were lodged, but the COFE requests for information from other Members States was 382 million (European Commission, 2013). This highlights how the rate of requests for additional information among customs is strikingly high. On average, the COFE cannot efficiently assess risks for 60% of containers (DG TAXUD, 2017c).

As a result, Customs Authorities have to inspect numerous cargos, resulting in lower efficiency, higher shipment costs and more delays throughout the trade lane. Research shows that 40% of delays are caused by the administrative burden imposed by authorities, which account for extra-costs in a range of 100–500 Billion US$ worldwide (Thomas & Tan, 2015). According to Grainger et al. (2018), customs incur costs for duplication of activities, unnecessary inspections, communications and lack of Coordinated Border Management (CBM), where customs authorities coordinate their activities to seek higher efficiency (Elmane-Helmane & Ketners, 2012; Rukanova, Huiden, et al., 2017). Ineffective risk assessment might have a detrimental impact on the European economy since it leaves room for fraud and irregularities, which undermine the socio-economic stability of the Union. Tax Fraud represents one of the most common irregularities: often, traders tend to undervalue the goods, or declare less volume, to pay fewer customs duties.

In 2018, the volume of customs declarations reached 332 million, with 1.8 billion tonnes of ship cargo checked by customs authorities (DG TAXUD, 2018a). In parallel, the number of fraud cases is increasing, causing losses in taxes in the order of tenths of billion euros per year in Europe only (Chang et al., 2020; European Commission, 2018). The need to find a solution to low data quality and missing information is urgent.

1.2. Possible solutions to improve trade-related documental flow

Focus on digitalization is expected to bring valuable benefits to risk assessment and global trade. According to the UN, digitalization of Asia-Pacific trade-related paperwork can potentially decrease costs by nearly 30% and boost export up to 200B€ yearly (The Economist, 2018). In 2008, Goldby stated that three main factors are impeding the process: “complexity of international sale transaction, the lack of an appropriate cross-border infrastructure and lack of urgency” (Goldby, 2008, p.140). As explained in the previous

section, the latter factor has changed during the past decade, whereas complexity has increased, making existing cross-border infrastructure unfit for the job.

To solve these issues, the EC developed, together with the MS, the plan Import Control System 2 (ICS2): the solution is to develop a Common Repository to make ENS information accessible to all relevant customs authorities (DG TAXUD, 2017c). Before ICS2, CORE, a European-wide project, aimed at improving trade security by establishing global trade lanes (CORE, n.d.). The essence of this project is to address data accuracy and completeness through the implementation of secure mechanisms for data collection and distribution (CORE, n.d.). Organizations involved in global trade are increasingly recognizing that to improve international trade, data fragmentation represents a key challenge and Digital Trade Infrastructures (DTI) could be the solution (Rukanova, Henriksen, et al., 2017). This leads to the concept of data pipeline: data quality is undermined by downstream communication throughout the chain, thus data should be captured directly at the source (Hesketh, 2009; Klievink et al., 2012). The result is an information system where information is shared among different organizations, and only authorized parties can access the data, providing safety and security (Hesketh, 2009; Klievink et al., 2012, 2016; Thomas & Tan, 2015).

Rukanova, Huiden, et al. (2017) showed how developing a data pipeline could improve CBM through direct access to key information, and therefore customs could be able to assess better which cargos should be inspected or not. Businesses, on the other hand, could improve their planning and optimization thanks to more available data and information (Klievink et al., 2012). This would lead to Supply Chain visibility, which could improve decision-making processes through data sharing across the chain (Hofman et al., 2019), and would reduce customs costs (Grainger et al., 2018). Abating supply chain barriers could boost global GDP by 5% (six times more than reducing tariffs) and increase Global Trade by 15% (World Economic Forum, 2013).

In 2018, the EU launched the PROFILE project, to improve customs risk assessment leveraging data analytics and incorporating new data sources (European Commission, n.d.). In 2017, the Commission identified blockchain Technology (BCT) as enabling technology for digital initiatives, and in 2018 DG TAXUD evaluated its application within customs (DG TAXUD, 2018a). In particular, one of the subtasks of the PROFILE project addresses the application of

BCT to improve the quality and availability of information among MS. Hofman et al. (2019) presented a demonstrator of a Supply Chain Visibility Ledger, an attempt to design a blockchain architecture which supports shipping processes. In a recent paper, Czachorowski et al. (2019) researched on the application of BCT in the shipping industry and provided some examples of ports (e.g. Singapore) and shipping companies (e.g. Maersk) to prove how the technology is increasingly being implemented. Among these, TradeLens, an open supply chain platform based on BCT developed by Maersk and IBM, is at the moment one of the most viable solution for shipping companies.

1.3. Overview of Blockchain Technology

BCT can be described as a distributed database where data are accessible by different actors simultaneously (Zheng et al., 2017). Every time a transaction is executed, it is firstly validated by each node through a consensus mechanism and, if nodes agree, a new block is linked to the chain (Ølnes et al., 2017). The main features of BCT are: decentralization, since no third parties or intermediaries are needed, and data consistency is maintained using consensus algorithms; persistency, given that it is nearly impossible to cancel a transaction after it has been approved; anonymity, considering that users could interact through generated addresses, without the need to reveal their real identity; auditability, given the persistency feature of blockchain, data can be easily verified. blockchain thus allows parties to exchange documents, without the need for intermediaries, keeping a permanent record of transactions which cannot be easily altered (Zheng et al., 2017). Nevertheless, the Blockchain is the product of social agreements, and human actors could decide to alter the history of the blockchain (Ølnes et al., 2017). Blockchain networks can be classified into three types (public, private and consortium) based on: consensus determination, which defines the nodes which will take part in the consensus process; immutability, which increases with the number of participants; efficiency, which decreases with the number of participants; read permission, to define the visibility of transactions.

Among the main challenges faced when developing a BCT architecture, scalability represents an essential factor, since different contexts require to handle a different number of users/transactions. Similarly, privacy concerns are raised since sensitive information could be shared with wrong or malevolent nodes, decreasing the willingness of organizations to join

the network. Technical hurdles though represent only a part of the problem since organizational issues could hinder technology adoption (e.g. low acceptance or no knowledge of the system).

1.4. Issues with BCT application in the shipping industry

As Francisco & Swanson (2018) argued, there are several variables, among which performance expectations or trust in technology, impact the behavioural intention of using BCT for supply chain visibility. Nevertheless, focusing on hindering factors is necessary to understand the issues and aversion towards the adoption of BCT. Technological aspects, such as security and scalability, are key challenges towards the wide application of distributed platform: Batubara et al. (2018) suggested that research should focus on developing standards by designing a reference architecture for practitioners. Standardization is also emphasized by Behnke & Janssen (2019), who recommended the development of consortia to drive the definition of wide-accepted standards. Chang & Shi (2019) identified two main obstacles to BCT application to cross-border trade: from a technical perspective, the state-of-art suggests that user experience has to be improved and lack of knowledge on how the system works represents a key issue.

Furthermore, other design requirements, such as system speed, scalability and interoperability, should be met to foster distributed platform implementation (Chang et al., 2020). A second impeding factor is collaboration reluctance: BCT would introduce a new decentralized system, where there is not a central operator responsible for managing transactions and interactions (Chang et al., 2020). This would lead to a governance issue: it is not clear who will be responsible for platform development and maintenance and be liable for it, thus organizations are hesitant to embrace the innovation. This shifts the attention from the IT system to the organizational network around the IT system.

Governance concerns are widespread among the existing literature. Behnke & Janssen (2019) questioned who should initiate the blockchain (p.8), given that it is unclear which organizations, public or private, would be in charge of developing and enforcing the platform, to lessen the opposition from the industry towards the technology. Beck et al. (2018) inquired how decision management rights and decision controls rights are allocated (p.1029) and

proposed decentralized autonomous organization (DAO) as entities responsible for enforcing governance rules. In Ølnes et al. (2017) the interrogative is who owns the data, introducing a new paradigm: governance by blockchain, since the system will be designed to manage transactions automatically among different organizations, and governance of the blockchain, meaning who is in charge of designing the platform and be accountable for it.

Centralization is required to enable decentralization: Ølnes et al. (2017) suggested that the transformation from the current system to a decentralized platform will happen in stages, where firstly a single governmental organization should develop and maintain the blockchain information infrastructure, and then the single-actor governance should be transformed into a networked governance. Considering the issue at stake, risk assessment in European Customs, developing an eCustoms platform would require supranational governance from a body like the EU, given that the diversity among border authorities would lead to conflicts in the design phases (Rukanova et al., 2015). Klievink et al. (2012, 2016) suggested that public-private governance could represent a viable solution to the conflicting interests of the industry: private companies have more interest in obtaining more information, but their diversity makes it more challenging to come up with a common solution. Hence, governmental bodies should enforce regulations and contribute to developing parts of the pipeline, necessary for the effective operations of the IT system (Klievink et al., 2012, 2016).

In conclusion, the issues can be divided into two main areas: technical hurdles, which require a deeper understanding of the underlying functioning and design of BCT; organizational obstacles, which imply defining the governance of the system to reduce the opposition of the industry towards the adoption.

1.5. Research Gap

By 2024, the new Import Control System (ICS2) will be deployed (DG TAXUD, 2017c): this will bring changes in practices and interactions in shipping transport. BCT could provide advantages in the development of platforms which will support the exchange of documents and information among maritime actors. Research on BCT applied in logistics has focused so far on exploring the potential and the advantages in a range of different applications, providing useful examples of how this technology can improve the efficiency and the

effectiveness of several business processes. Nevertheless, extensive research on how a potential blockchain-based platform could be designed to support these processes is missing. More in particular, Beck et al. (2017) argued that blockchain application development approaches need to be elaborated.

Developing a blockchain-based platform has also implications for the governance structure, meaning who is in charge of developing and maintaining the platform. Which organizations will be in charge of the governance could affect how the platform is structured and how the interactions and data sharing will take place (Van Engelenburg et al., Forthcoming 2020). Nevertheless, clear examples of how and to what extent the governance structure influences the design of the platform are missing.

In addition, the implementation of BCT to enable data sharing could bring several benefits for the involved actors: as argued from Susha et al. (2019), sharing business data with government can generate public value. In the context of risk assessment, customs might improve the analysis of import goods using data provided by traders, thus increasing public safety and security. Information sharing could bring benefits in terms of efficiency, effectiveness and quality of service (Gil-Garcia et al., 2019). Gil-Garcia (2012) argues that settings, where multiple governmental agencies from different countries cooperate with private firms, should be further analysed.

1.6. Main research question

To address the aforementioned issues, a research goal has to be formulated. The main research question (MRQ) is:

> *"Which design of a* blockchain-*based platform can be developed to support the availability of Entry Summary Declarations to customs authorities for incoming cargo flows into the EU?"*

The main goal of this study is to develop a platform which would support the information exchange among traders and customs authorities during the risk assessment procedure. In particular, the focus will be on the ENS data sharing. This study will address deep-sea containerized cargo, since they must be covered by ENS long ahead before arrival, resulting

in possible deviations in the planned itinerary, possibly causing missing ENS data (in comparison, bulk cargo must be covered by ENS within only 4 hours before arrival, thus reducing the risk of deviations). To develop a platform, its architecture needs to be designed, which encompasses defining protocol level, application level and their interactions (middle layer). The second dimension of the platform is governance. The aim is not to go deep into the details of the governance structure, but to analyse organizational tensions on a high-level and define how they impact the platform design and development.

The final output would be insightful in terms of design, as well as increase the awareness towards the application of BCT for enabling information sharing in international trade. Figure 1 provides a visualization of how the research goal can be divided into different parts.

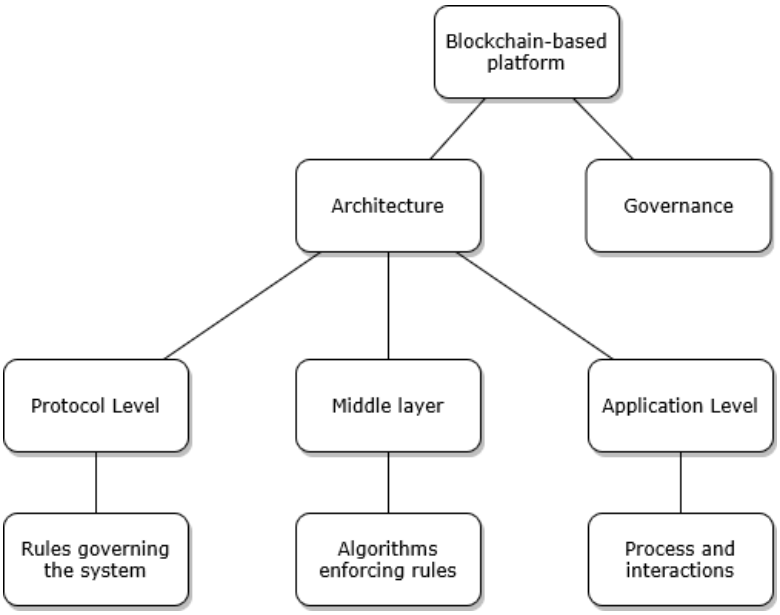

Figure 1 - Research goal subparts adapted from (Rossi et al., 2019)

1.7. Scientific contribution

The main goal of this research is to provide suggestions for the ICS2 implementation: the application of BCT to enable the upgrade of new Import Control System could prove to be valuable in improving the efficiency and effectiveness of information sharing. In the "Transition Strategy and Plan for Import Control System" (DG TAXUD, 2017c), the high-level process description and main requirements have been addressed. This research will start from this to analyse if and how developing a blockchain-based platform could improve the

exchange of ENS data and solve data availability problems in the context of the European Union.

Additionally, little work contributes to empirical research and this represents a problem, since the transition from a theoretical framework towards the real-world application is challenging. Design-oriented research would thus be valuable to existing research in information systems. The existing research covers topics concerning advantages that such technology could bring to organizations and society, and issues related to its implementation. Nevertheless, approaches to develop blockchain-based platforms needs to be further researched (Beck et al., 2017).

Furthermore, given the limited research on governance issues, this study will analyse how the governance structure impacts the platform design, contributing to Van Engelenburg et al. (Forthcoming 2020)

Finally, the study will reflect on motivation drivers in contexts where blockchain can enable business and government collaboration. This would contribute to (Susha et al., 2019), by providing a new example of how voluntary business data sharing can be achieved in the context analysed in this research.

1.8. Societal relevance

This research is part of PROFILE, a Horizon 2020 European project which goal is to improve customs risk assessment through data analytics, new data sources and better coordination among customs. In particular, a sub-task of the project addresses the application of BCT as a backbone for secure and safe data sharing. In particular, information sharing among European customs will be investigated, with a significant contribution to society.

For the maritime transport industry, this could result in highly facilitated trading contexts: customs risk assessment would improve effectiveness since suspected cargos could be better identified, and efficiency, since it would take less time and effort to assess the risks. As a consequence, traders could decrease shipping costs since a lower number of investigations would reduce delays throughout the supply chain. All this would produce an increase in global

trade, with benefits for exporting and importing countries and the worldwide economy as a whole.

Additionally, a better risk assessment will safeguard the interests of the European economy and the safety of European citizens. As of today, the number of tax frauds and illicit trading of dangerous goods represents a vital issue. More effective identification of irregular activities could reduce these risks and improve the socio-economic health of the Union.

Moreover, awareness towards this technology could increase, together with perceived usefulness and ease of use, so that companies would be keen to implement BCT within their IT systems, reaping all the benefits mentioned above.

2. Research design

To achieve the goals of this study and make sure that the contribution to science and society is relevant, it is essential to establish a research strategy. This leads to the first Sub-research question (SRQ):

> SRQ 1 - *Which research strategy allows to design a* blockchain-*based platform to support ENS availability among customs authorities?*

The research requirements should first be identified to answer this question, and then different research methods will be compared with these requirements.

As aforementioned, this study aims to investigate and design a blockchain-based platform to enable data sharing between customs and traders. Design-oriented IS research is needed, and the research framework that will be used in this study should allow designing an information service architecture. The problem should first be investigated in-depth to understand the underlying issues and then should be translated into requirements. After the design is done, it should be demonstrated and evaluated, before communicating the results.

According to Sekeran & Bougie (2016), different research strategies are available: experiment, to test for causality using manipulations; survey, to assess opinions, values, and beliefs; case studies, to collect data in a natural setting; design research, to design and evaluate novel artefact; desk research, to analyse already collected data. Considering design as the focus of this study, traditional research methods used within descriptive research do not serve this scope: as argued from Peffers et al. (2007), science and social sciences try to interpret reality to understand particular phenomena, instead design science intent is to create IT artefacts (e.g., models, methods, constructs) for organizational or societal purposes. In this sense, the Design Science Research Methodology (DSRM) provides a useful framework, divided into six different steps, from the problem definition and design process to the evaluation and communication of results (Peffers et al., 2007, pp. 56–58).

Nevertheless, as stated in the previous chapter, the input to research on Governance and Business data sharing literature represents a minor but essential aspect, since they are concerned more with implementation issues. As stated by Hevner et al. (2004), one main

pitfall of the DSRM is a lack of theory base, which could lead to perfectly designed IS, which do not serve organizational purposes. To achieve research rigor and relevance, DSRM needs theoretical frameworks to lead the construction and evaluation of the design (Hevner et al., 2004).

In 2007, Hevner introduced a three-cycle view (Figure 2). Firstly, the relevance cycle is concerned with the environment where the artefacts will be introduced and links the design with the context, which is customs risk assessment and issues with documental flow mentioned in the first chapter (Hevner, 2007). Instead, the rigor cycle connects the design with the knowledge base of existing research (Hevner, 2007). Finally, the design cycle focuses on building artefacts and evaluating them. The activities identified in DSRM are: "problem identification and motivation; define the objectives for a solution; design and development; demonstration; evaluation; communication" (Peffers et al., 2007, pp. 56–58). These steps will be further elaborated below.

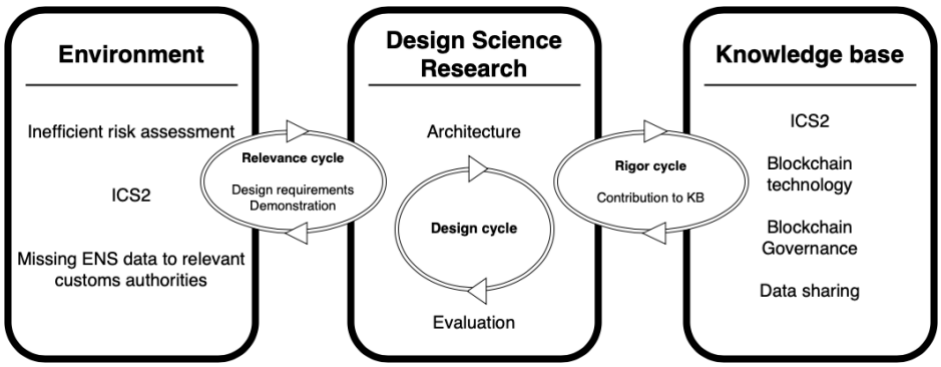

Figure 2 - DSRM cycles, adapted from Hevner (2007)

Activity 1. Problem identification and motivation.

The goal of this activity is to introduce the problem. Chapter 1 covers this part: the issues with risk assessment have been introduced and BCT has been identified as a viable technology to implement the ICS2. The motivation resides in the little research contributing to the topic and the urgency to solve the issues. From this, the MRQ has been formulated.

Subsequently, the goal is to analyse the current Import Control System and the upgrade to the ICS2. In the first instance, the maritime shipping process will be analysed through a literature review, focusing on the documental flow concerning deep-sea vessels. After that,

the focus will be on better understanding the issues with communication and information sharing and how risk information sharing is affected when a vessel changes its itinerary. Once the current Import Control System is described (AS-IS), the process in the new ICS2 will be presented. This will serve as input for describing a first concept of the interactions and information sharing implemented on a blockchain-based platform, providing UML diagrams. SRQ2 focuses on the application level:

> SRQ 2 - *How would the interactions/information flow among trade actors during the submission of ENS look like when implemented on a blockchain-based platform?*

Activity 2. Define objectives for a solution.

Once the process is defined, it should be translated into a description of the desired solution, which will take the form of requirements. The requirements should be derived rationally from Activity 1, with knowledge of current solutions, analysed in SRQ2 (Peffers et al., 2007). In this phase, SRQ3 will be answered: the architecture requirements to enable itinerary updates and ENS sharing will be formulated through a literature review where the Knowledge Base on business data sharing will be analysed to establish research rigor.

> SRQ 3 - *What are the design requirements to support data sharing in the context of European customs?*

The requirements are concerned with the protocol level: they define the rules of the system.

Activity 3. Design and development.

Artefacts are created at this stage. The goal is to design the architecture that will comply with the requirements defined during the previous stage. This phase is critical: firstly, it will produce one of the research outputs; secondly, given its complexity, it will require more time and effort. BCT's core concepts will be studied with a literature review, to ground the research in the Knowledge Base on information systems and identify the core BCT components:

> SRQ 4 - *What are the core blockchain components and design choices to be considered during the design phase?*

Next, the architecture will be designed, answering the SRQ5.

SRQ 5 – *How does the architecture of the blockchain-based platform that supports ENS data exchange look?*

Figure 3 shows how the previous activities will contribute to a different level of the architecture.

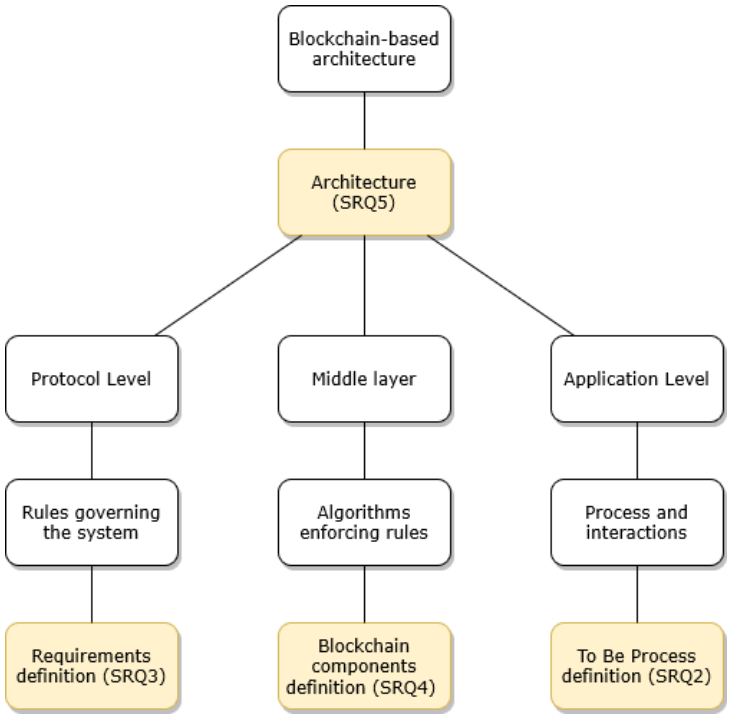

Figure 3 - Research questions relation with research goals adapted from (Rossi et al., 2019)

Activity 4. Demonstration.

In this phase, experiments or simulations could be carried out to demonstrate how the developed designs solve the problem. Knowing how to use the artefact when addressing the issue is fundamental to perform this phase successfully. The demonstration can be performed with a walkthrough: Verschuren & Hartog (2005) described this as a detailed outline of the artefact. A walkthrough represents a viable demonstration option because it precedes the prototyping step: to realise a prototype, is necessary a written description of its functionality and design.

SRQ 6 - *How can the blockchain-based platform be used to share ENS data?*

Activity 5. Evaluation.

According to Peffers et al. (2007), the evaluation can be carried out in different ways, including measuring the performance quantitatively or proving logically. Including quantitative measures would require a large-scale implementation phase, which is out of this research scope. Verschuren & Hartog (2005) identified several criteria, among which clearness, ethical acceptability, affordability and feasibility, to be analysed when judging a designed artefact. Considering that the design precedes the development phase, it would be necessary to evaluate the feasibility of the design its development, to assess whether the design makes practical sense. The evaluation will be performed through a comparison with existing platforms. The factors which will be assessed are scalability, security, trust, and immutability (see sections 1.3-1.4), answering the SRQ7.

> *SRQ 7 - How does the designed platform rate compared to an existing platform in the shipping industry in terms of scalability, security, trust, and immutability?*

Also, a reflection on the implementation will be carried out in this phase. This would be instrumental in assessing the tensions on the organizational level and how they impact or are impacted by the technical design choices. Firstly, by using the platform for CSSP (Selsky & Parker, 2005), the organizational tensions will be analysed. Then, using the blockchain governance framework from Van Engelenburg et al. (Forthcoming 2020), the governance's impact on design choices will be analysed.

> *SRQ 8 – To what extent the design choices are subject to the governance structure?*

Activity 6. Communication.

The last step is communicating the results of the study. The goal is to critically discuss the outcome, recognise the limitations, and define the final contribution to science and society. The MRQ will be answered at this stage.

Figure 4 summarises the different stages and the links between different activities. Each activity will be addressed in one chapter, starting from chapter 2 for activity 1.

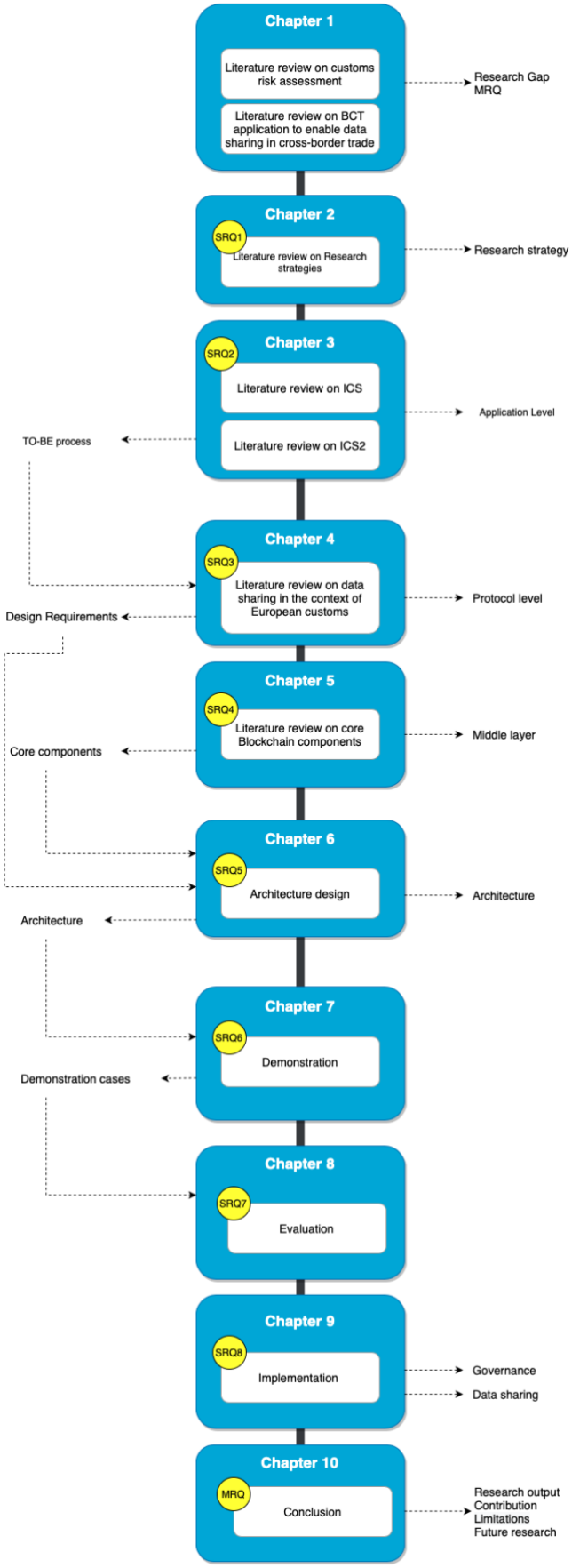

Figure 4 - Research Outline (own figure)

3. Process description

This chapter will answer SRQ 2 - *How would the interactions/information flow among trade actors during the submission of ENS look like when implemented on a blockchain-based platform?* Initially, the current Import Control System will be analysed, through a literature review on official documents from the European Commission, to visualise the maritime shipping process in detail and to understand data-sharing issues. After that, the new ICS2 will be introduced. This will serve as input to visualise how the interactions would look like when deployed on a blockchain-based platform.

This chapter will cover step 1 of the DSRM, providing a representation of the application level. Picturing the interactions will be valuable in chapter 4, to develop the architecture requirements, and in chapter 6, to design the architecture.

3.1. Risk assessment process

Before diving into the analysis of the interactions and information exchange among actors, the risk assessment process will be introduced.

Customs authorities use information as the main input for assessing import risks. Documents and declarations, such as the ENS, constitute the primary sources of knowledge: they contain the country of origin and destination, name of buyer and seller and a description of the goods. Additional documents could be requested in case of particular goods (e.g. livestock). Other sources of information include other customs offices, institutions and businesses. Before the information can be used for risk analysis purposes, it should be processed and analysed to become intelligence. In particular, three levels of intelligence exist (European Commission, 1998):

1. Operational intelligence: information which requires a prompt response for detection. Time is often critical since it is needed to detect fraud and smuggling.
2. Tactical intelligence: information on activities, means of transport and organisations, used to detect suspected trade flows.
3. Strategic intelligence: information on common methods of customs fraud.

EU customs assess all traffic by comparing declared data against risk profiles (a combination of risk rules). The risk rules are confidential and not shared outside the customs domain, but basic risk rules can check whether *the weight of the shipment corresponds declared commodity and quantity*, or whether *the shipper exists in commercial registers* (European Commission, 1998). Shipments are then selected for controls-based risk scores that indicate the level of various customs risks associated with them. Shipments of high-risk score get blocked for examination (European Commission, 1998).

Targeting decisions determine which goods should be selected to control and to what extent, where, when, and with which techniques the selected goods should be examined. The targeted shipments may be examined with X-rays, canine teams or other inspection methods. Customs officers may also want to inspect the goods and accompanying documents manually (European Commission, 1998).

As illustrated in Figure 5, customs risk assessment is decomposed into two different steps, (a) an algorithmic step and (b) where a targeting officer can interfere. These two basic steps may be decomposed even further, depending on the solutions and policies for risk assessment implemented by a customs authority (European Commission, 1998). The algorithmic step is mentioned as 'Risk Assessment Module'. The human intervention by a targeting officer is shown as 'Filtering'. This second step can also be supported by algorithms, e.g. for instance, analysis of a hit against operator behaviour. Eventually, either good are released, or hits will lead to inspections that provide so-called control feedback (European Commission, 1998).

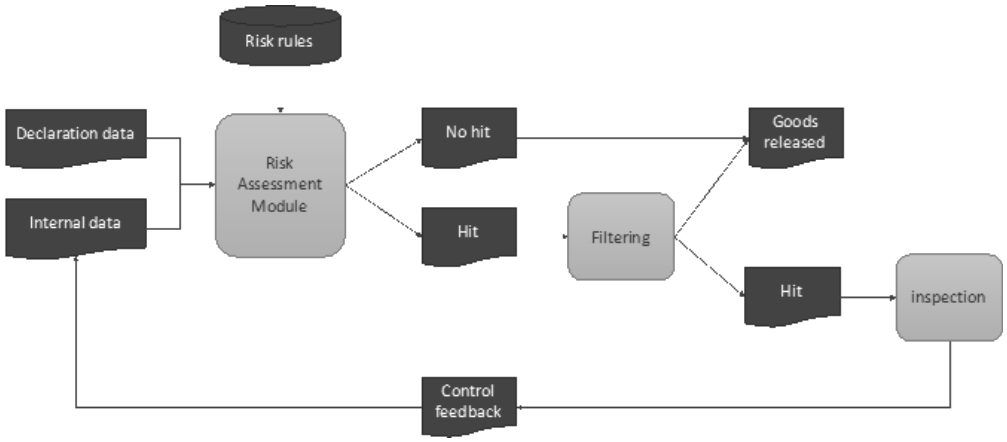

Figure 5 - Risk assessment process, based on (European Commission, 1998)

Different customs risks can also be categorised by looking at how urgent it is for customs to control them. Fiscal contraband like untaxed cigarettes is less urgent than transport security risks like a bomb on a plane. Transport security risks typically have the highest degree of urgency, given their potential for immediate damage, so customs seek to identify, isolate and neutralise them as soon as possible. The EU advocates the pre-loading risk assessment to prevent security threats from being loaded on a vehicle of transport. The Entry Summary Declarations (ENS) and Exit Summary Declarations (EXS) that need to be submitted to customs by transport-mode specific times are designed to support the pre-loading security, and safety risk assessment[2].

The main takeaway from the description of the risk assessment process is that data plays a vital role: declaration data are processed, together with internal data and risks rules, to define whether to inspect or not a cargo. If the input is not sufficiently informational, the final output could lead to wrong decisions, affecting trade facilitation and security.

3.2. Actors

The maritime shipping process starts with a consignor, which could be referred to as seller, who is the original owner of the goods and arranges the transport to the consignee, namely the buyer. The consignor usually entrusts a freight forwarder, responsible for arranging the shipping and related services: in particular, freight forwarders have the expertise to prepare documentation for international carriage. A carrier is an actor responsible for performing the shipment. Before the carrier can load the goods on the vessel, customs authorities check the related documentation and perform the risk assessment (see 3.1). The goods are then loaded on a vessel, and the carrier performs the shipment. When the goods reach the country of

[2] Safety threats refer to hazardous goods that may cause damage during transit *accidentally* because of their hazardous properties. Security threats include explosive devices, weaponised chemicals and biological agents and other weapons that are *intended* to cause damage during transit or at the destination.

destination, customs at entry might inspect the cargo. Subsequently, the goods are consigned to a freight forwarder in the importing country, who is responsible for transporting the products directly to the consignee (Figure 6 pictures the actors and goods flow).

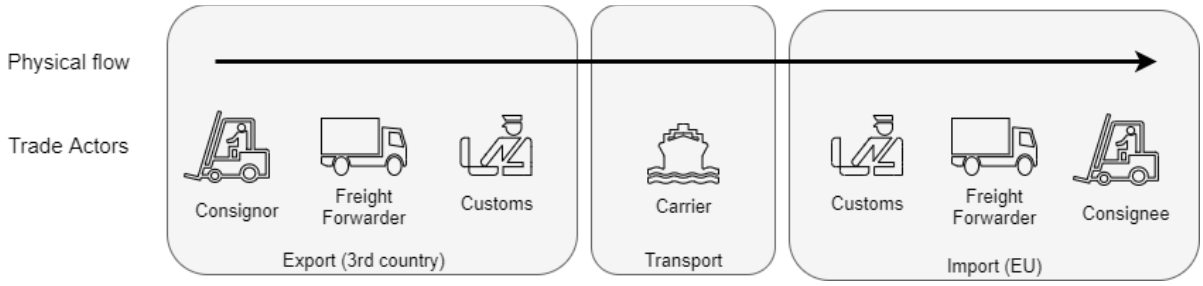

Figure 6 - Actors, adapted from (Hesketh, 2009)

Even though the process looks rather smooth, numerous interactions and dozens of organisations are involved for an average shipment. Sometimes, the actors involved in the process might differ based on the products shipped. Nevertheless, for the scope of this research, two categories of actors are of interest: carriers, because of their awareness of the itinerary of the vessel and since they should be responsible for providing ENS data, and customs at import, since they perform a risk assessment and represent the main gatekeeper between traders and Europe.

3.3. Interactions and information sharing

The number of documentation and communications exchanged during the process is directly proportional to the number of actors: more traders and authorities involved means numerous interactions. Traders are requested to submit several documents to customs authorities, containing information on the cargo shipped to Europe. Customs base the risk assessment process on this information. Nevertheless, for this study, only the ENS will be analysed.

The ENS submission is managed by the ICS at the European level. A carrier lodges the ENS to a customs office during pre-arrival filing. This declaration contains information such as:

- Information on the consignor and consignee, for instance, Names and Addresses;
- Planned itinerary, with code(s) country(s) that are part of the transport route and office of first entry specification;
- Contents of the consignment, with classification of the goods.

To better explain the interactions and data sharing process, an example could be used. For instance, it can be assumed that a vessel coming from Asia is shipping products to Europe. The vessel is planned to enter the EU through Belgian customs in Antwerp (BE), and after that, the itinerary includes Rotterdam (NL), Hamburg (DE) and Le Havre (FR). Some products will not be unloaded in the ports mentioned above but will transit Europe to reach North America.

The EU requires economic operators coming to Europe to submit ENS data, for goods brought into the Union territory, within a predefined timeline, which depends on the means of transport (European Union, 2013). Regarding deep-sea containerised cargo, the ENS should be sent to Customs Authorities 24 hours before loading goods on the vessel (DG TAXUD, 2018b). In case the vessel calls at more than one port in the EU, all the ENS should be lodged at the Customs office of First Entry (DG TAXUD, 2018b). So, in the example, the carrier has to lodge all the ENS to the Belgian customs. Also, goods which transit but do not enter the EU customs territory should be covered by an ENS: this means that also containers which have been loaded in China and will be discharged in North America, should be covered by ENS while transiting in Europe. Dutch customs will only receive ENS of products to be unloaded in Rotterdam (NL); German customs will only receive ENS of products to be unloaded in Hamburg (DE) and so on.

The COFE, BE in this case, is responsible for performing risk analysis on all goods, regardless of their destination, to assess threats for safety and security (See 3.1 for a detailed explanation of the risk assessment process). Information plays a crucial role in assessing the risks related to importing goods. During the risk assessment, some goods might be labelled as risky: if the level is deemed to be severe (e.g. explosive devices or disease spreading products) the custom office will notify to "do not load" (DNL) the goods (European Commission, 2013). If the risk assessment is positive (the good needs to be checked) the results are sent to the customs office of unloading (COU): this means that if Dutch customs should check a product to be unloaded in Rotterdam, Belgian customs will send them the risk assessment results (European Commission, 2013). The COFE is responsible for sending to customs relevant data, meaning that each next office in the itinerary will receive only ENS for goods which will be unloaded in that specific port: so Customs in Antwerp sent ENS data of containers to be unloaded in Rotterdam to Dutch customs, ENS data of containers to be unloaded in Hamburg to German customs and so on (Figure 7 pictures the interactions)

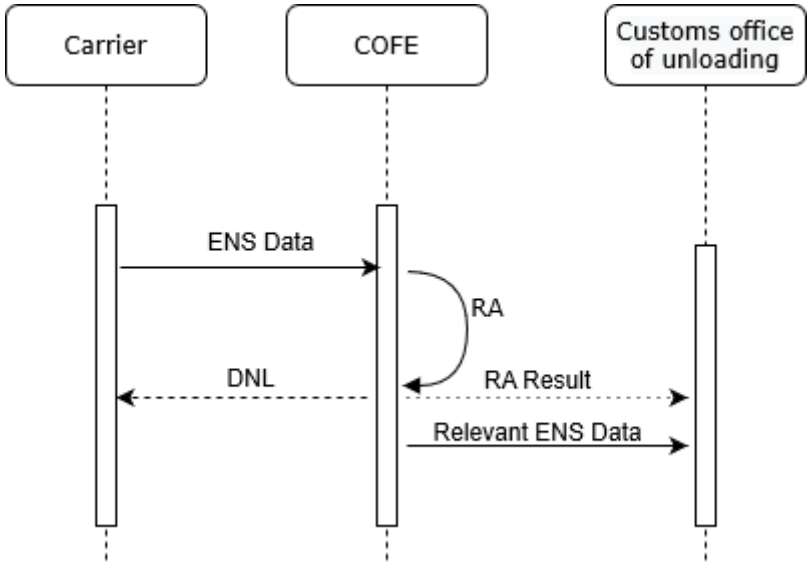

Figure 7 – AS-IS Interactions among actors based on (European Commission, 2013;DG TAXUD, 2018b)

3.4. Changing itinerary case

As aforementioned, ENS are sent to the COFE 24 hours before loading the goods on the vessel, to ensure that a pre-loading risk assessment is performed to identify possible risks promptly. Nevertheless, the COFE could change from the planned one: transoceanic shipments from the Far East or North America towards Europe could take up to one month, a long-time horizon which brings challenges in terms of planning which could result in changes in the initial itinerary. Furthermore, the vessel could load some cargos in subsequent ports which require to enter from different countries. Operational reasons can also cause a change in the itinerary. As a consequence, the COFE might not possess the necessary information and data on ENS, which are fundamental for risk assessment.

To address this problem, vessels which are diverted to a different COFE from the initial declared one must submit a diversion notification (DN) to the initial COFE who will be in charge to share the relevant information with the designated customs authorities (DG TAXUD, 2018b). Continuing with the previous example, the vessel might change its itinerary so that Le Havre (FR) is the first office of Entry. The economic operator communicates the change to customs in Antwerp. At this point, French customs do not have all the ENS data, so Belgian customs have to provide them with information on time. This case is represented in Figure 8.

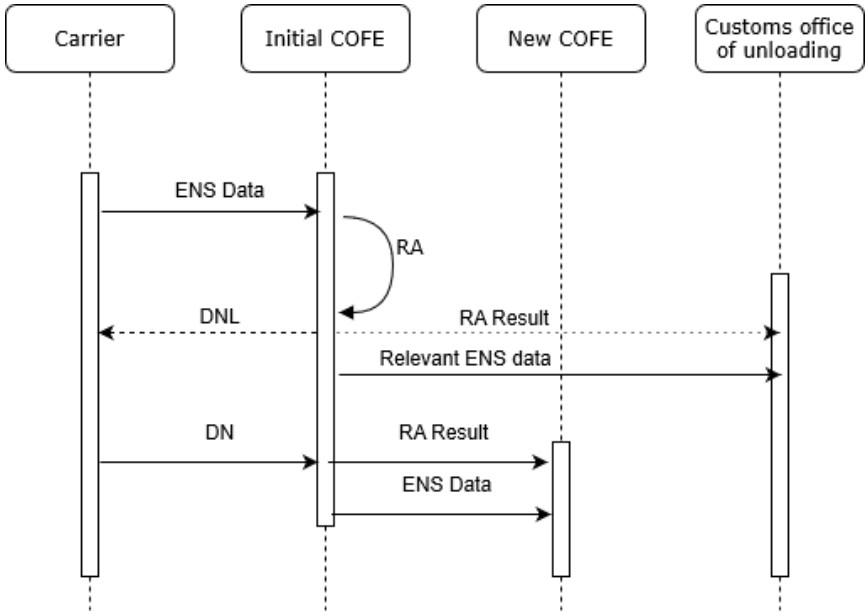

Figure 8 - Interactions in case of diversion based on (European Commission, 2013;DG TAXUD, 2018b)

With the current methodologies, data availability represents an issue: indeed, the COFE often needs to request additional information to other customs. This is problematic in terms of risk assessment efficiency since with a lower number of information customs cannot perform an accurate analysis.

3.5. Assumptions and simplifications

In order to simplify the description of the interactions, some assumptions and simplifications have been made within this research project.

According to the Union Customs Code (UCC) (European Commission, 2018; European Union, 2013), a third party can lodge the ENS on behalf of the carrier, but in this research it has been assumed that the carrier is the only actor who is in charge of submitting ENS to customs authorities. Similarly, it has been assumed that the carrier always submits the ENS to the COFE even though the ENS could be lodged at a customs office different than the COFE (European Union, 2013).

Goods can be unloaded at the first port of call, but this does not represent an issue in terms of missing ENS since the COFE does not have to share information with the following ports. The focus is on goods which will be unloaded at a different port than the first one.

The ENS could be incomplete or present mistakes, and customs could request follow up information after the first submission of the declaration. Similarly, carriers can amend the ENS when certain conditions are met. To simplify the process, it has been assumed that, once the ENS is submitted, no changes are made, and no other documents are shared.

Other documents (e.g. the bill of lading[3]) are exchanged between involved actors. Since the research focus is particularly on ENS, other documents will not be considered in this thesis. Other activities are carried out during import procedures, for instance, customs supervision and temporary storage. These nevertheless do not influence how the sharing of ENS data take place, thus they have not been included in the process description.

3.6. New Import Control System

Data need to be accessible at the same time to the multiple Member States to support flexible use, management and exploitation (European Commission, 2013). This would require changes in practices and systems. For this purpose, the EC proposed an upgrade of the ICS: the ICS2.

The ICS2 solution is to set-up a common repository for mandatory use by all Member States. The main objectives are (DG TAXUD, 2017a):

1. Improve ENS data quality;
2. Improve availability of ENS data among relevant customs authorities.

Objective 1 covers topics which go beyond the scope of this study, whereas objective 2 addresses the same issues as this study: cooperation among the Members States using IT capabilities for effective and efficient risk analysis; availability of ENS data to relevant customs

[3] A bill of lading (also Master Bill of Lading MBL or House Bill of Lading HBL) is a legal document which certifies the ownerships of goods described.

offices. This would produce valuable benefits for the Member States. Customs offices will promptly receive and retrieve relevant information to identify and address risky goods while facilitating the import of low-risk trade (DG TAXUD, 2017a). To achieve these goals, some areas of improvement have been identified, namely the definition of a new collaboration process between the Member States to share additional information among customs and the definition of new exchanges between a central IT process and national risk processes(DG TAXUD, 2017a).

Diving into the technical features of the ICS2 system, the plan foresees the introduction of a common data repository for mandatory use at the EU level to gather ENS data and share risks results (DG TAXUD, 2017c, 2017a). Furthermore, a shared interface for trade and service for "e-Screening and Risk Management" support for the Member States have been proposed as additional services from DG TAXUD, but are not if interest for this research (DG TAXUD, 2017c, 2017a).

Concerning the maritime shipping process and exchange of information, the ICS2 system provides different functionalities for traders and customs. Considering the pre-loading filing of deep sea containerised cargo (Figure 9 – left side block), carriers share the ENS (1) with the COFE, which performs risk assessment (2) and stores the result on the common repository (3): in case of DNL, the cargo will not be embarked on the vessel. Right before the arrival (Figure 9 – central block excluding short sea filing), the carrier can submit the Arrival Notification (4 - AN) and Presentation Notification (5 - PN), triggering the security and safety (6 - S&S) control. In case of positive S&S control, the cargo will be released, otherwise, further controls will be necessary. All this information will be stored on the common repository so that they can be retrieved from the country of destination (7). Figure 9 shows the process as designed in ICS2.

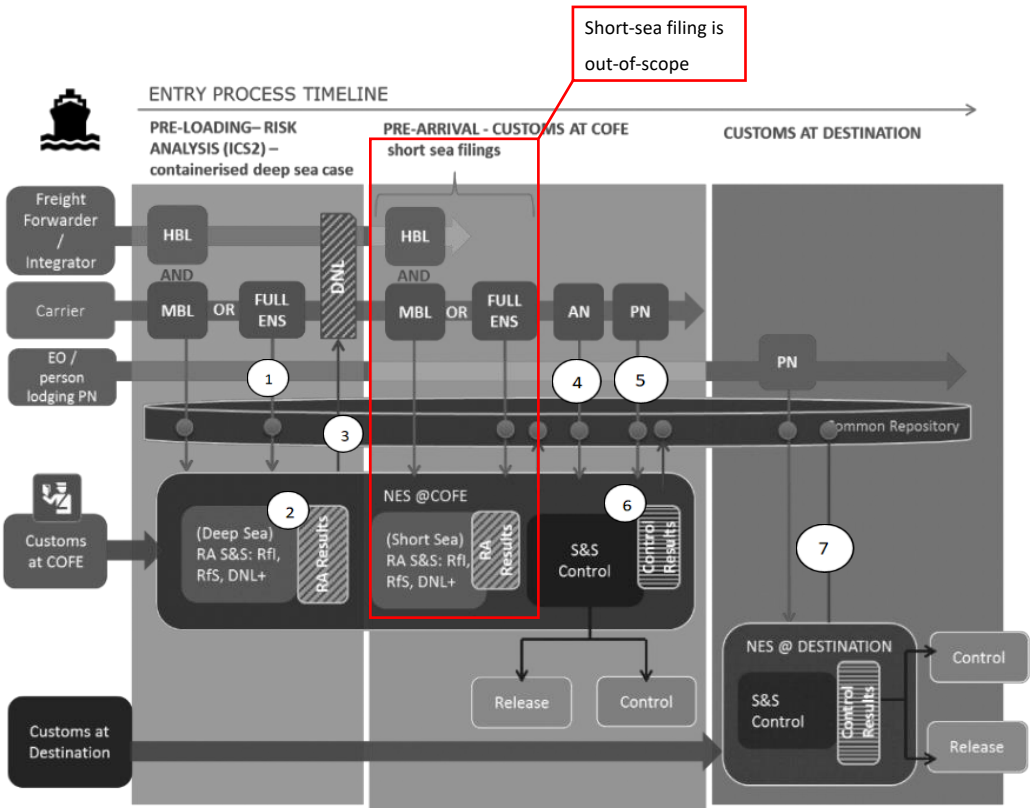

Figure 9 - ICS2 Maritime Process, retrieved from (DG TAXUD, 2017c)

3.7. Interactions with a blockchain-based platform

The deployment of the ICS2 will change how actors will interact. In particular, key information will be lodged into a common repository, and interested actors can retrieve data autonomously. This serves as input to the case analysed in this research, where actors interact using a blockchain-based platform to share ENS data.

In the high-level interactions, carriers can lodge ENS (or a reference to the document, as indicated from the dotted line in the picture) and Itinerary Data on the platform, indicating COFE and following ports of unloading. The itinerary data will provide access to customs: the COFE will be to read all the ENS data, whereas each following COU will receive relevant ENS (e.g. of cargo unloaded at their port). Say that the itinerary is BE, NL, DE and FR, then BE customs will have access to all the ENS data published on the platform, while NL customs can access ENS data of containers unloaded in Rotterdam, DE customs can access ENS data of containers unloaded in Hamburg, and FR customs can access data on containers unloaded in Le Havre. If the vessel is diverted to another COFE, FR customs, for instance, the carrier can

upload this change on the platform through updating the itinerary: so now the new COFE will have access to all ENS data. Figure 10 shows this case.

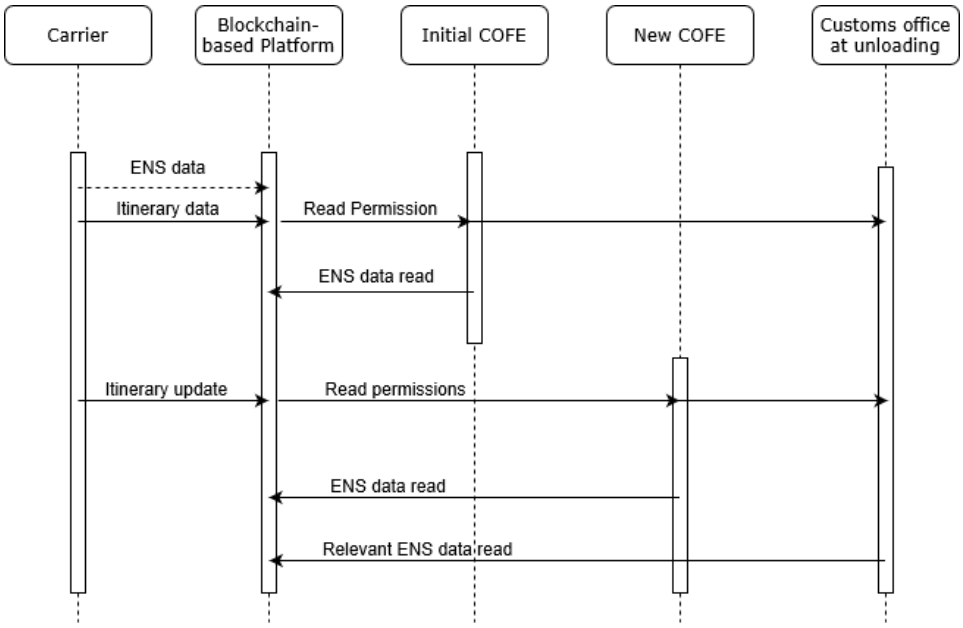

Figure 10 – Interactions using a blockchain-based platform (own figure)

3.8. Conclusions

This chapter started with an introduction to the risk assessment process to show how information, especially ENS data, plays a vital role when assessing import risks and threats. After that, the actors involved with international shipping have been introduced to show how they interact to exchange ENS data, using the current ICS. Things get a bit more complicated when a vessel changes its itinerary, entering the EU from a COFE different than the initial declared one: the number of additional communications needed is inefficient and often results in missing ENS data. Next, the new ICS2 has been described. This new system will bring changes in the interactions among shipping actors and how information is exchanged.

The main takeaway from this chapter is that the upgrade to the ICS2 will add to the current "data push system", where information is shared directly among actors, a "data pull system", so that customs can also retrieve information directly from the common repository, increasing the availability of data in a more efficient way. In line with this, the proposal is to develop a blockchain-based platform, which would enable a more efficient exchange of ENS data. Considering that the diversion of vessels to a COFE different than the initial declared

one creates significant issues, the proposal is to use the itinerary as a pre-arrival notification in order to allow customs to access new ENS data when the itinerary changes.

This will serve as input for the next chapter, which will instead focus on which requirements the architecture should comply with in order to support the new case.

4. Design requirements

To develop a blockchain-based platform, an architecture has to be designed. To design an architecture, the design requirements have to be elicited. This chapter aims to answer SRQ 3 - *What are the design requirements to support data sharing in the context of European customs?* Initially, a definition and classification of requirements will be provided in section 4.1. Section 4.2 will describe the functional requirements. Section 4.3 will instead focus on the non-functional requirements. Section 4.4 concludes the chapter, summarising the requirements and answering SRQ4.

This chapter will cover step 2 of the DSRM, defining the objectives that the final architecture should achieve. The requirements will define the constraints that should be considered in the design phase, addressing the protocol level.

4.1. Requirements classification

Information system requirements communicate the needs of the system owner, explicating what the system is expected to achieve (Koski & Mikkonen, 2017). Requirements can be divided into functional requirements, which include "*statements regarding the services which the system should provide, how the system should react to particular inputs and how the system should behave in particular situations*" (Koski & Mikkonen, 2017, p. 6), and non-functional requirements, which are more concerned with security issues and the development process.

In order to define the functional requirements, the conclusions from chapter 3 will be valuable, since they state how the platform should function. Non-functional requirements are instead be analysed through a literature review on data sharing issues.

4.2. Functional requirements

Section 4.2 introduces the functional requirements. For this section, the input from chapter 3 is valuable in order to define what the architecture is expected to do. In addition, the requirement definition will be complemented through a literature review

The goal is to enable customs to access ENS data. Coordinated border management and information sharing across governmental agencies would facilitate the flow of goods and risk management (Elmane-Helmane & Ketners, 2012; Rukanova, Huiden, et al., 2017; Shafiq et al., 2010; Yasui, 2011). Customs often operate with incomplete information and find themselves asking for additional information to other agencies. The result is a scenario where customs hold complementary information, but the information exchange does not take place or is ineffective. Making information available to all concerned authorities (customs authorities in the case at stake) could help with coordinating trade activities and improve risk management. As a consequence, considering the process description and the current regulations on availability of ENS data (Chapter 3), the COFE should have access to the ENS data of all containers, whereas following customs authorities can only access ENS data of containers to be unloaded in their ports.

> *Req. 1: A customs authority should always have access to the proper ENS data. The COFE will access ENS data of all containers, whereas other customs offices will only access ENS data on products unloaded in their ports.*

In order to enable information access from customs, businesses should provide information in the first place. Business-government collaboration could be fostered using digital infrastructures (Hesketh, 2009). Collaboration can take place in different ways, but information sharing represents the most valuable opportunity for businesses and government: in particular information has to come from the commercial sector since private firms gather a considerable amount of data for their operations, but do not share them with customs (Hesketh, 2009, 2010; Rukanova, Huiden, et al., 2017). Collecting information from private firms is vital to improve services performance: customs base the trade management on data which is generally vague and inaccurate, so increasing the number of information could bring public value while increasing companies efficiency and effectiveness (Bharosa et al., 2013; Engelenburg et al., 2019; Overbeek et al., 2011). Risk management could be improved only if economic operators submit data to customs before the arrival of goods (Yasui, 2011).

> *Req. 2: The a*rchitecture should give customs real-time information on changes on the itineraries, and carriers should be the source of this information.

4.3. Non-functional requirements

The case analysed in this research is not extensively addressed in the current literature. Nevertheless, similar cases could be found, such as the data pipeline (introduced in 1.2), which is insightful to define the non-functional requirements. Even though the data pipeline is designed to solve mainly data quality issues, data sharing implications are extensively expressed. Here a strong assumption is introduced: it is expected that the information-sharing issues addressed in the data pipeline research do not substantially differ from the case analysed in this research. This is due to the similarity of the research areas: both focus on distributed platforms to enable information sharing among businesses and customs and improve risk assessment. Thus, to define the non-functional requirements, the literature on the data pipeline concept will be used. This can be complemented with the more general literature on data sharing. Furthermore, guidelines from the European Commission will also be taken into account.

According to Hesketh (2009), the key to enabling data sharing is to handle data efficiently, promptly and securely. Starting from the latter, information security is based on the well-known CIA triad (Johnson, 2010): confidentiality, integrity and availability. The following sections will elaborate on this concept

Confidentiality

Confidentiality[4] could be defined as restricted access to private information. Secure transactions are necessary to ensure the reliability of the system (Engelenburg et al., 2019; Pruksasri et al., 2014). Confidentiality represents a barrier to use e-customs platforms to exchange information since without ensuring that private data will not reach unauthorised

[4] https://dictionary-cambridge-org.tudelft.idm.oclc.org/dictionary/english/confidentiality

parties, private firms could be reluctant to expose sensitive information (Urciuoli et al., 2013). ENS contains data which should not be publicly exposed.

To ensure confidentiality, identification, authentication and access control should be taken into account (Hofman & Bastiaansen, 2013; Knol et al., 2014; Pruksasri et al., 2014; Yasui, 2011). The identification requires each user to be univocally known. The user is intended as an organisation (carrier or customs authority).

Req. 3: Each user should be registered as one digital identity (identification)

Req. 4 Each digital identity must be associated with only one user (authentication)

While open information can be publicly accessed, sensitive data should be concealed. According to Pruksasri et al., (2014), data concealment should be a two steps process: data should be initially stored in a safe place and encrypted; when an authorised party requests it, information is shared securely. The key point is that the system should recognise that customs are an authorised party so that they can access information (Hulstijn et al., 2012; Klievink et al., 2012). In particular, customs should access information on products transported to their countries (Pruksasri et al., 2013; van Engelenburg et al., 2017).

Req. 5: Data should be stored in a safe place and be encrypted (concealment)

Req. 6: Carriers should only access information related to their shipment (access control)

Req. 7: Customs should only access information on vessels passing through their jurisdiction (access control)

This is also linked to the concept of “data pull system”: custom can directly access relevant information from external databases through authorisations and read permission mechanisms (Pruksasri et al., 2014; Rukanova, Huiden, et al., 2017; van Engelenburg et al., 2017; Yasui, 2011).

Integrity

Integrity addresses the quality of data: information provided from traders should be correct (Pruksasri et al., 2013). This is crucial since customs need reliable data for the risk assessment to be effective: if data have been altered and do not represent reality correctly, it can result in wrong decisions (Hulstijn et al., 2012; Overbeek et al., 2011). For the same reasons, a high level of immutability is necessary for adequate information sharing among customs administrations (Engelenburg et al., 2019; van Engelenburg et al., 2017; Yasui, 2011).

> *Req. 8: Control mechanisms should be in place to ensure the integrity of exchanged information so that data are not tampered when shared (integrity)*

Availability

Availability focuses on making sure that key information is available to organisations promptly. *Req. 1* and *Req. 2* already addressed this. Also, to enable the availability of data, interoperability is a crucial requirement (Klievink et al., 2012): governmental agencies carry on their activities using different information systems and infrastructures, which have to be interconnected to ensure effective and efficient data sharing. This is associated with the format of data exchanged: according to Hamza et al. (2011), electronic systems should use the same data format to make information sharing easier. Interoperability is expected to increase the completeness of data so that all the interested parties will receive all the information they need (Hofman & Bastiaansen, 2013). Considering that interconnection of different IT infrastructures is out of the scope since it is related to implementation issues which the designed architecture will not address, only data structure requirements is addressed.

> *Req. 9: The data structure should be consistent, to ensure interoperability (availability)*

Scalability and volumetric

Considering performance related requirements, scalability represents an essential factor. In particular, the volumetric of maritime ENS has been estimated from DG TAXUD as much as

87 million per year, which requires a peak transaction rate of 29.3[5] per second (DG TAXUD, 2017b). Additional transactions are needed in order to share itinerary data.

Req. 10: The architecture should handle a high rate of transactions.

Moreover, since the number of carriers could increase, the architecture should be scalable in terms of how many parties can join the network.

Req. 11: The architecture should accommodate an increasing number of parties joining the platform.

4.4. Conclusions

This chapter started from the conclusions of chapter 3: the UML and process descriptions have been used as input to define which conditions have to be met in order to ensure the operational feasibility of the changing itinerary case. The non-functional requirements have been defined mainly using the literature from the Data Pipeline: this concept has many similarities with the case analysed in this research. This has been insightful in terms of requirements to ensure in order to avoid data-sharing issues. Furthermore, DG TAXUD and EC documents were helpful to define some additional requirements, mainly related to the performance of the platform, such as scalability or interoperability.

So, to answer SRQ3 "What *are the design requirements for data sharing in the context of European customs?",* Table 1 will provide an overview of the defined requirements.

[5] DG TAXUD (DG TAXUD, 2017c) estimates that, when the ICS2 transition will be completed, the peak transaction rate will be 108 ENS submission per second. Considering that maritime traffic makes up to 37% of all ENS submission, 29.3 has been calculated as 108*37%

Table 1 - Design requirements for the architecture design

Code	Description
Req. 1	*A customs authority should always have access to the proper ENS data. The COFE will access ENS data of all containers, whereas other customs offices will only access ENS data on products unloaded in their ports.*
Req. 2	*The architecture should give customs real-time information on changes on the itineraries, and carriers should be the source of this information.*
Req. 3	*Each user should be registered as one digital identity (identification)*
Req. 4	*Each digital identity must be associated with only one user (authentication)*
Req. 5	*Data should be stored in a safe place*
Req. 6	*Carriers should only access information related to their shipment (access control)*
Req. 7	*Customs should only access information on vessels passing through their jurisdiction (access control)*
Req. 8	*Control mechanisms should be in place to ensure the integrity of exchanged information so that data are not tampered when shared (integrity)*
Req. 9	*The data structure should be consistent*
Req. 10	*The architecture should handle a high rate of transactions.*
Req. 11	*The architecture should accommodate an increasing number of parties joining the platform.*

5. Core Blockchain components

This chapter aims to describe in detail the architectural components of BCT and address SRQ 4 - *What are the core blockchain components and design choices to be considered during the design phase?* In order to answer this question, the main components should initially be identified, using a literature review on BCT architecture. After that, each component will be further analysed through a literature study, to provide the design choices that should be considered in the design phase, and that will make up the middle layer. These will be summarised in the conclusions, to answer the SRQ4.

This chapter falls in Activity 3 of the DSRM. The goal is to apprehend the necessary knowledge on BCT in order to make well-oriented design choices in the next chapter.

Before diving into the core of this chapter, it should be underlined that the technical aspects of BCT will be discussed at a high level since the scope of this thesis is not to analyse in-depth the main features of BCT, but to identify what are the main design components and, based on this, define the architecture. For a more exhaustive explanation of the different components, the reader is redirected to the cited literature.

5.1. Identified core components

The first step is to identify which components make up a blockchain architecture. To do so, it is vital to select papers which classify the blockchain architecture components. On search engines like Google Scholar or Scopus, search terms like "Blockchain" AND "Architecture" OR "Overview" OR "Taxonomy" were used. Papers were selected based on the number of citations (e.g. above 250) and journals with a high impact factor (e.g. above 1). The search resulted in papers from IEEE (Proceedings of the IEEE and IEEE Transactions on Knowledge and Data Engineering) with citations averaging at 270 (Zheng et al. (2017) almost a thousand citations). The only outlier is a paper from Tasca & Tessone (2018), which despite the low number of citations, provides a good overview on architectural components, so it was included in the review. Table 2 provides an overview of the literature review.

Table 2 - Identified Blockchain components

Paper	Component	Generalisable as
Xu et al., 2016	Data storage	Data Storage
	Consensus mechanisms	Consensus mechanisms
	Network topology	Network Topology
	Blockchain ledger	Data Storage
	Validation	Consensus mechanisms
	Permission	Network Topology
Xu et al., 2017	Decentralisation	Network Topology
	Permission	Network Topology
	Data storage	Data Storage
	Consensus protocols	Consensus mechanisms
Tasca & Tessone, 2018	Decentralisation	Network Topology
	Consensus mechanisms	Consensus mechanisms
	Transaction Model	Data Storage
	Identity Management	Network Topology
Dinh et al., 2018	Network topology	Network Topology
	Distributed ledger	Data Storage
	Consensus	Consensus mechanisms
	Cryptography	Cryptography
	Smart Contract	Application
Zheng et al., 2018	Decentralisation	Network Topology
	Consensus mechanisms	Consensus mechanisms

The literature review has been carried out in this way: the main components cited from each paper have been listed, like in Table 6. So, for each paper, many core components can be identified. From this list, five main categories can be identified: data storage, consensus mechanisms, network topology, cryptography and application. This has been done with a more in-depth analysis of the literature. Some components refer to the same aspects of blockchain: for instance, 'permission' in Xu et al. (2016, 2017) is related to the 'network

topology' since, as it will be further explained in this chapter, for defined network topology, permissions will be distributed in a certain way. With these considerations, 4 main BCT components can be identified:

- Network topology, which defines how the nodes in the blockchain network are connected. This entails determining decentralisation level, permission and identity management. Section 5.3 will address this component.
- Data storage is concerned with where the data will be stored: the options are on-chain or off-chain storage. This will be discussed in section 5.4.
- Consensus mechanism regulates how nodes in the network reach consensus when executing a new transaction. Several protocols are available, and this will be addressed in section 5.5.
- Application component, which implement the business logic in algorithms and smart contracts which are stored in the chain and are automatically executed. Section 5.6 will focus on this component.

Cryptography needs to be separated from the previous since it is not a blockchain specific component, but it is related to information system security in general. The key elements of cryptography will be explained in the next section, before going into the details of the four main BCT components.

5.2. Data security

This section will be necessary to explain some basics of data security, namely cryptography, which will be used throughout this chapter and the design phase. Cryptography is based on two processes: encryption and decryption. Encryption converts information into a secret code in order to hide sensitive data from unauthorised parties. Conversely, decryption reveals information hidden into a secret code. In cryptography, unencrypted data is known as plain text, whereas encrypted data is knowns as cyphertext (Buchmann et al., 2013).

5.2.1. Cryptography

Cryptographic mechanisms are composed of an algorithm (cryptographic function) and one (or more) keys. Only the secrecy of the key (or one of the keys) can guarantee the

confidentiality and authenticity of messages. There are two classes of algorithms (Buchmann et al., 2013):

- Symmetric key algorithms, only one key is used for information encryption/decryption. For instance, the Caesar cypher, a symmetric key algorithm, requires that the message is encrypted by replacing letters of the message with one located *k* positions ahead in the alphabet. So, if the plaintext is "ABCD", with k=4, the encrypted message will be "EFGH". *K* is the key to be shared between the sender and recipient.
- Asymmetric key algorithms, each subject has a pair of private (PR) and public keys (PU). Data is encrypted using the PU of the recipient and decrypted using the PR of the recipient. For instance, the sender (A) encrypts the message with the PU of the recipient (B), and therefore the message can be decrypted only with the PR of B. This will ensure confidentiality. In addition, A should also encrypt the message with his PR. In this case, B must decrypt the message with the PU of A. This will ensure that the message was sent by A. Asymmetric key algorithms are computationally more complicated, since each message needs to be encrypted using the PU of the recipient, whereas with symmetric key algorithms only one key is used. In turn, asymmetric algorithms provide more security.

Hashing

Symmetric and asymmetric encryption algorithms guarantee the properties of confidentiality and authenticity. Hash functions are needed to provide integrity. A hash function is a function that transforms a message into a fixed-length message called hash (Buchmann et al., 2013). The hash function is characterised by:

- consistency since the same hash must be associated with the same messages;
- uniqueness, given that the probability that two different messages are associated with the same hash must be almost null;
- non-invertibility the function must not be invertible, it must be impossible to trace the message from the digest (Buchmann et al., 2013).

The hash functions thus generate the hash that can constitute proof of the integrity of the message (that unauthorised agents do not manipulate it during communication). A sender who wants to send a message can calculate the hash through a hash function and send it attached to the message. Once received by the recipient, he must decouple the message from the hash and recalculate the hash of the message received. If the hash received and that calculated from the message received are the same, then the message is intact, otherwise, the message has been manipulated by unauthorised agents during transmission (Buchmann et al., 2013).

Digital signatures

For safe use of the hash function, the hash must also be protected from external attacks. Consequently, the hash must be used in combination with public-key systems, such as digital signatures. The objective of the digital signature is to guarantee the authenticity of the data and to identify their creator with certainty. The digital signature is defined as the hash encrypted using the PR of the sender (Buchmann et al., 2013). This signature is attached to the message, and the two are sent. In some cases, signature and message are encrypted with the PU of the recipient who must use his PR to decrypt what has been received (Buchmann et al., 2013). Generally, once a signature and message are received, two actions are performed in parallel: recalculate the message hash and decoding of the signature with the PU of the sender. At this point, the two hashes can be compared to understand if the document has been manipulated by unauthorised agents (Buchmann et al., 2013).

5.2.2. Encryption key management

One of the main aspects of cryptography is the generation, management and distribution of keys.

Key pair generation

Systems that support key generation are called PKI (Public Key Infrastructure). These provide methods and tools to perform basic cryptographic functions for a specific community of users, such as (Buchmann et al., 2013):

- issue of public-key certificates (PU and PR), after carrying out the necessary checks technical and procedural;
- revocation of public-key certificates;
- distribution of public-key certificates and information about certificates revoked;
- optionally, a PKI can also provide support for validating one digital signature through identification functions of the time when it was affixed the signature (timestamp), of the role covered by the individual who signed (certification of the role) and why the signature was made (policy signature).

The process is as follows. The user requires a personal certificate from the CA (Certification Authority), which guarantees the identity of the parties and also plays the role of (RA) Registration Authority. Alternatively, the CA may appeal to a trusted third party for the role of RA, in charge of identifying the user, through a particular phase of acquisition of trust credentials. Certificates are stored in a repository appropriately shared, which can be accessed to verify the identity of a part. That repository must also contain information on the status of certificates, which have an expiry date, or they can be revoked at the request of the CA or RA. A Revocation Authority takes care of revoking expired certificates. The revocation of a certificate must be made known to the environment promptly to avoid fraud relating to expired certifications (Buchmann et al., 2013).

To ensure that a certificate cannot be altered, it is protected with the digital signature of the CA that issued it. When a public key is received through a certificate, integrity and validity of the signature must be checked: the hash calculated on the certificate (on the PU and the data associated with it) is compared with the extracted digest by the digital signature affixed by the CA that issued the certificate. If this comparison is successful, the certificate is undoubtedly intact, but it remains to be seen whether the issuing CA is a trusted CA. For this reason, a list of public keys of trusted CAs is maintained. The CA guarantees the validity of a digital certificate. A digital certificate is a document containing information about who is the owner of the PU, the PU itself, and it is signed by the CA to ensure that no one has altered the certificate. This, however, does nothing but move the problem to a higher level: how to guarantee that the PU used to verify the signature on the certificate by the CA, does the CA own it. This requires that even the CA has its certificate issued by another level CA higher.

This is solved by the presence of particular CAs called root CAs. This CA can sign their certificates. The PKI is, therefore, an infrastructure that also includes a CA tree in which it highlights who has issued the certificate to other entities (Buchmann et al., 2013).

Access control methods

In order to define which parties are authorised to access messages, access control methods can be used (Karp et al., 2009). A party requests to access an encrypted document to the document owner. The document owner should assess whether the requesting party is authorised to access the document. For this purpose, several methods are available. The two most common are:

- Role-based access control (RBAC). In RBAC, the roles are firstly determined. Each role is then tied to access authorisation. Finally, each user is given a role. If a user has a role who authorises it to access the document, then it will receive access;
- Attribute-based access control (ABAC). In ABAC, the attributes of a user determine the access. If the user can prove that it has some attributes, and the policy establishes that user with that attribute can access the document, it can access the document (Karp et al., 2009).

The main difference between the two methods is the flexibility: since RBAC relies on roles, it can be harder to establish access policies in dynamic environments, where there is no clear definition of roles. On the contrary, ABAC can be more adaptive, based on the context (Karp et al., 2009).

XACML is a standard used to implement authorisation policies (Crampton, 2005). Four main components characterise the XACML: PEP (policy enforcement point), PDP (policy decision point), PAP (policy administration point), PIP (policy information point) (Crampton, 2005). The user sends an access request to the PEP; the PEP in turns sends a request to the PDP. The PDP screens the request against the access policies stored in the PAP. If the request is valid, the decision is sent to the PEP, which sends it back to the user (Crampton, 2005). The PIP can provide more information on the role in case the request does not contain enough information. In the next section, the four main BCT components are described more in full.

5.3. Network configuration

One of the main features of blockchain is decentralisation: nodes are connected in a peer-to-peer network and execute transactions without relying on central authority (Wright, 2019). The network can be configured in different ways, which will be explained below.

5.3.1. Network Topology

Network topology defines how nodes are interconnected and how transactions are executed (Tasca & Tessone, 2019). Several aspects characterise the network topology: permission to join the network, meaning which real-world entities are entitled to become a node of the network; read permission, determines which nodes can read transactions and information stored in the ledger; write permission, which nodes can perform a transaction and store it in the ledger; consensus determination defines which nodes can take part in the consensus protocol (Tasca & Tessone, 2019; Zheng et al., 2017). In the literature, three main topologies can be identified:

- Public: a public blockchain is a purely decentralised network, with no central control (Dinh et al., 2018; Tasca & Tessone, 2019; Zheng et al., 2017). In a pubic blockchain, anyone can join or leave the network, and all the nodes can take part in the consensus process (Dinh et al., 2018; Tasca & Tessone, 2019; Zheng et al., 2017). Similarly, every node can read and write transactions, keeping its identity anonymous (Xu et al., 2016). This raises privacy concerns since information is accessible from everyone, and there are no control mechanisms to hide sensitive data.
- Consortium blockchain: in this case, only recognised parties can join the network (Zheng et al., 2017). Decentralisation is not absolute since several nodes govern the platform: as a consequence, only authorised nodes can join the consensus process, some nodes might have read permissions and others might have write permission (Dinh et al., 2018; Tasca & Tessone, 2019; Zheng et al., 2017).
- Private blockchain: this represents a peculiar case since the platform is purely centralised into one organisation (Dinh et al., 2018; Tasca & Tessone, 2019; Zheng et al., 2017). In a private blockchain, only nodes from the organisation can join the network, read and write transactions (Dinh et al., 2018; Tasca & Tessone, 2019; Zheng et al., 2017).

One of the main differences among the three types of blockchains is the number of nodes joining the network: a higher number of nodes is expected to be part of a purely decentralised blockchain; conversely, fewer nodes can join the purely centralised blockchain (Zheng et al., 2017). According to Zheng et al. (2017), this is directly connected with scalability and immutability of the platform: in particular, the lower the number of nodes, the higher the scalability, the lower the immutability (Xu et al., 2017; Zheng et al., 2017).

The design choice to establish the level of decentralisation of the platform is to define the network as either "permissionless", like in public blockchains, where nodes can freely join the network, or "permissioned", like in consortium and private blockchain, where only authorised parties can join the network (Dinh et al., 2018; Tasca & Tessone, 2019; Xu et al., 2016, 2017; Zheng et al., 2017). While in permissionless blockchain, identities can be kept anonymous, in permissioned blockchain, two further elements are included: identity management and permission management. According to Karp et al. (2009), four different components have to be defined: identification, authentication, authorisation and access decision:

- Identification links a digital identity and a real-world entity;
- Authentication entails defining a way to ensure that only the defined real-world identity has access to the digital identity;
- Authorisation means granting rights to a digital identity;
- Access decision is the combination of the previous components to decide whether permission is granted (Karp et al., 2009, p.5).

Considering a blockchain network, the identity and permission management can be translated into 1) identify real-world identities (e.g. traders) who have the rights to join the network and provide them with a digital identity, to become a node in the network; 2) define some authentication system which will ensure that only one real-world identity can access the digital identity; 3) define the rights of the digital identity, namely read permission, write permission and permission to join the consensus process; 4) grant the read/write/consensus permissions.

Table 3 summarises the network topology components and design choices. From the requirements defined in chapter 4, it can be argued that a permissionless network does not represent a viable solution: in fact, given the absence of identity and permission management components, requirements of identification, authentication and access control cannot be fulfilled. Thus, only permissioned network characteristics will be further analysed in the next sections. This allows to reduce the number of design options, making it easier for the reader to understand the components. Chapter 6 will provide more explanations for this choice.

Table 3 - Network Topology Component

Topology	Characteristics	Performance	Design choices
Public	• Fully decentralised • Anyone can join or leave the network • Identity can be kept private • Anyone can write or read transactions.	Privacy issues Low scalability High immutability.	Permissionless
Consortium	• Partly decentralised • Control mechanisms on who can join, who can read and who can write transactions.	Privacy preserved High scalability Low immutability	Permissioned Identity Management Permission Management
Private	• Centralised • A control mechanism on who can join, who can read and who can write transactions.	Privacy preserved High scalability Low immutability	Permissioned Identity Management Permission Management

Additionally, it should be argued that the terms public/private blockchain are used to describe the network configuration and not the governance structure, such as public domain blockchain or private domain blockchain.

5.4. Data storage

This section analyses the design choices for data structure and storage. The ledger can be used to store and exchange data, or information can be stored "off-chain" in another database (Tasca & Tessone, 2019). Section 5.4.1 will focus on the former, while 5.4.2 on the latter.

5.4.1. Ledger storage

Transactions in the blockchain ledger are stored in blocks, which are divided into two main parts: the block header and the block body (Zheng et al., 2017). In particular, the transactions are stored in the block body (Dhillon et al., 2017; Zheng et al., 2017). Blocks are linked using cryptographic hash pointers[6]: the content stored in block i*+1* contains the hash of block i, which in turns contain the hash of block *i-1*.

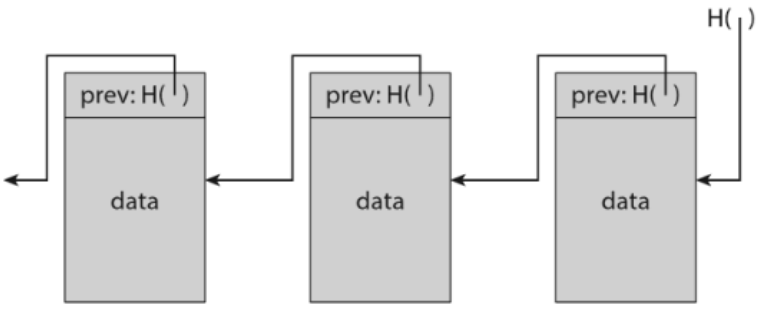

Figure 11 – Hash pointers, retrieved from (Zheng et al., 2017)

This structure allows the transactions to be tamper-proof: in facts, every new block is appended at the end, creating a chain of blocks (hence the name blockchain); so, if the information has to be modified, it would be necessary to tamper with hash pointers back to the beginning, which would be computationally almost impossible. Merkle tree root hash could be used to improve the efficiency, but a detailed description goes beyond the scope of this research (see Narayanan et al., n.d.; Tasca & Tessone, 2018)

Transaction model

The transaction model keeps track of the inputs and the outputs of every transaction, describing how nodes in the P2P network update and store transactions on the ledger (Tasca & Tessone, 2019). Two possible configurations are available for the transaction model:

[6]. A hash pointer is a pointer to the place where some information is stored.

- The Unspent Transaction Model (UTXO): only unspent output transactions can be used as input to new transactions, thus avoiding the double-spending problem (Scherer, 2017; Tasca & Tessone, 2019; Tschorsch & Scheuermann, 2016; Zheng et al., 2017). To simplify, this model works like banknote: for new transactions, you can only use banknotes that you still own, and you have not used previously. This model is beneficial for scalability since multiple transactions can be checked at the same time, and for privacy since the user's identity and status are kept anonymous.
- Account-based model: this model keeps track of every account on the blockchain ledger. Before validating a transaction, the state of each account is checked, to see if the conditions to execute a new transaction are fulfilled. Differently from the UTXO model, where the system keeps track of all the transactions, here the system tracks the state of the account. The state of the account is updated after each transaction. This model works like a credit card: to perform a transaction, the state of the account has to be checked first in order to execute the operation. This enhances efficiency since only one account has to be checked when executing a transaction (Dinh et al., 2018).

Ledger structure

Data stored in the blockchain can be distributed in a single or multiple ledger structure. A multiple ledger structure allows to improve data security, creating access level to read transactions, and scalability since each level will be smaller if compared with a single ledger structure.

5.4.2. Off-chain storage

As mentioned before, data can also be stored in systems out of the blockchain ledger. This leads to advantages in terms of performance, flexibility and cost-efficiency, since a lower amount of information is stored in the ledger, thus reducing the computational burden of the platform (Xu et al., 2017). Furthermore, this setting can improve confidentiality, since sensitive information is not shared directly with other nodes, but are store in a third system (Xu et al., 2017). To enable off-chain storage, a reference to the data has to be stored on-chain. Besides the reference, a hash has to be included. The hash is needed to prove the integrity of the document: the interested party can calculate the hash of the document and

confront it with the hash included in the reference. If the two are equal, the integrity has been preserved.

Table 4 - Data storage

Storage	Characteristics	Subcomponents	Design options	Advantages
On-chain	More immutable	Transaction model	UTXO	Scalability Security
			Account-based	Efficiency
		Ledger structure	Single	Easier
			Multiple	Scalability Security
Off-chain	More scalable, flexible and secure	Reference on-chain Hash		

5.5. Consensus mechanism

This section analyses the consensus mechanisms that can be applied in a blockchain platform. Before diving into the design choices, it is essential to point out what is consensus in blockchain and why it could represent a problem. Consensus can be defined as the process through which nodes validate transactions on the ledger. It is one of the fundamental characteristics of blockchain: there is no central authority which makes sure that transactions are legitimate, so nodes are accountable for this. This set-up brings a problem known as the Byzantine Generals Problem (BG) (Lamport et al., 1982): a group of generals, commanding the Byzantine army, circle a city; there is no consensus on the next move since some generals would like to attack, while others prefer to retreat; however, the attack would succeed only if all the generals will decide to attack, so they have to reach consensus. This scenario represents what happens in distributed network platforms: parties who do not fully trust each other have to reach consensus in order to validate new transactions since there is not a

central node which controls this. As a consequence, protocols are needed to establish the rules to reach consensus.

5.5.1. Consensus protocols

When implementing a consensus algorithm, two main issues have to be considered: Failure Tolerance and Consensus Immutability (Tasca & Tessone, 2019). There are different types of failures (e.g. Byzantine faults, errors), and it is practically not possible to design an infallible system. Concerning blockchain, a fault-tolerant system is capable of keeping functioning in the presence of faulty nodes, granting validity, security and reliability of stored information (Tasca & Tessone, 2019). Information is duplicated on each node so that it is not stored in a central database: as a consequence, efficient consensus mechanisms are necessary to ensure that the version owned by every node is consistent throughout the network. This leads to consensus immutability. Among the primary protocols for Failure Tolerance and Consensus Immutability, Practical Byzantine Fault Tolerance, initially introduced in section 1.4, represents the best viable solution.

PBFT (Practical byzantine fault tolerance)

PBFT is an algorithm which can handle up to 1/3 of nodes which show faulty behaviours, thus ensuring consensus and avoiding BG problems (Xu et al., 2017; Zheng et al., 2017). Transactions are executed in rounds. In each round, a node acts as primary node (or leader) and is in charge of ordering the transaction, whereas all the others are selected as backup nodes (Xu et al., 2017; Zheng et al., 2017). A round is divided into three stages: pre-prepare, prepare and commit (Castro, 2001). A node can enter the next phase after receiving more than 2/3 of votes from the network.

The round starts with nodes proposing new transactions. The primary node firstly orders the transactions and then send the request to all the backup nodes, through a pre-prepare message, which contains a hash to the block proposal. The leader signs the pre-prepare message. Backup nodes check the pre-prepare message validity. If valid, the backup node creates a prepare message and sends it to other backup nodes. Each node checks the prepare message received from other nodes. If a backup node receives valid prepare messages, pointing at the same block proposal from at least 2/3 of the nodes in the network, it creates

a commit message to send to all other backup nodes. If a backup node receives valid commit messages from at least 2/3 of the nodes, the proposed block is inserted into the blockchain.

In PBFT, the identity of nodes has to be known, in order for transactions to be validated. As a consequence, it can be deployed only in permissioned networks, where there is control on who can join the consensus process. It follows that the number of nodes which can join the consensus process has to be limited, given that the number of messages increases with the number of backup nodes: according to Dinh et al. (2018), no major performance issues have been encountered up to 32 nodes joining the consensus process. The transaction throughput makes this algorithm robust, with a rate of transactions per second in the order of tens of thousands.

Proof-of-authority

Proof-of-authority (PoA) is a consensus protocol which overcomes the BG problem by only including trusted parties in the consensus problem (Dinh et al., 2018). Indeed, the central assumption is that nodes will not behave maliciously because they have their reputation at stake, considering that the consensus is executed in a small network (Dinh et al., 2018). In order to become a node in PoA, some conditions have to be fulfilled:

- Validators identity need to be known
- Becoming a validator is difficult and might require time and effort to build a reputation
- There should be a standard selection method for validator nodes

Several nodes (authorities) take part in the PoA algorithm and run consensus to order the proposed transactions. Two different algorithms can be implemented in PoA: Aura and Clique (De Angelis et al., 2018).

In Aura, a round is split into two steps: block proposal and block acceptance. In each round, a leader node sends a block proposal to other authorities. Each authority sends the received block proposal to all other authorities. If all the nodes received the same block proposal, the block is accepted (De Angelis et al., 2018).

Besides the leader, other authorities can propose new blocks in Clique. Each authority is allowed to propose a block every N/2 +1 blocks (N being the number of nodes), which means

at each step N-(N/2+1) nodes can propose new blocks. During a step, when a leader proposes a block, it is directly committed to the chain (De Angelis et al., 2018).

Considering that these algorithms require fewer message exchanges than PBFT algorithms, they are more performant. In particular, Clique is faster than Aura, considering that a block is committed immediately to the chain, and Aura outperforms PBFT. One main pitfall of PoA is that the presence of Byzantine nodes can create issues in terms of integrity. Thus in networks where byzantine nodes could be present, PBFT represents a better option (De Angelis et al., 2018).

In conclusion, two main protocols are available to structure the consensus process. Each protocol has its advantages and disadvantages: PBFT works well in networks where some nodes might show byzantine behaviour, while PoA is most suited in smaller networks with few trusted authorities. PoA outperforms PBFT in terms of transaction throughput. Table 5 summarises this section.

Table 5 - Consensus protocols

Protocol	Characteristics
PBFT	High transaction throughput Resistant to Byzantine nodes
PoA	Highest transaction throughput Not Resistant to Byzantine nodes

5.6. Application

The final component analysed in this chapter is the application component. The application component is determined based on the conditions dictated from the business logic (e.g. determines which information are stored on the ledger and how these are shared among the peers). To design the application component, smart contracts represent a design option.

5.6.1. Smart contract

A smart contract is a computation which runs when a transaction is executed (Dinh et al., 2018; Xu et al., 2016). More simply, it is a formalised procedure. The term smart contract is

misleading since it is not a legally binding contract (e.g. sale contract), but it is an algorithm/code which is stored in the blockchain and is automatically executed after satisfying certain conditions. Its structure (e.g. inputs and outputs) is agreed upon by every node (Dinh et al., 2018).

Different phases characterise a smart contract:

- Development: the first step to develop a smart contract is to reach an agreement on terms and conditions among the actors involved in the blockchain. Then, they can be translated into code, only using if-then-else statements. After that, the code is deployed as a transaction and stored in the blockchain, becoming immutable;
- Awaiting execution: once the code is stored, it waits for an input;
- Execution: an event/message/transaction sent by a node can trigger the execution of a smart contract.
- Finalisation: the output of a smart contract is a transaction, which undertakes the consensus process before being stored in the ledger (Governatori et al., 2018).

A smart contract allows automating the creation of a transaction. Instead of nodes having to propose transactions themselves, the blockchain platform will automatically execute a transaction.

However, nodes could propose transactions without the need for a smart contract. For more basic operations, which do not require specific conditions to be met, nodes can propose a new transaction to other nodes and undertake the consensus process directly. If the nodes agree and validate the transaction, it is appended to the blockchain.

5.7. Conclusions

This chapter aimed to identify main blockchain components and analyse what the design options are and how they affect factors such as security, privacy and scalability. In the next phase, these design options will be cross-checked with the requirements elicited in chapter 4, to define how the components can be designed to comply with the requirements.

Table 6 summarises the chapter and answers SRQ4 *"What are the core blockchain components and design choices to be considered during the design phase?".*

Table 6 - Blockchain components and design options

<table>
<tr><th>Component</th><th>Design choices</th><th colspan="2">Sub choices</th></tr>
<tr><td rowspan="3">Network topology</td><td>Permissionless</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Permissioned</td><td colspan="2">Identity Management</td></tr>
<tr><td colspan="2">Permission Management</td></tr>
<tr><td rowspan="4">Data storage</td><td rowspan="3">On-chain</td><td rowspan="2">Transaction model</td><td>UTXO</td></tr>
<tr><td>Account-based</td></tr>
<tr><td rowspan="2">Ledger structure</td><td>Single</td></tr>
<tr><td>Multiple</td></tr>
<tr><td>Off-chain</td><td colspan="2">On-chain reference
Hash</td></tr>
<tr><td rowspan="2">Consensus mechanisms</td><td>PBFT</td><td colspan="2"></td></tr>
<tr><td>PoA</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Application</td><td>Smart Contract</td><td colspan="2"></td></tr>
<tr><td>Transaction</td><td colspan="2"></td></tr>
</table>

6. Design of the architecture

Before diving into the design of the architecture, a recap of the few chapters is useful. In chapter 3, the TO-BE process description has been provided. This served as input for chapter 4, where the requirements have been elicited: these describe the main constraints that the final architecture should comply with, in order to ensure that the platform will indeed support the exchange of information among actors. In addition, chapter 5 instead focused on BCT, in particular on identifying the core technological components and describe the design options.

The goal of this chapter is to apply chapter 4 and 5 for the design of the architecture by choosing and setting up the BCT components which will comply with the predefined requirements, in order to enable the scenarios described in chapter 3. This will answer SRQ 5 – *How does the architecture of the blockchain-based platform that supports ENS data exchange look?* The design phase will conclude Activity 3 of the DSRM, started in the previous chapter, providing the architecture design.

In order to design the architecture, the network should first be defined: section 6.1 will address this. Section 6.2 will instead focus on defining the data-sharing model, in order to describe how the data sharing and storage will take place. Section 6.3 presents how a smart contract is used in the case analysed. The consensus mechanism will be introduced in section 6.4. Section 6.5 concludes the chapter.

6.1. Network configuration

The network configuration component defines the structure of the peer-to-peer network and which actors will be able to join.

Considering the requirements described in chapter 4, the architecture should support a B2G exchange of information (see *Req. 1* and *Req. 2*), in order to make information available to customs, where carriers are the source. As a consequence, both carriers and customs authorities would need to be represented as a node in the peer-to-peer network. This also means that actors, besides customs or carriers, should not be able to join the network, affecting the blockchain topology. As mentioned in 5.3.1, three main types of blockchain configurations are possible: public, consortium and private. A public blockchain is not a

feasible option since there would be no limits on who can join the network and become a node. Private blockchain, on the other hand, is centralised into a single organisation. Consortium blockchain instead represents the most viable solution for this scenario: only a selected number of nodes is allowed to join the network. The first design choice is then to set up a permissioned blockchain, where European customs and Carriers are allowed to become a node in the peer-to-peer network[7]. The choice to set up a permissioned blockchain is also dictated by the fact that that, in order to ensure confidentiality (*Req. 6, Req. 7*), there is the need for access control mechanisms that a public blockchain cannot provide. This will be further elaborated below. Additionally, A permissioned blockchain allows also to increase the rate of transactions (*Req. 10*).

Being permissioned, identity management, and permission management need to be addressed. These will be described in sections 6.1.1 and 6.1.2, respectively.

6.1.1. Identity management

In order to identify the nodes joining the network, identity management is needed. A PKI is used to enable identity management.

The first step is to issue a PU identity certificate for each customs authority in the European Union, and for carriers which transport products to/through Europe, in order to bind the real-world entity to digital identity. As of today, every country has a National Electronic Identities (e-ID) system (Hulsebosch et al., 2009). This e-ID corresponds to a PU certificate, issued by national CA, in order to access (semi-)public services using the same certificate. According to Pruksasri et al. (2014), the national PU certificate could be used to identify and authenticate

[7]. How the nodes join the network is out of scope.

actors of an international trade lane. This would reduce the steps for joining the platform, considering there is no need to go through the registration process.

At the end of the registration process (outside of the scope of the research), each node will be represented by a pair of private and public keys. Identity management is needed to satisfy *Req. 3: Each user should be registered as one digital identity (identification)* and *Req. 4 Each digital identity must be associated with only one user (authentication)*.

6.1.2. Permission Management

After that, a real-world entity has been identified and authenticated, it should be given several permissions. 5.3Four different permissions have been defined: permission to join the network; read permission; write permission and permission to join the consensus process.

Permission to join the network is based on the PU certificate: once a carrier or customs authority which takes part in the import of goods in the EU is identified through its PU certificate, consortium parties can allow the actor to join the network (*Req. 11*). Read and write permission will be analysed in section 6.2. Consensus process permission will be discussed in section 6.5. The table below summarises the network configuration design choices.

Table 7 – Network configuration design choices

Component	Design choice
Network configuration	Permissioned Consortium Blockchain
Identity Management	Carriers and Customs authority are identified and authenticated through a PU certificate (keypair)
Permission to join the network	All carriers and customs identified through their PU certificate

6.2. Data-sharing model

This section will address the data-sharing model. In initially a reference model will be introduced in section 6.2.1, in order to define the data structure. The next sections will address Data storage 6.2.2 and data security 6.2.3.

6.2.1. Data structure

In order to describe the data-sharing model, the data structure should be defined. To define the data structure, a reference model can provide valuable knowledge. A reference model makes use of a semantic model to represent real-world objects (or trade objects) and make associations between them. The goal is to choose a data structure which allows representing the real-world objects and activities which take part during the sharing of ENS data.

For this study, the reference model from the FEDeRATED consortium has been chosen as the main input for structuring data, since it contemplates the main transport concepts of interest in this research. FEDeRATED is a consortium which goal "is to assist the EU Member States and business to build a future proof federated network of platforms for data sharing in logistics and freight transport" (FEDeRATED, 2020, p.4). In the reference model from FEDeRATED, several Trade Objects are present, as shown in Figure 12 (FEDeRATED, 2020).

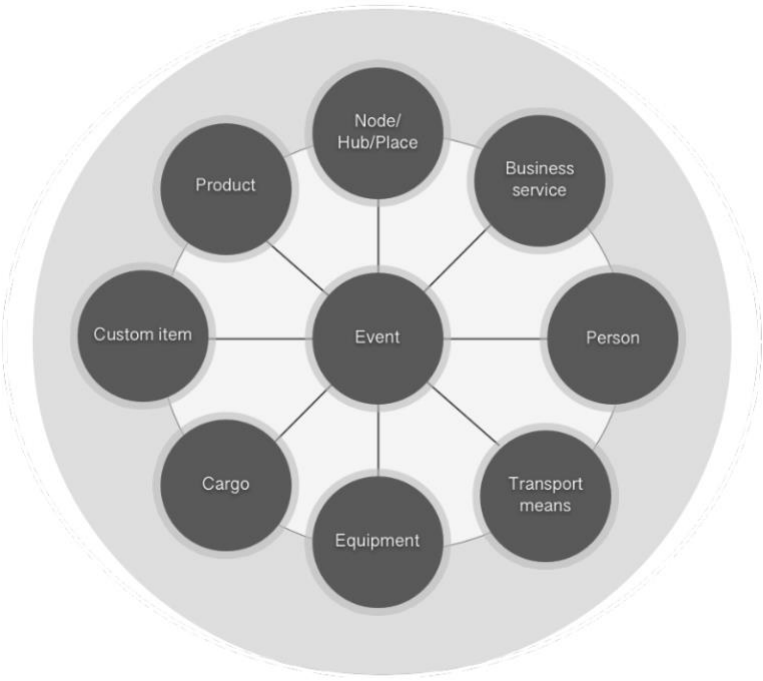

Figure 12 - FEDeRATED reference model, retrieved from (FEDeRATED, 2020)

Considering that some elements are not of interest for the case analysed in this research, the FEDeRATED reference model can be simplified into the data structure represented in Figure 13. The main transport objects are:

- *Port*, which represents the area of interest where transhipment activities (e.g. loading and unloading) take place.
- *Cargo*, which represents the goods transported. Considering that in this research only containerised cargo are investigated; cargo is specialised into *container*;
- *Transport means,* which represent how the goods are transported. Considering that the focus is on deep-sea vessels, transport means is specialised into *vessel.*

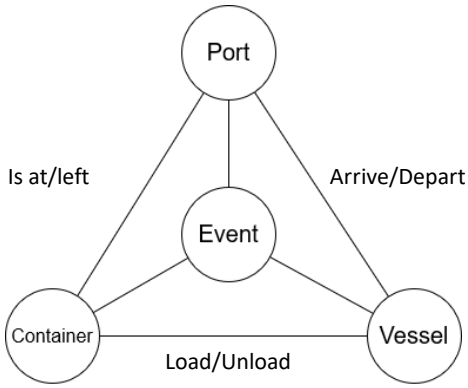

Figure 13 - Data structure (own figure)

Once the model has been represented, the trade objects should be translated into information: this is the concept of digital twin (Boschert & Rosen, 2016). A digital twin is a virtual replication of a real-world object. The three digital twin categories will be port, vessel and container.

The specialisation of the trade objects has been carried out following the semantic model proposed from FEDeRATED, shown in Figure 14 (FEDeRATED, 2020).

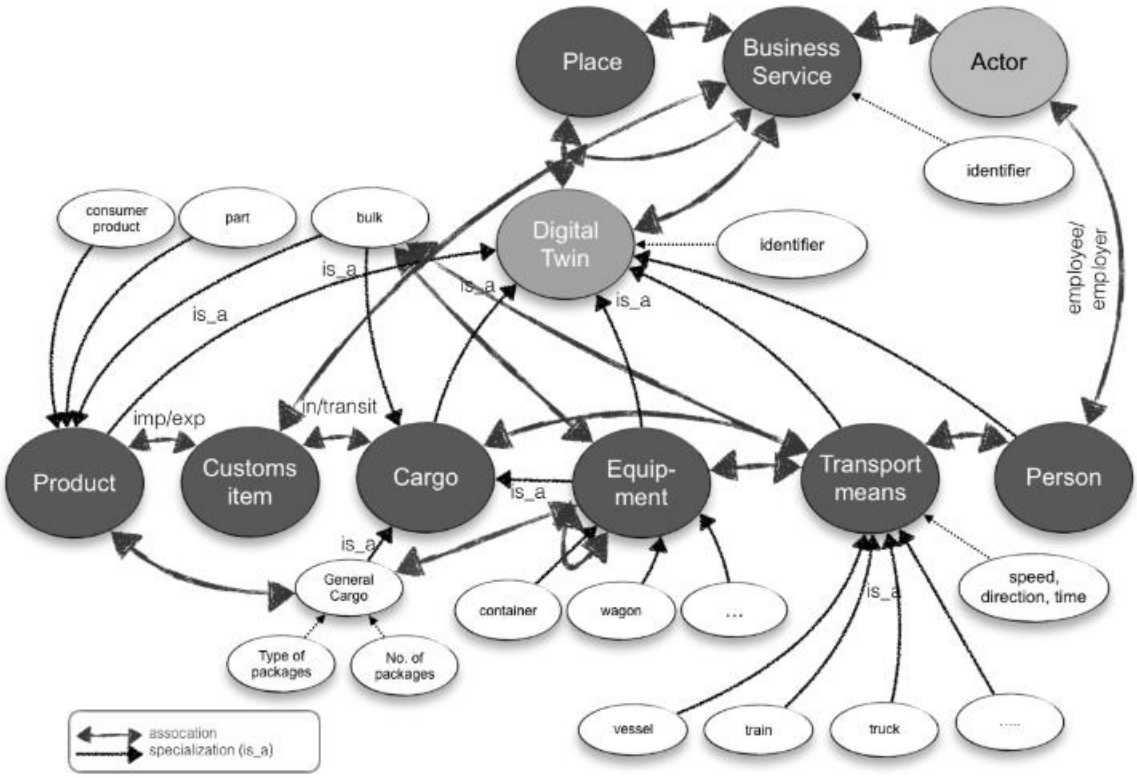

Figure 14 - FEDeRATED semantic model, retrieved from (FEDeRATED, 2020)

The central element of the reference model is the concept of event: an event is the representation of a real-world activity. An event itself creates associations between instances of concepts of the reference model, where these instances represent real-world objects. Each association starts and ends with a milestone, such as an arrival/departure of a vessel in/from a port or Load/unload of a container onto/from a vessel.

The main categories of events are:

- Planned event: the carrier of a shipment is responsible to define and issue the Planned Event. The planned event defines when the vessel is planned to reach a port. For instance, a planned event can be the planned arrival/departure of a vessel to/from a port. The sequence of planned events creates the planned itinerary, where the port planned as first is the first port of call and should receive all the ENS data related to the containers loaded on the vessel. When the itinerary changes, the planned events could be invalidated, so the carrier has to issue an updated plan.

- Expected event: this defines updates to planned events, for instance, delays in the arrival of a vessel. Expected events could make the planned event invalid: for instance, in case of a deviation, the planned event needs to be adjusted.
- Actual event: this category defines events which already took place. In case the actual event deviates from the planned event, the plan can be invalidated and updated.

6.2.2. Data storage

In the architecture that supports the case analysed, each transaction executed is appended to a block stored on a ledger: this ensures that nodes which have a copy of the ledger could access the transactions. In this way, transactions could be used to exchange data among parties. In order to store transactions, UTXO or account-based model are available. Considering that the event allows picturing the state of the transport activities, account-based transaction model can be beneficial in this case. Furthermore, to add a security layer, a multiple ledger structure is beneficial, with a ledger for each carrier. In this way, carriers will not be able to access information on other carriers. Customs, on the other hand, will have access to each ledger. There are no links between different ledgers.

While transactions have to be stored on-chain, documents can be stored both on-chain and off-chain. Off-chain storage allows improving the scalability of the platform in terms of how many transactions per second it can handle (*Req. 10*), as well as providing higher confidentiality levels. As a consequence, off-chain storage of documents represents a better option in this case: ENS will be stored in an external repository, which can be the carrier's ERP system, or a common repository has suggested in the ICS2. In order for the documents to be accessible to third parties, a reference should be stored on-chain: this reference will contain a URI (unified resource identificatory), which will be used as a link to retrieve the document from the document storage. To ensure integrity (*Req. 8*), a hash of the document should be included in the reference. Once an authorised party access the document, a new hash is generated. The fresh-generated hash is compared with the hash stored with the reference: if equal, the document has not been altered.

6.2.3. Data security

Considering that ENS contains sensitive data, such as name and address of consignor and consignee, the access to documents must be restricted. Indeed, since the reference to the document is stored on-chain, every node with read permission could gain access to the source. For this reason, the document is encrypted before it is stored.

Symmetric and asymmetric key algorithms are available. Asymmetric key algorithms could prove to be inefficient in this scenario since it would require each transaction to be encrypted with a different PU key. On the other hand, symmetric key algorithms provide computational advantages: only one key will be used to encrypt/decrypt data. The point is then how to share the key securely. For this purpose, access control methods provide valuable benefits.

Two main access control methods exist: ABAC and RBAC. The main difference in the two methods is the definition of access policies: while in ABAC the access is determined based on attributes that a user can prove to have, in RBAC users with a specific role are granted access. In this case, the goal is to provide authorisation to two categories of users: COFE and COU. Considering then that the role definition is rather smooth, RBAC can provide advantages over ABAC. In particular, the RB-XACML will be used in this case (Crampton, 2005). RB-XAMCL implements role-based access control using the XACML standard.

Besides the encryption of the ENS document, also messages and events need to be restricted: in fact, these contain sensitive commercial information on carriers, which should not be made available to competitors. Asymmetric encryption could provide advantages in this case, especially considering that authentication is necessary to check the source of a message/event. So, a pair of private/public keys will be used by each node when sending a message or submitting events.

Table 8 - Data sharing model design choices

Component	Design choice
Data structure	Port, vessel, container, event
Data storage	Transactions stored on-chain Multiple ledger structure per carrier Documents stored off-chain Reference of the document stored on-chain Account-based model
Data security	Symmetric cryptography (ENS document) Asymmetric cryptography (messages and events) RB-XACML

6.3. Smart contract

The use of smart contracts could provide valuable benefits for improving the interactions between different components of the architecture. Among the main processes that a smart contract could support, the itinerary represents the one where a smart contract could improve the interactions among actors. The itinerary is used in order to check the role of customs.

As mentioned in section 6.2, the data structure is based on events which make associations between different trade objects. When a node submits an event, some conditions have to be met in order for the event to be valid: these conditions are based on the business logic, which is represented in Figure 15. These conditions make sure that the events are consistent: for instance, the planned arrival of a vessel in a port cannot be earlier than the departure of that same vessel from the previous port in the itinerary. Similarly, a planned container unload onto a vessel cannot be earlier than the planned container load onto the same vessel. These conditions can be made explicit through if-then-else statements and stored in the smart contract. Besides, the smart contract can implement dependencies between events in the conditions: if a container is loaded onto a vessel, then the container left the port; similarly, if a container is unloaded from a vessel, then the container is at the port. The reverse is also true.

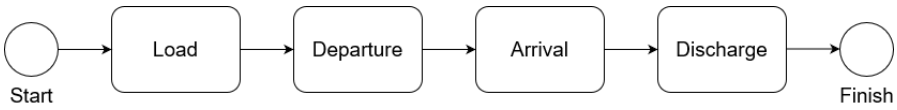

Figure 15 - Business logic sequence diagram, adapted from (Hofman et al., 2019)

The submission of each event calls a smart itinerary contract, where the business logic conditions will be assessed. If the event is valid and does not violate the conditions, it will update the state of the smart contract. The state of the smart contract will represent the itinerary of the vessel and will be updated after every related event is submitted, including any deviation. Once all the planned events are actualised, meaning that for each planned event, a corresponding actual event is submitted, the smart contract can be finally executed. The execution of the smart contract will result in a transaction which will inform all the interested parties that the transport is complete.

Figure 16 shows the structure of the smart contract. The input is the event issued by a node. The conditions will check if the event is valid and, if so, it will update the state of the smart contract, including also dependent events. Once all the planned events are actualised, the smart contract will be executed to notify the completion of the itinerary.

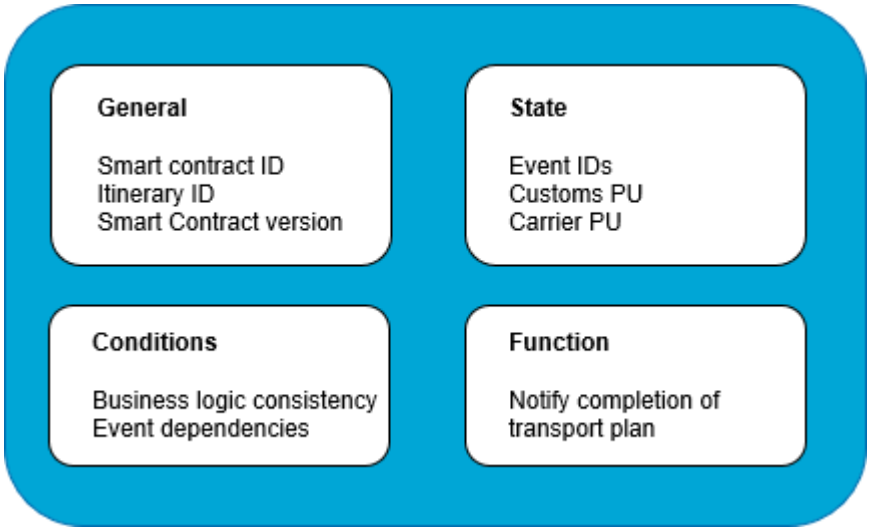

Figure 16 - Smart itinerary contract overview (own figure)

6.4. Consensus mechanism

Considering that all the nodes in the peer-to-peer network have a copy of the blockchain ledger, each transaction needs to be verified before it can be stored in a block, in order to

avoid integrity issues. The consensus process serves this purpose by defining the process of transaction validation. As mentioned in 5.5, several algorithms are available to implement the consensus process. While PBFT consensus mechanism is fault-tolerant thanks to the three rounds which every transaction needs to undertake, PoA only entrusts nodes which have their reputation at stake and will thus not behave maliciously. Considering that the case analysed includes only customs authorities and carriers, the conditions to apply PoA are met since these actors have their reputation at stake and will not behave maliciously: customs are public authorities, while carriers would not risk their reputation, which would result in higher chances of inspections.

Even though Clique (section 5.5) is the fastest algorithm to implement PoA, it could lead to integrity issues, since blocks are committed directly to the chain when proposed by a leader. In Aura instead, all other nodes will check the block proposal sent from the leader before it is accepted.

The consensus mechanism is applied in order to validate the submission of ENS reference on the platform. The carrier, which acts as a leader node, will send the block proposal to other authorities: in this case, the authorities are the COFE and the COU. Each authority will perform risk assessment using the ENS data and, if the risk assessment is positive, will send the block proposal to the other authority. For instance, the COFE receives the block proposal; the COFE retrieves the ENS data and will perform risk assessment; if the risk assessment is positive, will send the block proposal to the COU. Meanwhile, the COU will perform the risk assessment as well and will send the block proposal to the COFE in case of positive risk assessment. If each authority receives the same block proposal, the block is accepted. If during the risk assessment, the risk is deemed to be too severe, the customs authority will not accept the block proposal. This will function as a DNL notification for the carrier, which cannot load the container onto the vessel. In this way, the consensus mechanism covers the pre-loading risk assessment.

6.5. Conclusions

The architecture should support a B2G exchange of ENS data: carriers make data available to customs authorities by providing access to ENS based on the itinerary of the vessel (*Req. 1*,

Req. 2). The peer-to-peer network is thus made up of carriers and customs authorities. In order to identify the actors joining the network and tie the real-world entities to one digital identity, PU certificates are used: each actor is univocally identified by a pair of private and public keys (*Req. 3*, *Req. 4*). Every European customs and carrier involved in the transport of goods in Europe are allowed to join the network (*Req. 11*). In order to define how data are shared, firstly the data structure should be delineated. Using the reference model from FEDeRATED, the data structure consists of event-based associations between ports, carriers and vessels which support the main physical activities tied to the submission of ENS data (*Req. 9*). Events are stored on-chain, on a smart contract. The architecture uses a multiple ledger structure. ENS data are stored in an off-chain repository: this could be the carrier's own IT system or a central repository as proposed in ICS2 (*Req. 5*). A reference to the ENS is stored on-chain, together with a URI and a hash of the document (*Req. 8*). In order to avoid confidentiality issues, symmetric encryption is deployed with the use of role-based access control, to control the access to the ENS document. The platform also makes use of asymmetric cryptography, in order to authenticate nodes issuing messages, transactions or events. This allows only COFE and COU to access ENS data (*Req. 6*, *Req. 7*, *Req. 8*). PoA Aura has been selected as a consensus algorithm, where the leader node is the carrier submitting ENS, and the COFE and COU are the validating authorities. Overall, using a permissioned blockchain, off-chain document storage, and PoA allows achieving a high rate of transactions per second (*Req. 10*).

Table 9 - Architecture design choices

Component	Design choice	Requirements addressed
Network configuration	Permissioned Consortium blockchain	Req.10 (Scalability)
Identity Management	Carriers and Customs authority are identified and authenticated through a PU certificate (key pair)	Req.3 (Identification) Req.4 (authentication)
Permission to join the network	All carriers and customs identified through their PU certificate	Req.1 (Customs access to ENS data) Req.2 (Updates on itineraries)
Data structure	Port, vessel, container, event	Req.9 (Availability)
Data storage	Transactions stored on-chain Multiple ledger structure per carrier Documents stored off-chain Reference of the document stored on-chain Account-based model	Req.5 (Concealment) Req.6 (Access Control) Req.7 (Access Control) Req.8 (Integrity) Req. 10 (Scalabilty)
Data security	Symmetric cryptography (ENS document) Asymmetric cryptography (messages and events) RB-XACML	Req.5 (Concealment) Req.6 (Access Control) Req.7 (Access Control)
Smart contract	Smart itinerary contract	Req.2 (Updates on itineraries)
Consensus algorithm	PoA	Req. 10 (scalability)

7. Demonstration

The previous chapter provided architectural design choices. The next step is to demonstrate how the architecture function to solve the problem at stake. This chapter addresses the demonstration and answers SRQ 6 - *How can the blockchain-based platform be used to share ENS data?*

A walkthrough will be used for demonstration purposes, showing different functionalities that the blockchain-based platform can support.

The demonstration will start by describing how the ENS is published in section 7.1. Section 7.2 describes the digital twin registration: understanding how the digital twin is structured is essential to describe how future transactions can refer to it, for instance, how an association between port and vessel takes place. After that, the events will be described: the events create an association between digital twins (section 7.3) Explaining events is necessary to describe how the itinerary is constructed and updated (7.4). The itinerary state is used in order to allow customs to access encrypted information, and section 7.5 explains how customs can retrieve ENS documents.

7.1. Publishing the ENS

The architecture does not foresee the lodging of ENS data directly on the platform. Instead, ENS data are stored in an off-chain repository. Carriers encrypt the document, using a symmetric key, and then store the document in its ERP or a shared repository. After that, the key is stored in the key storage, and the reference to the document is stored on-chain.

This reference contains the Master Reference Number (MRN), the hash and URI.

Table 10 - ENS hash reference

Element	Value
Transaction ID	11148d8f6ad4d4f24b1a3e91b11f69d925a2bd03409bb4f0f486f13d311aea88
MRN	01AB01234C56789012
URI	http://www.trustedstore.com/01AB01234C56789012
Hash	b4f0f486f13d311aea88a3e91b11f69d925a2bd03409b11148d8f6ad4d4f24b1

7.2. Digital twins' registration

The registration of a digital twin is carried out as a transaction. The transaction will register the digital twin as an asset and the node executing the transactions is the owner of the asset: for instance, a carrier registering a vessel as an asset is the owner of the asset and thus is responsible for it.

7.2.1. Port

The registration of the port digital twin takes place as a transaction, that can be carried out by the responsible customs authority. The port digital twin will contain information on the responsible customs PU, digital signature (in order to verify that the responsible customs performed the transaction) and the port code, as defined from the UNECE. In this example, the digital twin of the Port of Rotterdam is shown.

Table 11 - Port digital twin

Element	Value
Transaction ID	9dbee948341e52213979fd3db3c9dc994d2e31fd9d92e99788bd9cc15ba678e0
Owner`s PU	NL Customs PU
Owner`s Digital Signature	NL Customs Digital Signature
Port Code	NLRTM

7.2.2. Container

The registration of containers can be carried out by the carrier responsible for its transportation through Europe. The container digital twin contains information on the carrier in charge of the transportation (PU and digital signature) and the container number, following the standard ISO 6346 (ISO, 1995). Additionally, the container digital twin includes the MRN, which is a number generated to identify univocally an ENS (DG TAXUD, 2016).

Table 12 - Container digital twin

Element	Value
Transaction ID	9449ff635930930e709c362af4d2fdc0063beb35a1b4ba7333539fdd4763024c
Owner`s PU	Carrier PU
Owner`s Digital Signature	Carrier Signature
Container number	ABCD1234567
MRN	01AB01234C56789012

7.2.3. Vessel

The vessel digital twin registration can be carried out by the carrier responsible for its transportation. The vessel digital twin contains information on the carrier in charge of the transportation (PU and digital signature) and the Unique vessel identifier (UVI)[8].

Table 13 - Vessel digital twin

Element	Value
Transaction ID	11148d8f6ad4d4f24b1a3e91b11f69d925a2b d03409bb4f0f486f13d311aea88
Owner`s PU	Carrier PU
Owner`s Digital Signature	Carrier Signature
UVI	TUVI-1234567

7.3. Creating the itinerary

Creating the itinerary is instrumental in providing access to the right customs. Based on the planned events, the itinerary of the vessel will be defined. Based on the itinerary, the COFE can be identified. The planned load/unload of vessels from the containers allows identifying the COU.

The events have a dual structure: the asset part, which make an association between two assets, and the transaction part, which gives the state of the event. The asset part is the static

[8] http://www.fao.org/global-record/background/unique-vessel-identifier/en/

part of the event since the association between two assets does not change throughout the execution of the plan: this contains the assets IDs and assets types. What changes is the transaction part, where the state of the event is described: this contains the status (e.g. planned, expected, actual), the date, the PU of the issuing node, the timestamp and the Event ID.

Table 14 - Event structure

Part	Element
Transaction	Event ID
	Timestamp
	Smart Contract ID
	Itinerary ID
	State
	Date
	PU.Issuer
Asset	ID.Asset1
	ID.Asset2
	Type.Asset1
	Type.Asset2

7.3.1. Vessel-port association

In order to associate a vessel and a port, a planned event has to be issued. The planned arrival and departure of a vessel from a port creates the itinerary of the vessel, where the first port of call in the timeline of events will be the COFE.

Table 15 - Vessel-port event example

Element	Value
Event ID	Event1
Timestamp	Timestamp1
Smart Contract ID	SmartContract1
Itinerary ID	Itinerary1
State	Planned arrival
Date	03/09/2020 06.30
PU.Issuer	PU Carrier
Digital signature issuer	Digital signature Carrier
ID.Asset1	TUVI-1234567
ID.Asset2	NLRTM
Type.Asset1	Vessel
Type.Asset2	Port

The vessel-port event contains a reference to the port digital twin and the vessel digital twin. This is needed to include the identities of the Customs authority and carrier (PU and PR).

7.3.2. Container-vessel

The next associations to be made are between the vessel and the containers to be loaded onto the vessel. This can be done by issuing a planned loading of a container onto a vessel,

Table 16 - Container-vessel event

Element	Value
Event ID	Event2
Timestamp	Timestamp1
Smart Contract ID	SmartContract1
Itinerary ID	Itinerary1
State	Planned load
Date	02/08/2020 06.30
PU Issuer	PU Carrier
Digital signature issuer	Digital signature Carrier
ID.Asset1	ABCD1234567
ID.Asset2	TUVI-1234567
Type.Asset1	Container
Type.Asset2	Vessel

7.3.3. Container-Port

The container-port association is an event which can be issued by the carrier or can be automatically generated by the smart contract as a result of dependency from a load/unload event.

Table 17 - Container-Port event

Element	Value
Event ID	Event3
Timestamp	Timestamp1
Smart Contract ID	SmartContract1
Itinerary ID	Itinerary1
State	Planned unload
Date	04/09/2020 07.30
PU Issuer	PU Carrier
Digital signature issuer	Digital signature Carrier
ID.Asset1	ABCD1234567
ID.Asset2	NLTRM
Type.Asset1	Container
Type.Asset2	Port

All the events will be stored in the smart contract. The state of the smart contract will contain all the complete itinerary, identified by the itinerary number. Figure 17 shows an example of a itinerary.

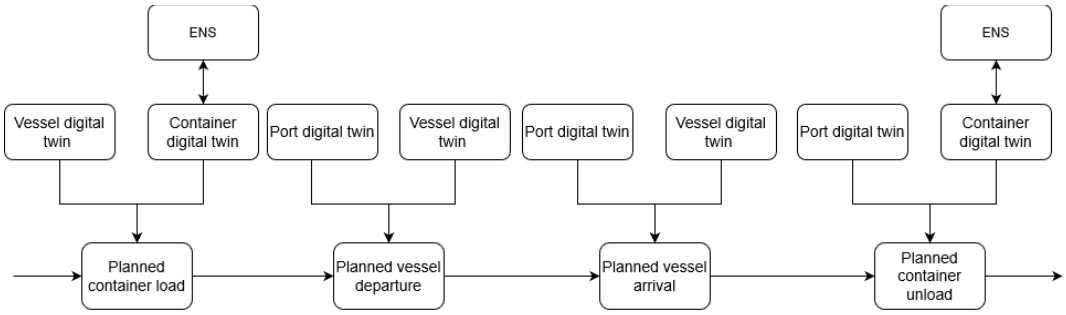

Figure 17 - Itinerary state example (own figure)

7.4. Updating the itinerary

Unexpected events can make an itinerary unfeasible. If this is the case, new planned events need to be issued. Changes can affect both the itinerary of the vessel, for instance, changes in the COFE or subsequent port of calls, or changes in the load/unload of containers. New planned events will have the same itinerary number, will call upon the same smart contract, but will have a different timestamp, in order to specify that the event is a new version of the plan. The new issued events will update the state of the smart contract.

7.5. Retrieve of ENS data by customs authorities

Whenever a carrier issues vessel-port events, the customs authority will be notified thanks to the association between the vessel digital twin and the port digital twin (which contains the responsible customs authority's PU). In case the event is the first version of the plan, the customs will also receive the block proposal, so that it can perform pre-loading risk assessment and carry out the consensus process, before accepting the block. Otherwise the event is an update to the itinerary. The main information customs obtain from the notification is the itinerary number, which will be used to obtain the decryption key.

When a customs authority needs to access ENS data of incoming cargo, it sends a request to access the document to the PEP (1- Figure 18). The request takes the form of a message, which contains the PU and digital signature of the customs, together with the itinerary

number. The PEP validates the integrity of the message by cross-checking the PU and the digital signature of the message: if the two match it means that the customs authority sent the message and not another party. The request is forwarded to the PDP (2). The PDP queries the blockchain ledger to check the itinerary (3), stored in the smart contract identified through the itinerary number, and whether the sender is an authorised party (e.g. is the COFE or the COU). Initially, the itinerary is identified, using the itinerary number provided by the sender. Once the itinerary is identified, the PDP uses the itinerary as input in the access policies (4-5).

Table 18 - Request message

Element	Value
Sender PU	Customs PU
Sender digital signature	Customs digital signature
Itinerary number	Itinerary1

The access policies are algorithms defined using a structured language, as shown in Figure 20. The algorithm first iteration is to find the first planned event where there is an association where the Customs PU matches the sender PU. In case there is no match, it means that the sender is not included in the itinerary, thus does not have a role. Otherwise, the first event where the PUs match, is a planned arrival of a vessel: this is ensured by the business logic of the itinerary since the vessel must plan to arrive at a port before it can perform load/unload of containers or departure. Next, if the event is the first planned arrival in the itinerary, it means that the port is the first port of call, and the responsible customs authority is the COFE. The result is that the sender act as a COFE for the itinerary. The PDP communicates the decision to the PEP, which will provide the sender with the decryption key for all the containers loaded onto the vessel. If the planned arrival is not the first planned arrival in the itinerary, the algorithm will check the next event scheduled in the itinerary. Three scenarios are possible, based on the business logic:

1. the event is a planned departure, which means that the vessel will arrive at the port and depart without performing load/unload of containers, thus the sender does not have a role in the itinerary;
2. the second scenario is that the event is a planned load, which means that the vessel will only load containers in that port without performing any unload, thus the sender does not have a role in the itinerary;
3. the final option is that the event is a planned unload of a container in that port, thus the sender has the role of COU in the itinerary.

The PDP communicates the decision to the PEP (6). The PEP will retrieve the decryption keys from the key storage (7) and will send them to the customs (8). The messages are encrypted using the requester PU. The requester will decrypt the messages using its PR, and then will use the decryption keys to decrypt the ENS.

Once the customs has decrypted the ENS document, it will generate a new hash and compare it to the hash attached to the document, to check if the ENS has been tampered. If valid, then the customs has access to valid and integral ENS data on the container. Now the customs can perform risk assessment procedures or consult the ENS to obtain information on incoming cargos. Figure 18 shows the exchanges. All the components are stored in the blockchain ledger.

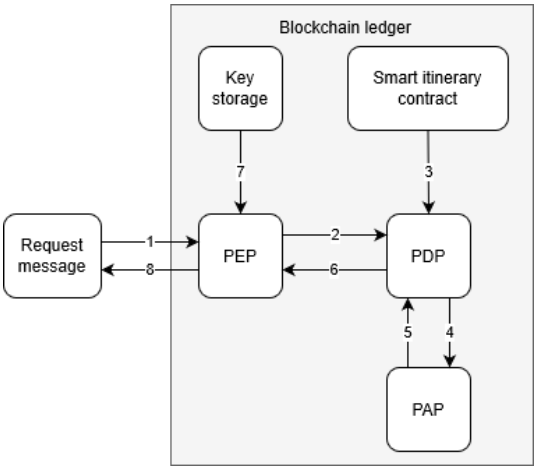

Figure 18 - Decryption key exchange messages (own figure)

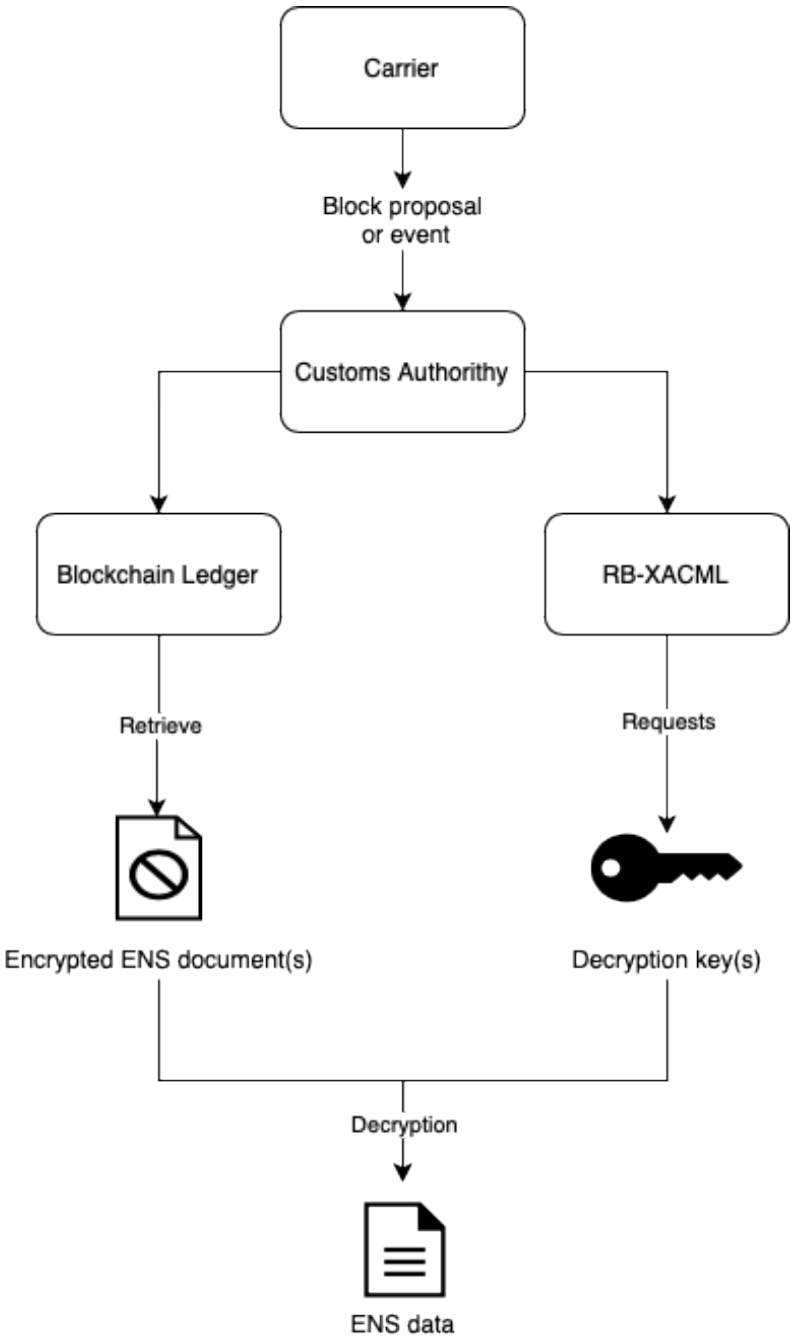

Figure 19 - Steps to access ENS data (own figure)

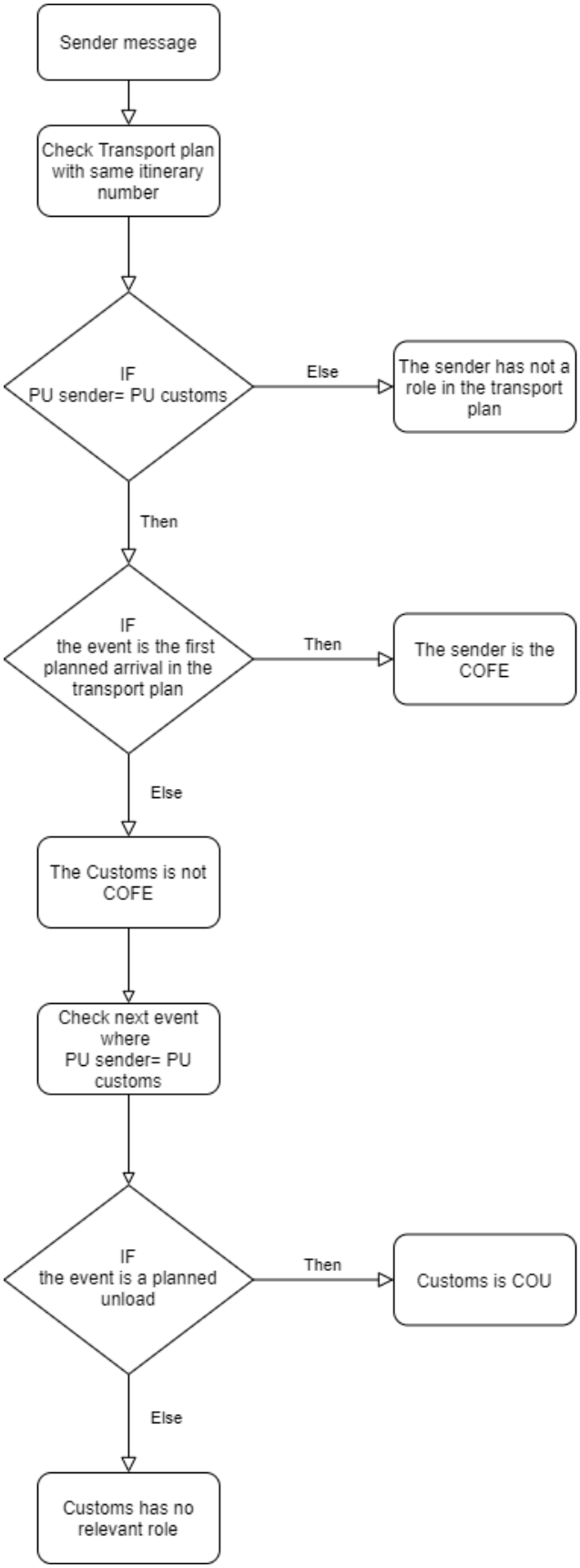

Figure 20 - Access policies algorithm (own figure)

7.6. Conclusions

This chapter provided a demonstration of how the platform can be used in order for a customs authority to access the correct ENS data. The process starts with a carrier encrypting the ENS document and store it in an off-chain data storage, store the decryption key in a key storage and publish the ENS reference on-chain. Next, the itinerary is created by submitting events which call upon a smart contract and with the same itinerary ID. The itinerary can be updated by submitting new planned events, with a new timestamp, which will substitute the previous events and update the state of the smart itinerary contract. It is important to notice that the itinerary number stays unchanged in case of itinerary changes. When a customs authority wants to access ENS data, it will send a request to the PEP. The PEP validates the request and forwards it to the PDP, which will query the state of the smart contract and cross-check it with the access policies, using the PU f the sender. The PEP will send the decryption key to the customs if it has a relevant role in the itinerary. The customs authority decrypts the documents, validates its integrity, and then accesses the ENS data.

It is interesting to notice that the main functionalities of the platform address the ENS data sharing and access: to make ENS data available to the right customs authorities is in fact the main goal of the platform. Risk result sharing is instead an implicit functionality of the platform: during the consensus process, the involved customs authorities will share their risk result among each other, in order to check whether the goods can be loaded onto the vessel. This covers the pre-loading risk assessment, but does not address the pre-arrival risk assessment, which instead assesses whether the cargo should be inspected or not, and the inspections results. As a result, new customs authorities (COFE or COU) can only get access to ENS data.

8. Evaluation

Chapter 6 provided a description of the design choices for the architecture, and chapter 0 demonstrated how the platform could support the exchange of ENS data. This chapter will evaluate the designed ENS platform and answer *SRQ 7 - How does the designed platform rate compared to an existing platform in the shipping industry in terms of scalability, security, trust, and immutability?* This can be regarded as a feasibility evaluation, to check how the ENS platform would perform in a real-world setting, taking the key hindering factors as a point of reference

In section 8.1, the ENS platform will be compared with TradeLens, since it represents the most popular (based on the number of transactions and end-users) existing blockchain-based platform which supports shipping processes. In section 8.2, the two platforms will be evaluated. Section 8.3 concludes the chapter.

8.1. Comparison

Developed by IBM (technology leader) and Maersk (Ocean Carrier), "TradeLens is an open and neutral supply chain platform underpinned by blockchain technology" (Tradelens, 2019, p.2). The goal is to enable supply chain visibility and spur global supply chains by capturing data directly from the source.

TradeLens solution is made up by three components:

1. Ecosystem (aka network configuration) which comprises private firms, such as carriers and freight forwarders, and governmental organizations, including customs authorities.
2. Platform which interconnects the ecosystem through a set of APIs based on blockchain technology. Actors in the network can share and access information using the APIs.
3. Marketplace where new services can be published on top of the platform, to foster innovation (Tradelens, 2019, p.3).

TradeLens represents as of today, one of the leading examples of a blockchain-based platform which supports shipping processes and interactions, with 10 million events and more than 100.000 documents handled per week (Tradelens, 2019, p.2). A comparison can provide valuable insights in terms of how the design options chosen in this research could perform in a real-world setting. In particular, the ecosystem and the platform components of TradeLens will be taken into account. To compare the two platforms, the design components network configuration, data sharing model and consensus mechanism will be compared individually in the following sections.

8.1.1. Network configuration

The network configuration is concerned with which actors are allowed to join the peer-to-peer network. Both TradeLens and the ENS platform are based on a permissioned network. While the ENS platform consists of a peer-to-peer network where only carriers and customs authorities can join as a node, several different actors (e.g. consignor, consignee, freight forwarders) are part of the TradeLens network (Tradelens, 2019). As a result, the TradeLens network consists of a more heterogeneous set of actors compared to the ENS platform.

The main reason why the networks are structured in such a different way is driven by the different goals of the two platforms. While TradeLens is designed to support the main logistics processes of actors involved with the shipment of goods, with a high B2B focus (even though also customs authorities can benefit from the platform) (Tradelens, 2019), the goal of the ENS platform is to support the B2G exchange of ENS data between carriers and customs: since only carriers and customs are involved in this exchange, other actors are not included in the network. This choice is also supported by the assumption made in section 3.5 that only carriers submit the ENS.

Regarding the identification and authentication of actors joining the network, a PKI is used in the ENS case. TradeLens, on the other hand, uses tokens: an access token is provided by a Cloud Identity and Access Management component in order to identify users; this token is then passed to a Solution Manager component, which keeps track of onboarded

organisations; if identified, they are granted a bearer token, to authenticate the user in the platform (Tradelens, 2019).

This section introduced the differences in the network configuration component, which are summarised in Table 19. The implications of these differences will be explained in section 8.2.

Table 19 - Network configuration comparison

Component	ENS platform	TradeLens
Network	Customs and carriers	Customs, all private organisations
Identification and authentication	eID	Tokens Cloud identity and access management Solution manager

8.1.2. Data sharing model

For comparison purposes, how data are structured in TradeLens will be described first. In TradeLens, the UN-CEFACT reference data model has been used to represent three Trade Objects: shipments, consignments and transportation equipment (TradeLens, 2020).

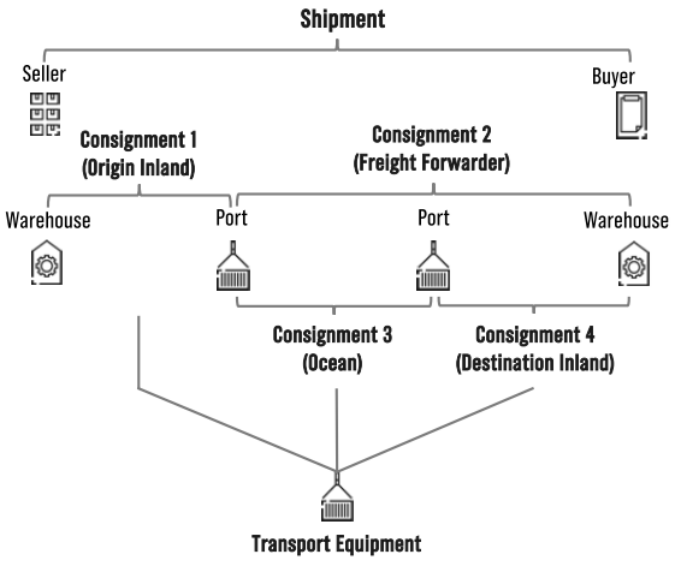

Figure 21 - Relationships between trade objects in TradeLens (2020)

Figure 21 is an example that describes the relations between different trade objects. A shipment is associated with two different consignments if for instance buyer or seller have subcontracted the transport of cargo from the warehouse to the port of origin, and a freight forwarder from the port of origin to the warehouse. The freight forwarder, in turn, has subcontracted transport from port of origin to port of destination to a carrier and the transport from port of destination to the warehouse to another actor. All relationships are associated with the same cargo (container) (TradeLens, 2020). Also, TradeLens makes use of events to create associations between trade objects.

The data structure used by ENS platform is based on three interrelated trade objects (vessel, container and port) which are associated through events. TradeLens, on the other hand, is based on a shipment-consignment-transport equipment data structure, also supported by events (TradeLens, 2020). This last structure allows to support logistic processes mainly from a B2B perspective: for instance, a shipment from the consignor to consignee can be divided into several consignments such as from consignor to port and from port to consignee. The designed data structure instead allows to support events which are related with the submission of ENS by the carrier to customs, like the load/unload of a container onto/from a vessel, or the arrival/departure of a vessel to/from a port.

Concerning data storage, both platforms make use of a multiple ledger structure per carrier. Documents are stored off-chain in both the ENS platform and TradeLens (TradeLens, 2020)While events are stored on-chain in the ENS platform, TradeLens makes use of an Enterprise Service Bus (ESB) to lodge the events (TradeLens, 2020). The ESB is connected with the blockchain ledger and triggers a permission mechanism based on the events submitted. This difference is crucial: by lodging events directly on the platform, the blockchain immutability is utilised to have a tamper-proof track of all the events which are planned or already took place (Dinh et al., 2018; Tasca & Tessone, 2019). The track of events has a crucial role in determining the permissions in both platforms.

In TradeLens, each actor is assigned to a participant type (e.g. Ocean Carrier. Rail Operator, Truck Operator, Customs Authority, Port Authority) and a participant role (Seller, Buyer, Consignor, Consignee, Import Authority, Export Authority). While the participant type does not change, the role of a trader can change based on the trade object: for instance, a customs

authority can be an importing authority in case of incoming goods, as well as an export authority in case of outbound goods (TradeLens, 2020).

Depending on the role played in a shipment, consignment or transport equipment, a participant might have read permissions or obligations to provide data. For instance, the carrier of a consignment/transport equipment is obliged to share planned/actual arrival/departure of a vessel, while the import authority will have access rights to read this information (TradeLens, 2020). These events are published on the ESB. Based on the role-based model, these events become available to interested parties.

Table 20 - Data sharing model comparison

Component	ENS platform	TradeLens
Data structure	Events, vessel, container, port	Events, shipment, consignment, transport equipment
Ledger structure	Multiple ledgers per carrier	Multiple ledgers per carrier
Data storage	Documents off-chain Reference on-chain Events on-chain	Documents off-chain Events on ESB
Access control	Role-based access control	Role-based access control

8.1.3. Consensus mechanism

TradeLens makes use of PBFT consensus algorithm to implement the consensus mechanisms, while the ENS platform is based on PoA (Tradelens, 2019). PoA provides computational advantages over PBFT, but it relies only on trusted nodes to undertake the consensus mechanism (De Angelis et al., 2018). In the case analysed, carriers and customs authorities are trusted parties and have their reputation at stake, so it is unlikely that they will behave maliciously. On the other hand, given the multitude and heterogeneity of logistics parties which take part in TradeLens, PoA does not represent a viable design option, since it would not be fault-tolerant against malicious nodes. PBFT, on the other hand, provides fault tolerance against Byzantine nodes (Castro, 2001).

Table 21 - Consensus protocols comparison

Component	ENS platform	TradeLens
Consensus algorithm	PoA	PBFT

This section presented the main differences between the ENS platform and TradeLens. Most of the differences are due to different objectives: while TradeLens is a solution which aims at improving document sharing among actors in the same supply chain, the ENS platform addresses the availability of ENS data to the right customs authority.

8.2. Assessment

The evaluation of the ENS platform will be carried out by analysing how the two platforms score in terms of scalability, security, trust and immutability. These factors were identified by different authors (Zheng et al., 2017; Chang & Shi, 2019; Batubara et al. 2018; Rossi et al., 2019) as key challenges for the adoption of blockchain-based platforms (see sections 1.3-1.4)

8.2.1. Scalability

The term scalability applied in the context of platforms which support the exchange of information among actors can be referred with two factors: a) ability to handle a high and an increasing number of interactions (Rossi et al., 2019) or b) ability to handle a high and an increasing number of actors (Vukolić, 2016).

Regarding a) several components contribute to the number of transactions that a platform can handle. The consensus mechanism represents a critical factor which influences the throughput of a blockchain-based platform: TradeLens, which deploys a PBFT algorithm could theoretically reach a rate of 10.000 transactions per second. By deploying PoA, the ENS platform can outperform TradeLens: PoA algorithms are characterised by fewer rounds and fewer messages to be exchanged among nodes to reach consensus when compared to PBFT (De Angelis et al., 2018). TradeLens provides off-chain storage of documents and events are stored into an external component. The ENS platform instead foresees the submission of events directly on the platform, while documents are stored off-chain. This also increases the rate of transactions (Xu et al., 2017).

Concerning b) the network configuration plays a role: TradeLens network is a heterogeneous mix of different private and public organisations, whereas the ENS platform only accommodates carriers and customs authorities. Firstly, the designed architecture can provide advantages in terms of performances, since a bigger network would need to sustain a higher rate of transactions per second (Dhillon et al., 2017; Dinh et al., 2018; Tasca & Tessone, 2019). Secondly, this also affects the average number of actors which join the platform concurrently: TradeLens needs to accommodate a higher number of nodes, thus requiring higher scalability. A second key factor is the identification process: TradeLens uses tokens to identify and authenticate parties in the network (see section 8.1.1), which could be computationally more demanding. If multiple actors join the platform simultaneously, TradeLens could potentially face issues of latency. Using eIDs instead, provides benefits in terms of efficiency, since the registration process is not undertaken by the platform, but takes place externally.

As of today, TradeLens handles 10 million weekly events and more than 100.000 documents, which total respectively 520 million events and 5.2 million documents yearly. The expected volumetric of the ENS platform (see Appendix A – Expected volumetric) instead is estimated as much as 565 million events and 87 million ENS document per year. The ENS platform is scalable enough to handle this volumetric (10.000+ transactions per second).

8.2.2. Security

Confidentiality is one of the main requirements to ensure security in IT systems. Several components of the ENS platform address confidentiality, among which the ledger structure and the data storage. The designed ledger structure foresees a ledger per carrier so that each carrier has only access to its data and cannot obtain information on other carriers. Likewise, TradeLens uses a multiple ledger structure divided per carrier. Nevertheless, the difference is in the nodes which join the ledger: in the ENS platform, only customs authorities have read permission on each ledger. In TradeLens, various private organisations will have access to different ledgers: this could lead to loss of confidentiality, as well as businesses being reluctant to join the network. A second component which directly influences security is data storage.

8.2.3. Trust

Trust can be defined as confidence that parties will not behave opportunistically (Engelenburg et al., 2019). A trusted network is one where nodes are represented by actors which are not expected to behave maliciously. This is most certainly the case of the ENS platform since carriers and public authorities are trusted actors, the former having their reputation at stake and the latter being a public authority. In TradeLens, the multitude of different actors which take part in the network could result in trust issues, since there will be less mutual control.

The second dimension of trust is trust in technology (Ølnes et al., 2017). Besides trust in BCT, trust should also be analysed for external components which interact with the blockchain-based platform. TradeLens uses several additional components, such as the ESB or the Cloud identity and access management. If the events are stored in a non-blockchain-based component like the TradeLens ESB, there would need to be trust in the technology and the parties responsible for it, which would put more emphasis on the governance. Instead, only the external data storage would need to be trusted in the ENS platform: this could take the form of a shared repository, or it can be each carrier's ERP system. The main difference with the last case is that the carrier can choose whether to store data in a common repository (this would require to be trusted), or in their own IT systems (with the assumption that a carrier will undoubtedly trust its own IT systems).

8.2.4. Immutability

Immutability is one of the main features of BCT: blocks are appended to a chain, with a hash to previous blocks, which make it nearly impossible to tamper information already stored (Zheng et al., 2017). Immutability thus needs to be analysed for data stored off-chain. In TradeLens, storage of events outside of the blockchain-based platform does not ensure an immutable record of lodged events. The ENS platform instead can achieve an immutable record of events, since these are published directly on the platform. On the other hand, the ENS platforms stores documents off-chain: nevertheless, through hashing, integrity checks can be performed to ensure immutability.

8.3. Conclusions

This chapter addressed the evaluation step of the DSRM and answered *SRQ 7 - How does the designed platform rate compared to an existing platform in the shipping industry in terms of scalability, security, trust, and immutability?* The result is that the ENS platform provides advantages compared to TradeLens over the four analysed factors. This has important implications: the analysed factors have been identified in the literature as key challenges for the adoption of blockchain-based applications. Since the ENS platform outperforms TradeLens on a theoretical base and considering that TradeLens acceptance among trade actors is high, the ENS platform could potentially not face challenges and resistance during the adoption phase.

Table 22 - Value added of the ENS platform

Component	ENS platform	TradeLens	Value-added to
Network	Customs and carriers	Customs, all private organisations	Scalability Security Trust
Identification and authentication	eID	Tokens Cloud identity and access management Solution manager	Scalability Trust
Data structure	Events, vessel, container, port	Events, shipment, consignment, transport equipment	
Ledger structure	Multiple ledgers per carrier	Multiple ledgers per carrier	Security (when associated with the network design)
Data storage	Documents off-chain Reference on-chain Events on-chain	Documents off-chain Events on ESB	Scalability Security Trust Immutability
Access control	Role-based access control	Role-based access control	
Consensus algorithm	PoA	PBFT	Scalability

Nevertheless, a reflection on this evaluation needs to be drawn. The ENS platform has been designed to fulfil the requirements of ENS data sharing, with a high B2G focus, whereas TradeLens has various functionalities, with a high B2B focus. The different purpose of the two platforms could result in different requirements such that the criteria analysed in this chapter would need to be fulfilled to a greater extent in the ENS platform when compared to TradeLens.

This evaluation was validated on July 29th, 2020 by Maarten Sies, TradeLens Onboarding and Managing Consultant from IBM NL, who confirmed the accuracy of the above mentioned TradeLens assessment.

9. Implementation

Up to this point, this research has focused on the design of a blockchain-based platform from a technical standpoint. Nevertheless, the organisational aspects cannot be disregarded during the design of an IT artefact. This chapter will introduce organisational issues, answering *SRQ 8* – To what extent the design choices are subject to the governance structure? The goal is to assess how governance issues could impact design choices since, according to the literature, organisational aspects play a crucial role for the design and development of digital infrastructures (Rukanova et al., 2018).

Initially, section 9.1 discusses the motivation drivers in contexts where blockchain can enable business and government collaboration, by using the platforms for cross-sectorial social partnership framework (Selsky & Parker, 2005): this will be key to describe on a high-level the tensions between carriers and customs and define what their motivations and interests in the blockchain-based platform are. After that, the impact of technical choices on the organisational level, and vice versa, will be defined in section 9.2 using the governance framework by Van Engelenburg et al. (Forthcoming 2020). Section 9.3 concludes the chapter.

9.1. Cross-sector social partnership

The implementation of the ENS platform is expected to foster a business-government collaboration which entails the development of a cross-sectoral social partnership (CSSP), "defined as cross-sector projects formed explicitly to address social issues and causes that actively engage the partners on an ongoing basis" (Selsky & Parker, 2005, p. 850). The case analysed in this research presents a situation where the collaboration is developed between European customs and carriers, with the primary goal to improve the risk assessment procedures through better availability of data. The social issue at stake is guaranteeing safety and security of imported goods, as well as avoid fraudulent transport of illegal goods. Nevertheless, as argued by Selsky & Parker (2010), motivation, goals and approaches are likely to differ between actors from different sectors. In order to understand these dynamics, the Platform for CSSP framework will be used (Selsky & Parker, 2005). The framework is divided into two different dimensions: the key factors, and the platforms (Table 23 - Dimensions and factors of CSSP, retrieved from (Selsky & Parker, 2010).

According to Selsky & Parker (2005), three main platforms have been identified in the literature:

1. Resource-dependent platform: the social partnership is structured in an instrumental way, where actors join forces to address organisational needs, with social needs as a secondary goal;
2. Social-issue platform: compared to the resource-dependent platform, where stakeholder's primary addresses their needs, in the social issue platform the social need is central to the endeavour;
3. Societal-sector platform: this platform is based on the idea that an organisation from a sector is not able to solve specific issues, so it borrows solutions or functionalities from another sector. This is referred to as intersectoral blurring. An example is government sub-contracting private firms to perform social welfare functions (Selsky & Parker, 2005).

Table 23 - Dimensions and factors of CSSP, retrieved from (Selsky & Parker, 2010)

Dimension	Platform		
	Resource-dependence	Social-issue	Societal-sector
Primary interest	Voluntary, based largely on self-interest with secondary interest in the social issue	Mandated or designed around a social problem	Mixed self- and social interest
Contextual factors	Pressure for mission related performance	Pressure for CSR	Pressure for adaptation to complexity, turbulence
Source of CSSP problem definition	Each organization brings its definition to the partnership	Externally defined by existing interest groups & public issues	Envisioned or emergent public issues; constructed over time
Orientation	Transactional – each partner solves its problem with added benefit of addressing a social issue	Integrative – address the social issue with the added benefit of organizational "goods"	Integrative – explore and learn about the issue area; a social investment
Dependencies	Retain autonomy	Manage/segment interdependencies; "layer cake"* (stacked on top of one another)	Integrate interdependencies; "marble cake"* (blended at margins but distinct at core)
Time frame	Finite, delimited to meet organizational needs	Finite or indefinite depending on the social need/issue	Long term and open ended to enhance learning
Conceptualization of sectors	Organizations operate in fixed sectors; clear functions & boundaries	Business sector contributes to addressing concerns re public- & semi-public goods of other sectors; substitution logic	Organizations are not distinct sectorally; shifting functions & boundaries; partnership logic
Prospective sensemaking themes	The past; the needs of the entities/partners	The present; the social issue/cause	The future; new sectoral roles and social innovation

Among the three platforms, the one which better represents this case is the resource-dependent platform, since the social issue (improving safety and security) is a secondary goal to carriers. Each key factor, which represents the tensions between actors, will be analysed below.

Primary interest

This factor analyses the primary goal and focus of each party. Carriers` main goal is to improve the efficiency of their business processes and avoid delays due to unnecessary inspections; customs on the other hands, being governmental organisations, focus more on the social problem, which could be solved with improved risk assessment and facilitation of legitimate trade.

Contextual factors

This factor analyses what are the external conditions which could foster or inhibit the development of a CSSP. The ICS2 deployment by 2024 requires a change in practices since actors will share data using a common repository so that customs will always have access to the right set of information to perform risk assessment (DG TAXUD, 2017c). Additionally, the agreements for trade facilitation aims at decreasing the number of inspections in order to improve the world trade volumes (Widdowson, 2007). Furthermore, the EU is addressing safety and security of trade to reduce fraud cases and decrease the import of dangerous goods, which requires new procedures and improved risk analysis (European Commission, 2018; The European Court of Auditors, 2019).

Sources of CSSP problem definition

This factor describes what spurred the initiation of the CSSP. Customs authorities recognise that low data availability represents a problem and requesting additional data from private firms could solve the issue. Carriers instead are interested in lower inspections and faster clearance times which can improve time and cost-efficiency.

Orientation

This factor describes towards which area the actors are aimed. Carriers main goal is business-related, but they are aware and are keen to cooperate in order to address the social issue. Customs authorities, on the other hand, being a governmental organisation, are mainly focused on the social issue.

Dependencies

This factor describes what are the interdependencies between the organisations during the CSSP, defining the level of autonomy of each party. The involved organisations cooperate to improve data availability but remain autonomous.

Timeframes

This factor describes the timeframe of the CSSP. The collaboration is expected to take place during a long-time horizon, considering that the implementation of a blockchain-based platform requires commitment as well as high upfront investments, which take an extended timeframe to pay off.

Conceptualisation of sectors

This factor describes the boundaries between the involved sector. Each organisation operates in a sector with clear-cut boundaries: on the one hand, customs are governmental organisations; on the other hand, carriers are private firms. Nevertheless, transformation is expected in the foreseeable future: carriers will be more focused on logistics facilitation, while customs will have more responsibilities in trade facilitation (Widdowson, 2007).

The business-government collaboration in the case analysed represents a complicated process since the resource-dependent platform is mainly driven by self-interests, with the added value of addressing the social issue. While authorities will undoubtedly benefit from additional information, carriers main concern is the provision of additional data without a clear benefit for their operations, while fearing risks of confidentiality breaches. In particular, even though carriers are obliged to share ENS, providing accurate information on their itinerary and actual logistics events is not foreseen in the current regulatory framework (European Union, 2013). Carriers might fear that this additional information is not securely stored and could result in competitors gaining access to sensitive data. While from a technical

standpoint, the blockchain-based platform is expected to provide security of stored data, the organisational network plays a vital role. Susha et al. (2019) suggested that the government plays an active role in aligning all other authorities and businesses in achieving a win-win scenario.

This section presented on a high-level the tensions between private firms (carriers) and public authorities (customs). These tensions can be summarised with the conflict between the economic benefit goal of carriers, and the public value goal of customs. Carriers fear that the provision of additional data on their itinerary could lead to confidentiality issues and competitors gaining an advantage. Considering that the CSSP is based on the voluntary provision of additional data by carriers, a combination of economic benefit and public value needs to be obtained to motivate carriers to cooperate. The next section will analyse the impact of these tensions on the design choices.

9.2. Blockchain governance

The previous section showed how the case at hand represents a complex socio-technical system, with conflicting interests at stake, driven by a technological imperative. How to align the interests of different stakeholders concerning the design of a blockchain-based platform represents a key challenge. This is related to blockchain governance, which is a "process of social organisation and coordination that relate to blockchain-based B&G information sharing" (Van Engelenburg et al., Forthcoming 2020, p. 3). The framework (Figure 22) proposed by Van Engelenburg et al. (Forthcoming 2020) allows to analyse the relationships between stakeholders, governance requirements and blockchain design choices in two ways: 1) stakeholder view, which firstly analyses stakeholder relationships to come to an agreement on the governance requirements and then identify compliant design choices; 2) blockchain control view, to determine the impact of design choices on the governance requirements and stakeholders relationships (Van Engelenburg et al., Forthcoming 2020). This section will start with the blockchain control view.

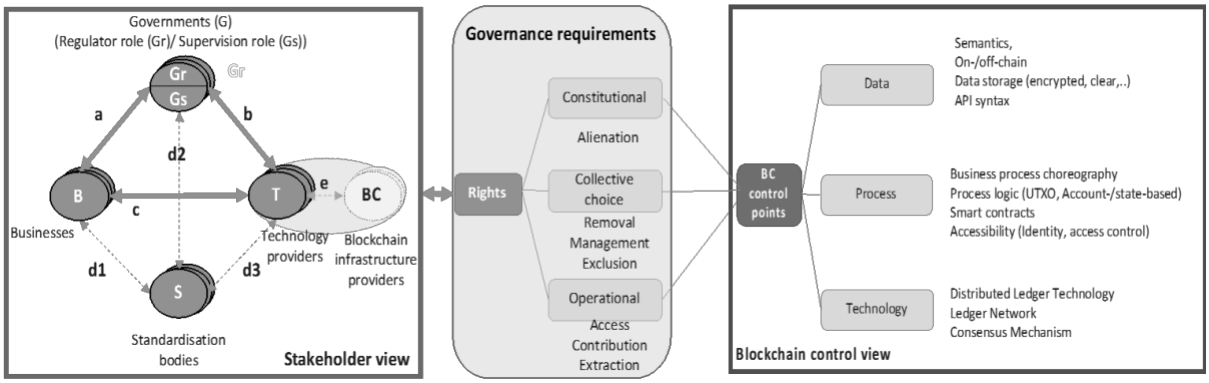

Figure 22 - Blockchain Governance framework, retrieved from (Van Engelenburg et al., Forthcoming 2020)

9.2.1. Blockchain control view

Several blockchain control points have been identified as having a direct impact on governance requirements. Each control point will be analysed, to derive what are the rights influenced by each design choice.

Network

The network design choices define which parties will be able to join the network, which will affect the access rights (Van Engelenburg et al., Forthcoming 2020). Carriers and customs will become a node in the peer-to-peer network, thus will have rights to access the blockchain-based platform (access rights). Considering that the network is heterogeneous, contribution and extraction rights will be determined by different components, namely consensus mechanism and data sharing model (Van Engelenburg et al., Forthcoming 2020).

Consensus mechanisms

The consensus mechanism defines which nodes can propose and validate transactions, affecting contribution rights (Van Engelenburg et al., Forthcoming 2020). The ENS platform makes use of PoA consensus algorithm, where carriers can propose new transactions to store the ENS reference on-chain, and customs validate the ENS. Carriers and customs will then have contribution rights.

Data sharing model

The data-sharing model defines how and where data are stored, which parties can or cannot have access to those data, and how data are shared. In the ENS platform, customs which have the role of COFE or COU will have extraction rights over the document and the additional database (Van Engelenburg et al., Forthcoming 2020). Carriers, on the other hand, do not have extraction rights, since it could otherwise lead to confidentiality issues.

Table 24 - Operational rights, adapted from (Van Engelenburg et al., Forthcoming 2020)

Rights		Rights in a blockchain-based system for B&G information sharing	Actors
Operational rights	Access	Rights to access part of the blockchain-based system	Customs, carriers
	Contribution	Right to store, revise or delete data shared using blockchain	Carrier, customs
	Extraction	Right to obtain access to data shared using blockchain	Customs (COFE and COU)

9.2.2. Stakeholder view

The previous section described how the design choices impact the operational rights. In order to define constitutional rights and collective choice rights, the stakeholder view needs to be analysed. Considering that carriers and customs represent the two main categories of actors affected by the blockchain-based platform, two different scenarios can be identified: a first scenario, where carriers, and possibly other private firms, will be in charge of the governance of the platform (private domain governance); a second scenario, where instead the governance is in the hands of customs, and possibly other public authorities (public domain governance).

Scenario 1 – private domain governance

In the first scenario, the platform would be developed and governed by private firms. The main implication is that the functionalities are agreed upon by carriers and other private firms, while customs will only be authorised to use these functionalities. In scenario 1, private firms would be in charge of the governance of the blockchain, which entails being at the forefront of the design of the platform and be accountable for it (Ølnes et al., 2017). The private firms are businesses, such as carriers or freight forwarders, with decision power on

what are the functionalities and can impose their own choices. Government is represented by customs, which are only users and are not involved in the development and maintenance of the platform. The stakeholder view also includes technology providers and standardisation bodies, but these are left outside the scope of this analysis since the goal is not to get into the details of the governance structure, but only to point out the role of private firms and public authorities.

Table 25 - Constitutional and collective choice rights scenario 1 adapted from (Van Engelenburg et al., Forthcoming 2020)

Rights		Rights in a blockchain-based system for B&G information sharing	Actors
Constitutional rights	Alienation	Right to determine who has what collective rights	Carriers
Collective choice rights	Removal	Right to remove parts of the blockchain-based system	Carriers
	Management	Right to determine how, when, and where parts of the blockchain-based system can be used and choices on control points may be changed	Carriers
	Exclusion	Right to determine who has what operational and removal rights and how these can be transferred	Carriers

Scenario 2 - public domain governance

In the second scenario, the governance of the platform will be in the hands of public authorities, among which customs authorities will play a key role in determining the functionalities of the platform. In this case, other public and governmental authorities, such as the EU, could be involved. Businesses will, in this case, be represented by carriers, which only have the role of users. Similar to the previous scenario, technology providers and standardisation bodies will not be considered.

Table 26 Constitutional and collective choice rights scenario 2 adapted from (Van Engelenburg et al., Forthcoming 2020)

Rights		Rights in a blockchain-based system for B&G information sharing	Actors
Constitutional rights	Alienation	Right to determine who has what collective rights	Customs
Collective choice rights	Removal	Right to remove parts of the blockchain-based system	Customs
	Management	Right to determine how, when, and where parts of the blockchain-based system can be used and choices on control points may be changed	Customs
	Exclusion	Right to determine who has what operational and removal rights and how these can be transferred	Customs

Conclusions

The application of the governance framework provides compelling results in terms of what are the interrelationships between technical choices and governance structure. Starting from the blockchain control view, the ENS platform influences operational rights. The access rights are determined by the network topology, which allows customs and carriers to access parts of the blockchain-based system: carriers access will be limited only to their blockchain ledger, while customs have access to all the ledger. The consensus mechanism determines the contribution rights: the implemented PoA consensus algorithm permits both carriers and customs to join the consensus process. The data-sharing model instead determines the extraction rights: customs having the role of COFE or COU can decrypt the ENS document, thus accessing the ENS data, while other customs cannot. The interesting result from the blockchain control view is that the operational rights are not affected by the governance structure. The effect of the organisational network is measured on the constitutional and collective choice rights level. In scenario 1, private domain governance, carriers, and other private firms will have decision-making power. This entails that both constitutional and collective choice rights are in the hands of the governing consortium. The same can be said for the second scenario.

9.3. Conclusions

This chapter addressed the implementation of the ENS platform and addresses *SRQ 8* – To what extent the design choices are subject to the governance structure? The application of the platforms for cross-sectorial social partnership framework provides an overview of the tensions between carriers and customs: the former focuses more on the economic benefits derived from the usage of such platform, while the latter prioritises the social issue at stake, which is the improvement of safety and security of goods imported into the EU territory and provide public value. These tensions have implications for the governance of the platform. Using the blockchain governance framework, the main result is that the governance structure influences only constitutional and collective choice rights. The operational rights, on the other hand, are independent from the governance but are only related to technical choices. This finding could be further elaborated: the design choices in this research have been built upon the business process to be supported and design requirements which are unlikely to differ depending on the governance structure. Since the business process stays unchanged the same whether there is a private or public domain governance (since the process is based on current regulatory frameworks which are indipendent governance structure), the resulting design choices, and thus the operational rights will stay unchanged with different governance structure.

10. Conclusions

This chapter concludes this research report. In section 10.1, each sub-research question will be answered. The main research question will be answered in section 10.2, and section 10.3 will describe the key findings. Section 10.4 analyses the scientific contribution, while societal relevance will be defined in section 10.5. Section 10.6 introduces final reflections.

10.1. Answering sub-research questions

In this section, each SRQ will be analysed, to provide an overview of the steps performed to answer the MRQ.

Sub-research question 1 - *Which research strategy allows to design a blockchain-based platform to support ENS availability among customs authorities?* addressed the research strategy to be used in order to undertake this study. Considering that the aim of this research was mainly design-oriented, traditional research methods did not fit with the purpose: indeed, traditional methodologies try to understand reality, while the scope of the research is to create artefacts. For this purpose, the DSRM represented a valuable framework. The goal is to create artefacts following six consecutive steps: "problem identification and motivation, define objectives for a solution, design and development, evaluation and communication (Peffers et al., 2007, pp. 56–58)". An additional step which discussed the implementation issues and governance has been added, in order also to address the secondary goal of this research to define what are the governance implications of the ENS platform.

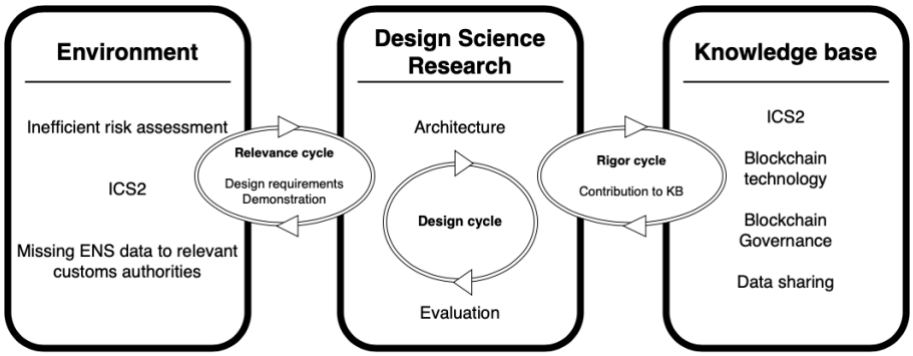

Figure 23 – DSRM cycles, adapted from Hevner (2007)

Sub-research question 2 - *How would the interactions/information flow among trade actors during the submission of ENS look like when implemented on a blockchain-based platform?* represents the first step of DSRM, problem identification and motivation addressed in chapter 3. This phase started with an analysis of the AS-IS situation, describing firstly the actors involved with the shipment of goods and how they interact to exchange ENS data. The main result is that carriers and customs are the involved actors in the information process for ENS data. Subsequently, the new import control system has been presented: the European Commission ICS2 Directive, to be implemented in the EU Member States by 2024, will bring changes in practices and in how actors interact. In particular, the ICS2 foresees the deployment of a common repository to store ENS data and other notifications/documents related to pre-arrival risk assessment and arrival of vessels in European ports. Starting from this, a scenario where interactions take place using a blockchain-based architecture has been described: the goal was to define a possible TO-BE situation, providing a representation of the application level of such an architecture.

Sub-research question 3 - *What are the design requirements to support data sharing in the context of European customs?* addressed the second phase of the DSRM, define objectives for a solution, addressed in chapter 4. The objectives, in this case, took the form of design requirements that the architecture had to fulfil. The requirements elicitation took place in two different ways: on the one hand, functional requirements, have been defined using the TO-BE description; on the other hand, the non-functional requirements, have been defined using the literature on the data pipeline concept, with the assumption that data sharing implications are similar. This resulted in several requirements, summarised in Table 27, which represent the protocol level.

Table 27 - Requirements

Code	Description
Req. 1	*A customs authority should always have access to the proper ENS data. The COFE will access ENS data of all containers, whereas other customs offices will only access ENS data on products unloaded in their ports.*
Req. 2	*The architecture should give customs real-time information on changes on the itineraries, and carriers should be the source of this information.*
Req. 3	*Each user should be registered as one digital identity (identification)*
Req. 4	*Each digital identity must be associated with only one user (authentication)*
Req. 5	*Data should be stored in a safe place*
Req. 6	*Carriers should only access information related to their shipment (access control)*
Req. 7	*Customs should only access information on vessels passing through their jurisdiction (access control)*
Req. 8	*Control mechanisms should be in place to ensure the integrity of exchanged information so that data are not tampered when shared (integrity)*
Req. 9	*The data structure should be consistent*
Req. 10	*The architecture should handle a high rate of transactions.*
Req. 11	*The architecture should accommodate an increasing number of parties joining the platform.*

Sub-research question 4 - *What are the core blockchain components and design choices to be considered during the design phase?* addresses the first part of the third phase of the DSRM, design and development, described in chapter 5. This part described what the core blockchain components and design options available are. Through a literature review on blockchain taxonomy, four key components have been identified: network topology, data storage, consensus mechanisms and application. These components have then been further divided into subcomponents, defining what the pros and cons of each design option are. Table 22 summarises the components, which address the middle layer of the information architecture.

Table 28 - Blockchain components and design options

Component	Design choices	Sub choices	
Network topology	Permissionless		
	Permissioned	Identity Management	
		Permission Management	
Data storage	On-chain	Transaction model	UTXO
			Account-based
		Ledger structure	Single
			Multiple
	Off-chain	On-chain reference Hash	
Consensus mechanisms	PBFT		
	PoA		
Application	Smart Contract		
	Transaction		

Sub-research question 5 – *How does the architecture of the blockchain-based platform that supports ENS data exchange look?* addresses the second step of the third phase of the DSRM, design and development, described in chapter 6. The findings from the previous three sub-research questions have been used as input in this phase: considering the TO-BE situation and the elicited requirements, the goal was to make design choices using the sub-components defined in chapter 5, weighing pros and cons of each decision.

Table 29 - Architecture design choices

Component	Design choice	Requirements addressed
Network configuration	Permissioned Consortium blockchain	Req.10 (Scalability)
Identity Management	Carriers and Customs authority are identified and authenticated through a PU certificate (key pair)	Req.3 (Identification) Req.4 (authentication)
Permission to join the network	All carriers and customs identified through their PU certificate	Req.1 (Customs access to ENS data) Req.2 (Updates on itineraries)
Data structure	Port, vessel, container, event	Req.9 (Availability)
Data storage	Transactions stored on-chain Multiple ledger structure per carrier Documents stored off-chain Reference of the document stored on-chain Account-based model	Req.5 (Concealment) Req.6 (Access Control) Req.7 (Access Control) Req.8 (Integrity) Req. 10 (Scalabilty)
Data security	Symmetric cryptography (ENS document) Asymmetric cryptography (messages and events) RB-XACML	Req.5 (Concealment) Req.6 (Access Control) Req.7 (Access Control)
Smart contract	Smart itinerary contract	Req.2 (Updates on itineraries)
Consensus algorithm	PoA	Req. 10 (scalability)

Sub-research question 6 - *How can the blockchain-based platform be used to share ENS data?* addresses the demonstration phase of the DSRM, described in chapter 7. A walkthrough methodology was used to address this phase: the functionalities are described in detail, to show how different actors can use the platform to exchange ENS data.

Sub-research question *SRQ 7 - How does the designed platform rate compared to an existing platform in the shipping industry in terms of scalability, security, trust, and immutability?* addressed the evaluation phase of the DSRM, described in chapter 8. In this phase, the

designed ENS platform was compared with TradeLens, and resulted in the ENS platform theoretically outperforming TradeLens on the analysed criteria. This feasibility evaluation was useful to analyse how the ENS platform would perform in a real-world setting. Nevertheless, this evaluation method is limited by the fact that TradeLens has a different orientation as it is focused on B2B interactions. In contrast, the ENS platform is focused on the ENS sharing functionalities, with the advantages of a more limited set of actors and interactions that need to be taken in to account.

Sub-research question 8 – To what extent are the design choices subject to the governance structure? addressed the second step of the evaluation, which is the implementation evaluation. This phase introduced the organisational perspective and network tensions which could affect the development of the blockchain-based platform for ENS data sharing. In a first step, the tensions between carriers and customs have been analysed using Cross-sectorial social partnership framework: the result is that the tensions can be summarised as a conflict between economic benefits prioritised by carriers, and public values prioritised by customs authorities. A combination of both objectives would motivate carriers to provide additional data and achieve the goal of the CSSP. Subsequently, using the Governance framework by Van Engelenburg et al. (Forthcoming 2020), the impact of the governance structure on design choices was assessed. The result is that the design choices, in this case, are not directly affected by the governance structure, but they are affected by the business process to be supported. By since the business process is not dependent on the governance structure, but depends on current regulations and operational methods, the governance structure does not have an impact on technical choices.

10.2. Answering Main research question

In light of the answers provided to the sub-research questions, the main research question "Which design of a blockchain-based platform can be developed to support the availability of Entry Summary Declarations to customs authorities for incoming cargo flows into the EU?"

A blockchain-based platform which supports the availability of ENS data to customs authorities is based on a permissioned peer-to-peer network, in which carriers and European customs authorities join as a node. The identification of users (organizations) is based on eIDs,

which are provided at the national level. The data-sharing model is based on a vessel-container-port data structure, driven by events. The events are real-world occurrences, submitted by carriers, which update the state of a smart itinerary contract to represent the itinerary of the vessel. ENS data are stored in an off-chain repository and encrypted with a symmetric key. The key is stored in an on-chain key storage, while a reference of the ENS is shared on-chain, together with a hash for record integrity and a URI to access the document. Through role-based access control, the blockchain assesses whether the requesting party has a relevant role in the itinerary and sends the corresponding symmetric keys. Transactions are validated using a PoA consensus algorithm. The platform uses a multiple ledger structure per carrier.

10.3. Key findings

Based on the answer to the SRQs and the MRQ, this section will identify the key findings. These will be further reflected in section 10.4 and 10.5.

The first main finding of this research is the design of the blockchain-based platform which supports the availability of ENS to European customs. This has several implications. Starting from the TO-BE process, an interesting use of itinerary data is proposed: carrier share information on their planned, estimated and actual itinerary, in order to trigger a dynamic access control mechanism, such that customs authorities are authorised to access ENS data. Itinerary data are overlooked by current regulatory frameworks and import control systems but could play a key role in reducing cross-border lead time and can provide benefits to other trade actors, as discussed next. Linked to this, is the use of smart contract to implement the business logic and keep track of the state of the itinerary.

The design process of the platform is insightful: designing a blockchain-based platform initially requires the definition of the process to be supported and design requirements. Based on these requirements and the TO-BE process, the design is carried out by defining network topology, data sharing model, consensus mechanism, application level and how these different components interact.

An important finding is how the platform can be used to access ENS data and it is based on three steps, the first one being the submission of ENS data: a carrier encrypts the ENS

document, stores it in an external database (such as carrier's own ERP or a common repository), and publishes a reference to the documents on-chain, as well as the decryption key in an on-chain key storage. Secondly, the carrier drafts the itinerary: the carrier issues planned events, which makes associations between digital twins of containers, vessels and ports. The final step is the retrieve of ENS data by customs authorities: a customs authority sends a request message to the RB-XACML structure where its role is determined, and it will be provided the decryption key accordingly. The customs can retrieve the encrypted ENS documents using the on-chain reference, can decrypt it using the decryption key received from the RB-XACML, and accesses the data.

The evaluation of the platform presents interesting results. To assess the feasibility of the ENS platform in a real-world setting, an evaluation has been carried out through a comparison with TradeLens, which is an existing blockchain-based platform which supports shipping processes. The conclusion is that the ENS platform theoretically outperforms TradeLens in terms of scalability, security, trust and immutability, factors which in the literature were identified as hindering the deployment of BCT.

The last finding is concerned with organisational aspects: the tensions between carriers and customs can be summarised by the often-conflicting economic and public values goals. The literature suggests that organisational and governance aspects influence the development of blockchain-based platforms. This research argues that the governance structure has no direct impact on the design, as the business process and design requirements define the directions for technical choices.

10.4. Scientific Contribution

The main output of this research is the contribution to the implementation of the ICS2 directive "Transition Strategy and Plan for Import Control System" (DG TAXUD, 2017c): the goal of the import control system 2.0 is to address both data quality and data availability. This research focused on the latter by proposing a blockchain-based platform for the exchange of ENS data. The inputs for the ICS2 are: 1) the use of blockchain to support the storage and exchange of information; 2) the use of a blockchain-based platform in addition to the common repository, 3) the use of itinerary data to provide dynamic access to relevant

customs authorities. The use of blockchain technology can provide several advantages when compared to the proposed common repository, the first one being the dynamic access control: in fact, while the ENS platform has an embedded dynamic access control based on the itinerary of the vessel, so that customs authorities can only access relevant data, the common repository is freely accessible by any customs authority. This could raise confidentiality issues, since a customs authority should only access relevant information (thus, on vessels passing through their jurisdiction). A second advantage is the immutability: while BCT features allow to obtain immutability, the immutability of the common repository is based on the governance. Immutability by governance means that the there is an authority, in this case the EC, which is directly responsible for the database. Considering that the EC is a governmental organization, it will ensure that each information stored on the common repository is not deleted. This could lead to organizational challenges, since such an implementation would require initially a strong alignment between stakeholders as well as a regulatory framework which supports this. The ENS platform instead has an embedded technological immutability, which is not dependent on the governance structure, thus could be easier to implement. A final consideration could be made on the data shared: while in both cases the focus is on ENS data, the difference relies in additional data shared. The ICS2 implementations requires Arrival and Presentation notification to notify a customs office about the arrival of a vessel. The ENS platform instead relies on real-time updates of the itinerary. One could argue that the latter is potentially more beneficial than the former, since broader set of actors could benefit from this additional information. This will be further explained in section 10.6.

Additionally, this study contributes to research on BCT (Beck et al., 2017) by providing an empirical example of how a platform can be designed making use of blockchain components, and how these are tuned. While literature on blockchain extensively addresses each component individually, the design choices and trade-offs, there are no guidelines on how a platform based on blockchain can be developed and different components interact. This research could be the starting point for developing of a blockchain design framework. The design should start from the TO-BE process description: this allows to visualise how actors interact and how information is exchanged using a blockchain-based platform. From here, design requirements should be elicited: these are divided into functional requirements, which

are mainly derived from the process description, and non-functional requirements, which are instead focused on issues such as security and scalability. The final step is making design choices based on blockchain components: as seen in this case, blockchain-based platform's key components are the network topology, the data storage, the consensus mechanism and the application level. Each of these components has several sub-components which represent design choices. Based on the process to be supported, and the requirements elicited, trade-offs between design choices will be made to define how different components are structured. This will provide the design of the blockchain-based platform.

This study also contributes to the research on governance, in particular governance of blockchain-based systems. In the literature, governance concerns are raised, since it is unclear what is the impact of a decentralised platform on the organizations involved, and vice versa. The conclusion, based on the case analysed, is that the governance structure does not influence technical choices. On the contrary, design choices are mostly determined by the business process to be supported by the blockchain-based platform and design requirements. If the process is not expected to vary with different governance structures, then there are no strong links between technical choices and governance structure, as put forward by the Blockchain governance framework by Van Engelenburg et al. (Forthcoming 2020). Research on blockchain governance should switch the focus from the design phase to the implementation phase: in fact, while governance does no impact the design of the platform, it will surely impact how the decentralised network is structured and will possibly affect existing regulatory frameworks.

The last contribution of this study is on the eGovernment research, with a focus on data sharing between businesses and governments (Susha et al., 2019). By using the platform for Cross sectorial social partnership framework, the main finding is that there are tensions between customs and carriers, that can be summarised by the contrast between public values and economic benefits. Government plays a crucial role in finding a combination of these two goals, in order to motivate carriers to share additional data with customs voluntarily, which in this case is represented by itinerary data. Considering that itinerary updates are essential for functioning of the platform, conciliation of economic benefits and public values has to be achieved.

10.5. Societal Relevance

Global trade is one of the pillars of nowadays socio-economic outlook: successful companies often reach out to markets in different countries and different continents, in order to increase their share. Consumers on the other hand, benefit from a wide range of products at competitive prices. This is made possible by global supply chains, which interconnect companies and countries from all over the world.

The European Union, as the major trade player worldwide, plays a key role in determining future trends of global trade. At the same time, the EU needs to protects its border from possible trade-related threats: often counterfeit products and illegit goods enter the European market, or traders try to avoid heavy tux burdens by incorrectly declaring value or quantity. For this reason, the EU enforces customs authorities to perform risk assessment. The goal is twofold: facilitate as much as possible cross-border activities, while stopping dangerous of fraudulent goods. Risk assessment plays a critical role in global trade, and the facilitation of crossing borders could potentially foster an increase in worldwide trade volumes (The Economist, 2018). Trade facilitation could be increased with a better risk assessment, such that customs authorities can better identify threats and inspect a lower number of incoming cargos.

Good risk assessment is based on two pillars: good data quality and good data availability. This research aims at one of the two pillars of proper risk assessment: data availability. The designed ENS platform targets the availability of entry declaration, one the main documents used for customs clearance, with the goal to make ENS data available to the relevant customs authorities. With the right data available to the right customs authority, the risk analysis can be better performed (DG TAXUD, 2017c). Once a customs authority has the necessary data, it can perform risk assessment and better identify possible threats. This could result in fewer inspections, which will then decrease cross-border lead time, with advantages for the shipping industry as a whole (Thomas & Tan, 2015). On the other hand, improved risk assessment could result in higher detection of dangerous or fraudulent goods imported in the EU territory. With higher security and safety standards, dangerous goods can be stopped before their loading or arrival. Furthermore, this can lower tax fraud cases, with benefits for

the European economy (The European Court of Auditors, 2019). The impact is extended to all global industries and consumers, which will benefit thanks to higher trade volume.

This research is also part of PROFILE, a European-wide project which aims at improving customs risk assessment employing new technologies and new techniques. This study focused on the application of BCT as backbone for secure and safe data sharing in the context of European Union. This also has implication for other studies, such as the use of data analytics to improve risk analysis: for instance, with more data available to customs, better analysis can be performed.

Besides the impact on risk assessment and the consequent benefits for global trade and the EU socio-economic outlook, this research can contribute to the development and spreading of BCT. Researchers and practitioners claim that this technology could bring several advantages, but there are not many real-world cases and there is still some aversion and unfamiliarity (DHL Trend Research, 2018). The application of BCT in a such large-scale and impactful area could change the perception of this technology: in fact, there are some chances that, if a governmental body such as the EU implements BCT to manage trade-related administrative paperwork, companies from other industries, could be more keen to adopt this technology. BCT would potentially provide even more benefit with widespread diffusion in today's society, with application from healthcare, to administrative paperwork in global supply chains.

10.6. Reflections

This section will reflect on the research conducted, by firstly describing the limitations, and then defining the basis for further research

Research method

The main drawback of the research approach chosen in this study is that an empirical evaluation and real-world implementation are missing. The platform has been designed relying on the literature on BCT and data sharing, so the functionalities are grounded on a theoretical basis. Nevertheless, when it comes to designing artefacts, the reality usually diverges from the theory, since during the implementation, additional issues can pop out,

requiring changes in the design. To partially address this limitation, an additional step in the evaluation phase, which addressed the implementation was described: this highlighted how the technical choices are not dependent on the governance structure. Moreover, the demonstration was performed with a walkthrough which has several shortcomings: in particular, it might be difficult for an inexperienced reader to grasp the content.

To address these limitations, the recommendation is to develop a proof-of-concept, which allows to analyse quantitatively how the designed blockchain-based platform performs in a real-world setting. In a first instance, this could take the form of a small-scale demo with limited volumetric and small set of actors, where the exchange of ENS data and upload/updates of itineraries through events are tested. Subsequently, this demo can be further developed to handle higher volumes, including an increasing number of actors. Each stage can be used to adjust the components, and, in case of positive outcomes, the platform can be fully deployed in large-scale. To solve the demonstration hurdles, the suggestion is also to develop a graphic user interface (GUI), to more simply showcase the functionalities.

Additionally, future research should empirically analyse how and to what extent blockchain-based platforms provide advantages over existing systems: for instance, a sensitivity analysis can be performed to define which percentage of availability is needed to improve risk assessment procedures, whether this percentage can be achieved using a blockchain-based platform and how. This is needed to ensure that investments in new system, in both monetary terms and effort to reach agreement between stakeholders, are outweighed by the advantages.

Assumptions

Throughout this research, several assumptions have been made. These assumptions allowed to facilitate the description of processes or to simplify some design choices.

Among the assumptions made in section 3.5, the first one assumes that only carriers submit ENS data, even though a third party, like a freight forwarder, can submit it on the carrier's behalf in the real-world setting. This would introduce a level of complexity since permission mechanisms would need to be adjusted such that a third party can submit the ENS data and support multiple filing, where multiple datasets are used to create the final ENS data. A

follow-up statement assumed that carriers only submit the ENS data to the COFE, but in reality, carriers can submit it also to different customs offices. This assumption does not represent a limitation since, with the ENS platform, carriers do not submit ENS data directly to customs offices, but they lodge it on the platform through a reference. The assumption that ENS data are not amended in reality represents an issue since incorrect data undermine the reliability of risk assessment. The focus of this thesis was not in data quality but on data availability. Nevertheless, functionalities to check the correctness of submitted data should be included.

To overcome the above-mentioned limitations, a platform with a larger network base should be designed. By including additional actors in the network, data correctness checks could be performed by other parties, to solve the data quality limitation. For instance, by including consignor and consignee in the network, a validation of the accuracy of submitted ENS data can be carried out before the document is stored. During the consensus process, carriers would send the block proposal to consignor and consignee, who can validate the ENS data. A freight forwarder could contribute to the submission of ENS, in order to implement multiple filing of ENS data, overcoming the first assumption. Additionally, these actors, could both contribute to and benefit from real-time updates of the itinerary: for instance, more accurate information on arrival of goods can facilitate logistics planning as well as increase customer satisfaction. The addition of new actors would require changes in some design components and functionalities, such as network configuration and consensus mechanism, which requires further research. This also highlights how additional data on the itinerary could serve multiple purposes, from providing dynamic access to sensitive data, to provide valuable information to trade actors. Further research should thus analyse how itinerary data can be used a reused by trade actors: potentially, the Arrival and Presentation notifications foreseen by the ICS2 implementation could be substituted by real-time itinerary data, which could prove to be more informative and could serve more purposes.

The assumptions that other documents are not included and that other activities are not considered does not represent a limitation, since this does not affect the submission and sharing of ENS data directly.

In chapter 4, the assumption that this research resembles the key data-sharing aspects of the data pipeline literature was introduced. This literature touches upon the key data-sharing requirements shared with other areas, such as the CIA triad. These have been complemented with the results on the analysis of the AS-IS scenario and regulations, in order to extend the applicability of the data pipeline concept to this case. As a result, this assumption does not seem to represent a limitation. Nevertheless, further research should analyse whether the application of BCT to implement ENS data sharing yields additional requirements: this would require a joint effort between customs authorities and technology provider to come up with spot-on requirements.

Concerning the implementation, a high-level description of the tensions between private firms and public authorities provided insights into organisational issues which could arise with the application of the ENS platform. Further research should analyse more deeply these tensions and how they could impact the deployment of the platform, as well as the impact on current regulatory frameworks.

Additional reflections

BCT has been showcased in this study as enabling technology to support trade-related exchange of information between private organizations and governmental authorities. This research presented some benefits that such technology could potentially bring, and some challenges that its application is expected to face. It would be interesting to analyse in future researche the combination of BCT with other emerging technologies, to improve even more the processes and interactions. For instance, this research is based on the idea that additional data on the vessel itinerary can significantly improve the availability of ENS data to customs authorities. Carriers would be the source of this data using the ENS platform, but by integrating tracking data using IoT (internet of things) technology, the itinerary would be updated automatically without the need for carriers to insert these data manually.

To conclude, this research was conducted as a master thesis project for the Management of Technology (MoT) master's programme. The use of technology as an organisational resource is central in the MoT programme, where innovation is seen as a key driver to develop/design products and maximise customer satisfaction, profitability and efficiency. This project

resembles the key characteristics of the MoT curriculum: scientific topic with technological underpinning which through the use of scientific method demonstrates the use of technology as an organisational resource. On the other hand, several courses of the MoT programme were instrumental to learn the key aspects of academic research: writing papers was essential to understand the academic writing style; studying research methods was pivotal to learn how scientific research is carried out and how a research report is structured; the socio-technical foundation of each module was key to understand the dynamics between technology and organizational aspects.

Albeit being linked with the MoT programme, this research also deviates from a standard MoT thesis: design-oriented research is not common in the MoT curriculum, where instead explorative, empirical, qualitative or case study research are mostly carried out. This required a more thorough study of the literature, technology and design techniques. Nevertheless, this report shows how, despite having no experience with design-oriented research, an MoT student can be flexible enough to carry out a successful research in this field.

Bibliography

Allison. (2016). *Shipping giant Maersk tests blockchain powered bills of lading - Accessed 2020-02-21*. International Business Times. https://www.ibtimes.co.uk/shipping-giant-maersk-tests-blockchain-powered-bills-lading-1585929

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. *Business and Information Systems Engineering*, *59*(6), 381–384. https://doi.org/10.1007/s12599-017-0505-1

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10), 1020–1034. https://doi.org/10.17705/1jais.00518

Behnke, K., & Janssen, M. F. W. H. A. (2019). Boundary conditions for traceability in food supply chains using blockchain technology. *International Journal of Information Management*, *March*, 101969. https://doi.org/10.1016/j.ijinfomgt.2019.05.025

Bharosa, N., Janssen, M., van Wijk, R., de Winne, N., van der Voort, H., Hulstijn, J., & Tan, Y. hua. (2013). Tapping into existing information flows: The transformation to compliance by design in business-to-government information exchange. *Government Information Quarterly*, *30*(SUPPL. 1), S9–S18. https://doi.org/10.1016/j.giq.2012.08.006

Boschert, S., & Rosen, R. (2016). Digital Twin—The Simulation Aspect. In P. Hehenberger; D. Bradley (Ed.), *Mechatronic Futures* (pp. 59–74). Munich, Germany. Springer International Publishing. https://doi.org/10.1007/978-3-319-32156-1_5

Buchmann, J. A., Karatsiolis, E., Wiesmaier, A., Buchmann, J. A., Karatsiolis, E., & Wiesmaier, A. (2013). PKI in Practice. In *Introduction to Public Key Infrastructures* (pp. 143–164). Berlin, Germany. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-40657-7_10

Castro, M. (2001). Practical Byzantine Fault Tolerance. *Proceedings of the Third Symposium on Operating Systems Design OSDI '99*, *February*, 1–172. http://pmg.csail.mit.edu/papers/osdi99.pdf

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

CORE. (n.d.). *The Core Project - Accessed 2020-02-21*. Retrieved February 21, 2020, from http://www.coreproject.eu/

Crampton, J. (2005). *XACML and Role-Based Access Control DIMACS Workshop on Secure Web Services and e-Commerce*.

Czachorowski, Karen; Solesvik, Marina; Kondratenko, Y. (2019). The Application of Blockchain Technology in the Maritime Industry. *Springer Nature Switzerland*. https://doi.org/10.1007/978-3-030-00253-4

De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. *CEUR Workshop Proceedings*, *2058*.

DG TAXUD. (2016). *Customs Policy, Legislation, Tariff Customs Processes and Project Management TAXUD A3(2016)2696117 Doc. DIH 16/003 FINAL EN. Brussels: DG TAXUD, October 6th 2016*.

DG TAXUD. (2017a). *Business Case UCC new Import Control System (ICS2) Doc. Version: 3.1.1.1 for TCG. Brussels: DG TAXUD, June 27th 2017* (pp. 1–81).

DG TAXUD. (2017b). *ICS2 Shared Trader Interface - Vision. Trader Interface - Vision Ref. Ares(2017)5574377. Brussels: DG TAXUD, November 15th 2017*.

DG TAXUD. (2017c). *Transition Strategy & Plan for Import Control System (ICS2). Brussels: DG TAXUD, December 12th 2017*.

DG TAXUD. (2018a). Annual Activity Report 2018 Ref. Ares(2019)2252622 - 29/03/2019. In *Annual Activity Report INCT-APA*.

DG TAXUD. (2018b). *Import and Export Formalities GUIDANCE DOCUMENT on Customs*

Formalities on Entry and Import into the European Union - Ref. Ares(2018)6352314. Brussels: DG TAXUD, December 11th 2018.

Dhillon, V., Metcalf, D., Hooper, M., Dhillon, V., Metcalf, D., & Hooper, M. (2017). Foundations of Blockchain. In *Blockchain Enabled Applications* (pp. 15–24). Berkeley, CA. Apress. https://doi.org/10.1007/978-1-4842-3081-7_3

DHL Trend Research. (2018). Blockchain in Logistics: Perspectives on the Upcoming Impact of Blockchain Technology and use Cases for the Logistics Industry. In *DHL Customer Solutions & Innovation*.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, *30*(7), 1366–1385. https://doi.org/10.1109/TKDE.2017.2781227

Elmane-Helmane, K., & Ketners, K. (2012). INTEGRATED CUSTOMS CONTROL MANAGEMENT IN LATVIA: LESSONS LEARNED. *ECONOMICS AND MANAGEMENT*, *17*(2), 528–533. https://doi.org/10.5755/j01.em.17.2.2177

Engelenburg, S. van, Janssen, M., & Klievink, B. (2019). Design of a software architecture supporting business-to-government information sharing to improve public safety and security: Combining business rules, Events and blockchain technology. *Journal of Intelligent Information Systems*, *52*(3), 595–618. https://doi.org/10.1007/s10844-017-0478-z

European Commission. (n.d.). *Data Analytics, Data Sources, and Architecture for Upgraded European Customs Risk Management | PROFILE Project | H2020 | CORDIS | European Commission - Accessed 2020-02-21*. Retrieved February 21, 2020, from https://cordis.europa.eu/project/id/786748

European Commission. (1998). *A guide to risk analysis and customs controls. Luxemburg.*

European Commission. (2010). *Secure Trade and 100% Scanning of Containers. SEC(2010) 131 final. Brussels: European Commission, February 11th 2010* (Issue February). SEC(2010) 131 final.

European Commission. (2013). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE on Customs Risk Management and Security of the Supply Chain - COM(2012) 793 final. Brussels. January 8th 2013*.

European Commission. (2018). *Report from the Commission to the European Parliament and the Council - 30th Annual Report on the Protection of the European Union's financial interests Fight against fraud 2018. Luxemburg.* ISSN 2599-9478.

European Union. (2013). *REGULATION (EU) No 952/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 October 2013 laying down the Union Customs Code. OJ L269/4, October 10th 2013.* https://audiovisual.ec.europa.eu/en/video/I-120321

FEDeRATED. (2020). *Interim masterplan* (Issue March).

Francisco, K., & Swanson, D. (2018). The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. In *Logistics* (Vol. 2, Issue 1, p. 2). https://doi.org/10.3390/logistics2010002

Gil-Garcia, J. R. (2012). Towards a smart State? Inter-agency collaboration, information integration, and beyond. *Information Polity*, *17*(3–4), 269–280. https://doi.org/10.3233/IP-2012-000287

Gil-Garcia, J. R., Pardo, T. A., & De Tuya, M. (2019). Information Sharing as a Dimension of Smartness: Understanding Benefits and Challenges in Two Megacities. *Urban Affairs Review*. https://doi.org/10.1177/1078087419843190

Goldby, M. (2008). Electronic bills of lading and central registries: What is holding back progress? In *Information and Communications Technology Law* (Vol. 17, Issue 2, pp. 125–149). https://doi.org/10.1080/13600830802239381

Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*, *26*(4), 377–409. https://doi.org/10.1007/s10506-018-9223-3

Grainger, A., Huiden, R., Rukanova, B., & Tan, Y. H. (2018). What is the cost of customs and

borders across the supply chain? ... and how to mitigate the cost through better coordination and data sharing. *World Customs Journal*, *12*(2), 3–30.

Hamza, H., Sehl, M., Egide, K., & Diane, P. (2011). A conceptual model for G2G relationships. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6846 LNCS*, 285–295. https://doi.org/10.1007/978-3-642-22878-0_24

Hesketh, D. (2009). Seamless electronic data and logistics pipelines shift focus from import declarations to start of commercial transaction. *World Customs Journal*, *3*(1), 27–32.

Hesketh, D. (2010). Weaknesses in the supply chain: Who packed the box? *World Customs Journal*, *4*(2), 3–20.

Hevner, A. R. (2007). *A Three Cycle View of Design Science Research A Three Cycle View of Design Science Research*. *19*(2), 87–92.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Hofman, W., & Bastiaansen, H. (2013). Towards an IT infrastructure for compliance management by data interoperability–the changing role of authorities. *Paper Presented at the 6th European …*, *xx*(October).

Hofman, W., Spek, J., & Dalmolen, S. (2019). Supply Chain Visibility Ledger. *6th International Physical Internet Conference*, 1–14. https://doi.org/10.4324/9781315611341

Hulsebosch, B., Lenzini, G., & Eertink Partner, H. (2009). *COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME ICT Policy Support Programme (ICT PSP) Towards pan-European recognition of electronic IDs (eIDs) Work Package : 2 Organisation name of lead contractor for this deliverable : Dutch Ministry of the Interior*.

Hulstijn, J., Overbeek, S., Aldewereld, H., & Christiaanse, R. (2012). Integrity of supply chain visibility: Linking information to the physical world. *Lecture Notes in Business Information Processing*, *112 LNBIP*, 351–365. https://doi.org/10.1007/978-3-642-31069-0_29

IBM. (2017). *Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain - United States - Accessed 2020-02-21*. IBM News Room. https://www-03.ibm.com/press/us/en/pressrelease/51712.wss#feeds

International Chamber of Shipping. (2017). *International Chamber of Shipping (ICS) - Accessed 2020-02-22*. International Marine Organizations. https://doi.org/10.1007/978-94-009-8261-1_7

Iordache, E. V. A. V. ,. (2007). Customs Risk Management in the European Union. *Romanian Economic Journal*, *25*, 55–72.

ISO. (1995). *ISO 6346:1995 - Freight containers -- Coding, identification and marking*. 23. https://www.iso.org/standard/20453.html

Johnson. (2010). Information security basics. *ISSA*.

Karp, A., Haury, H., & Davis, M. (2011). From ABAC to ZBAC: The evolution of access control models. *5th European Conference on Information Management and Evaluation, ECIME 2011*, 202–211.

Klievink, B., Bharosa, N., & Tan, Y. H. (2016). The collaborative realization of public values and business goals: Governance and infrastructure of public-private information platforms. *Government Information Quarterly*, *33*(1), 67–79. https://doi.org/10.1016/j.giq.2015.12.002

Klievink, B., Van Stijn, E., Hesketh, D., Aldewereld, H., Overbeek, S., Heijmann, F., & Tan, Y. H. (2012). Enhancing visibility in international supply chains: The data pipeline concept. *International Journal of Electronic Government Research*, *8*(4), 14–33. https://doi.org/10.4018/jegr.2012100102

Knol, A., Klievink, B., & Tan, Y. H. (2014). Data sharing issues and potential solutions for adoption of information infrastructures: Evidence from a Data Pipeline Project in the Global Supply Chain over Sea. *27th Bled EConference: EEcosystems - Proceedings*.

Koski, A., & Mikkonen, T. (2017). Requirements engineering for service and cloud computing. In *Requirements Engineering for Service and Cloud Computing* (pp. 3–21). Leeds, UK.

Springer International Publishing. https://doi.org/10.1007/978-3-319-51310-2

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382–401. https://doi.org/10.1145/357172.357176

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. G. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. [Foreword: The Long Road To Bitcoin]. *Princeton University Press*, 304. https://doi.org/10.1016/j.vetimm.2013.08.005

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. In *Government Information Quarterly* (Vol. 34, Issue 3, pp. 355–364). https://doi.org/10.1016/j.giq.2017.09.007

Overbeek, S., Klievink, B., Hesketh, D., Heijmann, F., & Tan, Y. H. (2011). A Web-based data pipeline for compliance in international trade. *CEUR Workshop Proceedings*, *769*, 32–48. http://customs.hmrc.gov.uk.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pruksasri, P., Berg, J. Van Den, Hofman, W., & Tan, Y. H. (2014). Data concealing of supply chain transactions using the Distributed Trust Backbone. *2014 9th International Conference for Internet Technology and Secured Transactions, ICITST 2014*, 151–156. https://doi.org/10.1109/ICITST.2014.7038796

Pruksasri, P., Van Den Berg, J., Hofman, W., & Daskapan, S. (2013). Multi-level access control in the data pipeline of the international supply chain system. *Contributions to Economics*, 79–90. https://doi.org/10.1007/978-3-642-41585-2-7

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems*, *20*(9), 1388–1403.

https://doi.org/10.17705/1jais.00571

Rukanova, B., Henningsson, S., Zinner Henriksen, H., & Hua Tan, Y. (2018). Digital Trade Infrastructures: A Framework for Analysis. *Complex Systems Informatics and Modeling Quarterly*, *01*(14), 1–21. https://doi.org/10.7250/csimq.2018-14.01

Rukanova, B., Henriksen, H. Z., Henningsson, S., & Tan, Y. H. (2017). The anatomy of digital trade infrastructures. *Lecture Notes in Business Information Processing*, *295*, 184–198. https://doi.org/10.1007/978-3-319-64930-6_14

Rukanova, B., Huiden, R., & Tan, Y. H. (2017). Coordinated border management through digital trade infrastructures and trans-national government cooperation: The FloraHolland case. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10428 LNCS*, 240–252. https://doi.org/10.1007/978-3-319-64677-0_20

Rukanova, B., Wigand, R. T., van Stijn, E., & Tan, Y. H. (2015). Understanding transnational information systems with supranational governance: A multi-level conflict management perspective. *Government Information Quarterly*, *32*(2), 182–197. https://doi.org/10.1016/j.giq.2014.12.003

Scherer, M. (2017). *Performance and Scalability of Blockchain Networks and Smart Contracts*. 46. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1111497&dswid=8567

Sekeran, U., & Bougie, R. (2016). *Research Methods for Business - A Skill-Building Approach*. Chichester, UK. Wiley.

Selsky, J. W., & Parker, B. (2005). Cross-sector partnerships to address social issues: Challenges to theory and practice. *Journal of Management*, *31*(6), 849–873. https://doi.org/10.1177/0149206305279601

Selsky, J. W., & Parker, B. (2010). Platforms for Cross-Sector Social Partnerships: Prospective Sensemaking Devices for Social Benefit. *Journal of Business Ethics*, *94*(SUPPL. 1), 21–37. https://doi.org/10.1007/s10551-011-0776-2

Shafiq, B., Vaidya, J., Atluri, V., & Chun, S. A. (2010). UICDS compliant resource management

system for emergency response. *11th Annual International Conference on Digital Government Research (Dg.o 2010)*, 23–31. https://dl.acm.org/doi/abs/10.5555/1809874.1809882

Susha, I., Rukanova, B., Ramon Gil-Garcia, J., Tan, Y. H., & Hernandez, M. G. (2019). Identifying mechanisms for achieving voluntary data sharing in cross-sector partnerships for public good. *ACM International Conference Proceeding Series*, 227–236. https://doi.org/10.1145/3325112.3325265

Tasca, P., & Tessone, C. J. (2019). A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger*, *4*. https://doi.org/10.5195/ledger.2019.140

The Economist. (2018). *Technology and international trade - The digitisation of trade's paper trail may be at hand | Finance and economics | The Economist - Accessed 2020-02-21*. https://www.economist.com/finance-and-economics/2018/03/22/the-digitisation-of-trades-paper-trail-may-be-at-hand

The European Court of Auditors. (2019). *Special Report - Fighting fraud in EU spending: action needed (pursuant to Article 287(4), second subparagraph, TFEU)* (Vol. 287, Issue 01, p. 100). https://www.eca.europa.eu/Lists/ECADocuments/SR19_01/SR_FRAUD_RISKS_EN.pdf

Thomas, J., & Tan, Y. H. (2015). Key design properties for shipping information pipeline. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9373*, 491–502. https://doi.org/10.1007/978-3-319-25013-7_40

Tradelens. (2019). *Solution Brief*. 1–11. https://www.tradelens.com/wp-content/uploads/2019/05/TradeLens-Solution-Brief_Edition-Two.pdf

TradeLens. (2020). *Data Sharing Specification* (Issue March).

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys and Tutorials*, *18*(3), 2084–2123. https://doi.org/10.1109/COMST.2016.2535718

Urciuoli, L., Hintsa, J., & Ahokas, J. (2013). Drivers and barriers affecting usage of e-Customs - A global survey with customs administrations using multivariate analysis techniques. *Government Information Quarterly*, *30*(4), 473–485. https://doi.org/10.1016/j.giq.2013.06.001

van Engelenburg, S., Janssen, M., Klievink, B., & Tan, Y. H. (2017). Comparing a shipping information pipeline with a thick flow and a thin flow. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10428 LNCS*, 228–239. https://doi.org/10.1007/978-3-319-64677-0_19

Van Engelenburg, S., Rukanova, B., Hofman, W., Ubacht, J., Tan, Y.-H., & Janssen, M. (2020). *Aligning stakeholder interests , governance requirements and blockchain design in business and government information sharing*. 1–13.

Verschuren, P., & Hartog, R. (2005). Evaluation in design-oriented research. *Quality and Quantity*, *39*(6), 733–762. https://doi.org/10.1007/s11135-005-3150-6

Vukolić, M. (2016). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9591*, 112–125. https://doi.org/10.1007/978-3-319-39028-4_9

Widdowson, D. (2007). The changing role of customs: Evolution or revolution? *World Customs Journal*, *1*(1), 31–37.

Wright, C. S. (2019). Bitcoin: A Peer-to-Peer Electronic Cash System. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3440802

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The blockchain as a software connector. *Proceedings - 2016 13th Working IEEE/IFIP Conference on Software Architecture, WICSA 2016*, 182–191. https://doi.org/10.1109/WICSA.2016.21

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. *Proceedings - 2017 IEEE*

International Conference on Software Architecture, ICSA 2017, 243–252. https://doi.org/10.1109/ICSA.2017.33

Yasui, T. (2011). *Case Studies on Systematic Exchange of Commercial Information between Customs Administrations in Bilateral and Regional Arrangements*. www.wcoomd.org.Theauthormaybecontactedviacommunication@wcoomd.org.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, *October*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Appendix

Appendix A – Expected volumetric

This section presents the calculation for the expected volumetric of information on the platform.

Number of ENS document

This number is provided by the EC, as also mentioned in section 4.3, and amounts to 29.3 ENS data submissions (transactions) per second (DG TAXUD, 2017c).

Number of vessels

According to EuroStat[9], in 2018 2.19 million vessels arrived in European ports. This number includes both incoming and outgoing cargos. In order to estimate the number of only incming cargos, numbers from the Port of Rotterdam authority[10] have been used. According to this source, the number of incoming containers represents 52% of the total. Assuming that on average, outgoing vessels are loaded with the same number of containers as incoming vessels, it can be inferred that the number of incoming vessels is 52% of 2.19 million, which equals 1.14 million vessels.

For each incoming vessel, 2 events need to be issued, arrival and departure, plus the planned, estimated and actual for each event, which totals 6 events for each vessel. This requires 1.14millionx6= 6.84 million events per year.

[9] https://ec.europa.eu/eurostat/statistics-explained/index.php/Maritime_ports_freight_and_passenger_statistics

[10] https://www.portofrotterdam.com/sites/default/files/facts-and-figures-port-of-rotterdam.pdf

	Calculation	Total
Total vessels	2.19 million	2.19 million
Incoming vessels	2.19 million x 52%	1.14 million
Events	1.14 million x 6	6.84 million

Number of containers

According to EuroStat, 71 million containers have been handled in 2018 by the top 20 EU ports. 52% represents the incoming containers, which equals to 37 million incoming containers. For each container, 4 events are issued, load, unload, is_at and left, plus planned, estimated and actual for each event, which totals 12 events for each container. This requires 12x37million = 443 million events per year.

In addition, since each container needs to be represented by a digital twin, a transaction needs to be executed, thus 37 million transactions per year.

	Calculation	Total
Total containers	71 million	71 million
Incoming container	71 million x 52%	37 million
Events	71 million x 12	443 million

Changing transport plan

When there are changes in a transport plan, a new set of planned events need to be issued. Considering a worst-case scenario where all transport plans are changed, this requires 2 new

events for each incoming vessel, totalling 2x1.14 million = 2.28 million events per year, and 4 new events for each container, totalling 4x37million = 114 million events per year.

	Calculation	Total
New incoming vessels events	2 x 1.14 million	2.28 million
New incoming container events	4 x 37 million	114 million

Total

Summing up all the calculations, the total amounts to 565 million events per year. Considering a distribution of submissions mainly during business hours (5 days a week, 40 hours a week), the expected volumetric is 75[11] events per second.

	Calculation	Total
Vessel Events	1.14 million x 6	6.84 million
Container Events	71 million x 12	443 million
New incoming vessels events	2 x 1.14 million	2.28 million
New incoming container events	4 x 37 million	114 million
Total	6.84 + 443 + 2.28 + 114	565 million

[11] 565 million events/260 days/8 hours/60 minutes/60 seconds

Concerning the number of transactions, 29.3 ENS per seconds plus additional 5[12] transactions per second to register container digital twins, totalling around 34 transactions per second.

All the above-mentioned calculations are not to be intended as an exact estimate of the volumetric, but as a baseline. These do not include growth in global trade or unforeseen events (e.g. pandemics etc.). The number of vessels and ports have not been considered since they do no significantly change the total amount.

[12] 37 million transactions/260 days/8 hours/60 minutes/60 seconds