Transforming Towards Secure Global Trade for Customs Administrations Powered by Blockchain

التحول نحو تجارة عالمية آمنة لإدارة الجمارك بدعم تقنية البلوك تشين

by

HUSSAM JUMA MOHAMMED

A thesis submitted in fulfilment

of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

at

The British University in Dubai

June 2020

Transforming Towards Secure Global Trade for Customs Administrations Powered by Blockchain

التحول نحو تجارة عالمية آمنة لإدارة الجمارك بدعم تقنية البلوك تشين

by

HUSSAM JUMA MOHAMMED

20170264

A thesis submitted to the Faculty of Engineering and Informatics

in fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

at

The British University in Dubai

June, 2020

Thesis Supervisor
Professor Khaled Shaalan

Approved for award:

_____	_____
Name	Name
Designation	Designation
_____	_____
Name	Name
Designation	Designation

Date: _____

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

Hussam Juma

_____

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

Abstract

As part of the international trade supply chain, Customs authorities act as the gatekeeper protecting the society and the economy. The trade supply chain involves several participants each performs its task based on the documents that are provided by the other participant in the trade supply chain. For instance, the customs officials process the customs declaration submitted by the broker and then send the results to the next participant. The customs authorities need to perform an accurate risk assessment to ensure that protection of society and trade are not impacted. The verification and risk assessment are costly processes. The isolation between the participants in the trade supply chain impacts the efficiency of the current international trade supply model.

In this work, a blockchain-based solution with a plugin to empower the solution with risk assessment capabilities is proposed. To build this solution, a proof of concept (PoC) approach is followed using the IBM Hyperledger fabric and Python programming language. The participants of this international trade process are identified. Then, the detailed process, activities, assets, transactions that are performed by each participant are analyzed. After that, a solution architecture is designed followed by building the smart contracts and building the PoC. This computational model ensures secure transactions, traceable transactions, and an immutable data communication model for better coordination among the entities along the supply chain. To further enhance the blockchain solution, two models are proposed to provide Customs authority with online risk assessment capabilities; distributed risk assessment method and a hybrid risk assessment method that consists of distributed and centralized risk assessment processes. The real data used in this work was obtained from Dubai Customs and contains shipment declaration applications. This labelled data is used to evaluate two models. The first method reported significant results that can provide classification with 83% in terms of accuracy. While, the accuracy in the extended work for the first method achieved a higher accuracy of 92%. This work addresses important issues related to security and risk assessment and provide powerful methods that complement the risk assessments performed at the customs authority by providing feedback from the early stage of risk analysis.

الملخص

كجزء من سلسلة توريد التجارة الدولية، تعمل سلطات الجمارك بمثابة حارس يحمي المجتمع والاقتصاد. تتضمن سلسلة التوريد التجارية عدة مشاركين يؤدون كل منهم مهمته بناءً على المستندات التي يقدمها المشارك الآخر في سلسلة التوريد التجارية. على سبيل المثال، يقوم موظفو الجمارك بمعالجة البيان الجمركي المقدم من قبل الوسيط ومن ثم إرسال النتائج إلى المشارك التالي. تحتاج السلطات الجمركية إلى إجراء تقييم دقيق للمخاطر لضمان عدم التأثير على حماية المجتمع والتجارة. تعتبر عمليات التحقق وتقييم المخاطر عمليات مكلفة على السلطات الجمركية. تؤثر العزلة بين المشاركين في سلسلة الإمداد التجاري على كفاءة نموذج الإمداد التجاري الدولي الحالي. في هذا العمل، يُقترح حل بالاعتماد على تقنية البلوك تشين ع مع مكون إضافي لتمكين الحل بقدرات تقييم المخاطر. لبناء هذا الحل، يتم اتباع نهج الدليل والنموذج التجريبي للمفهوم باستخدام نسيج اي بي ام هيبرلدجر ولغة البرمجة بايثون. تم تحديد المشاركين في عملية التجارة الدولية هذه. بعد ذلك، يتم تحليل تفاصيل العمليات والأنشطة والأصول والمعاملات التي يقوم بها كل مشارك في السلسلة. بعد ذلك، يتم تصميم هندسة الحلول متبوعة ببناء العقود الذكية وبناء النموذج التجريبي. يضمن هذا الحل المعاملات الآمنة والمعاملات التي يمكن تتبعها ونموذج اتصال البيانات غير القابل للتغيير لتحسين التنسيق بين الكيانات على طول سلسلة التوريد. لزيادة تعزيز حل البلوك تشين، تم بناء نموذجان لتزويد السلطات الجمركية بقدرات تقييم المخاطر بشكل آني؛ طريقة تقييم المخاطر الموزعة وطريقة تقييم المخاطر المختلطة التي تتكون من عمليات تقييم المخاطر الموزعة والمركزية. يتم استخدام هذه البيانات لتقييم أداء النموذجين المقترحين في هذا العمل. حققت الطريقة الأولى نتائج مهمة يمكن أن توفر تصنيفًا بنسبة 83٪ من حيث الدقة في المتوسط. بينما حققت الطريقة الثانية نتائج أفضل بدقة وصلت إلى 92٪. يتناول هذا العمل قضايا مهمة تتعلق بالأمن وتقييم المخاطر ويوفر طرقًا قوية تكمل تقييمات المخاطر التي يتم إجراؤها في مصلحة الجمارك من خلال توفير التغذية المرتدة من المرحلة المبكرة لتحليل المخاطر.

Dedication

At first, I dedicate this work to my family, my colleagues and Dubai Customs. I also would like to dedicate this work to the United Arab Emirates for providing me with full support to succeed in every aspect of my educational development.

Acknowledgement

I would like to acknowledge everyone who played a role in my academic accomplishments. First of all, I would like to express my sincere gratitude to my advisor Prof. Khaled Shaalan for the continuous support of my Ph.D. study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D. study.

Besides my advisor, I would like to thank the second supervisor of my thesis: Prof. Ibrahim Kamel, for the insightful comments and encouragement, but also for the hard question which incented me to widen my research from various perspectives.

My deep and sincere gratitude also goes to my family, who supported me with love and understanding. Without you, I could never have reached this current level of success. Finally, Dubai Customs, each of whom has provided patient advice and guidance throughout the research process specifically the Intelligence Department. In addition, for their support in providing the required dataset through a formal agreement.

Thank you all for your unwavering support.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

B2C	Business-to-Consumer
B2B	Business-to-Business
B2G	Business-to-Government
BoL	Bill of Lading
C2C	Consumer-to-Consumer
CoC	Contract of Carriage
DLT	Distributed Ledger Technology
EPC	Electronic Product Code
GDP	Gross Domestic Product
HACCP	Hazard Analysis and Critical Control Points
HS-code	Harmonized System code
IoT	Internet of Things
IIoT	Industrial Internet of Things
LOF	Local-density Outlier Factor
P2P	Peer to Peer
PBP	Peer Blockchain Protocol
PoA	Proof-of-Authority
PoC	Proof of Concept
PoS	Proof-of-Stack
PoW	Proof-of-Work
RFID	Radio Frequency Identification
RPA	Robotic Process Automation
RTA	Road and Transport Authority
UNECE	United Nations Economic Commission for Europe

1. Chapter 1: Introduction

1.1. Trade Supply Chain

The formalities of trade and supply are often burdensome, time consuming and inefficient. Trade being a major factor in determining a country's economic viability, eliminating unnecessary cost and procedural challenges will ensure delivery of effective trade services. From the perspective of the trade supply chain parties, availing information about goods to all participating parties at the right time and place is of great economic value. For example, information about the provenance of goods, the terms of trade, the ownership of goods, the credit exchange data, tariff codes, classification data, import/export data, certificates, manifests, loading and unloading lists, customs values and status information is highly critical (Lehmacher, 2017).

The supply chain involves a number of activities performed by various private and public parties. Activities are carried out subject to certain terms, factors of business and methods of operation. For a supply chain to operate effectively and efficiently we need to clearly identify and manage relationships and activities.

Efficiency of trade procedures refers to the speed and ease with which cross-border business transactions are conducted with high degree of quality. Lowering supply chain barriers is critical in eliminating resource waste and reducing costs to trading firms, consumers and society. Supply chain barriers can result from inefficient procedures, regulations and infrastructure services, among many others. The supply chain is a set of

activities performed in producing and getting a product to consumers (Figure 1-1). It spans the manufacturing process as well as transport and distribution services.

Figure 1-1 Buy-Ship-Pay Model (UNECE, 2013)

Supply chain barriers is a major burden for governments, businesses and the economy resulting in the following:

1. Greater operating cost and increased expenditures
2. Long and unpredictable formalities
3. Reduce volume of trade
4. Increase risk

Reducing operating costs remains the most frequently pursued goal. Consequently, companies incurring additional costs due to barriers may discover that it is no longer feasible to continue participating in a specific market and resort to reducing their volume of trade. Companies that suffer reduced volume usually see a rise in their production costs due to their inability to sustain and capture economies of scale (Lehmacher & Mcwaters, 2017).

Procedures, formalities and mechanisms that help simplify and standardize information flows related to the import and export of goods can help reduce or eliminate un-necessary steps and improve transparency. Countries that are interested in attracting investments need to essentially increase the speed at which and the reliability of movement of goods they import or export within their borders.

The economic impact is felt by many countries and action is required to ensure the current barriers do not impact their GDP. Authorities and businesses must immediately collaborate on effective ways and mechanisms to eliminate supply chain barriers and encourage participation of small and medium-sized enterprises.

So how the trade supply chain being impacted? In international trade, there are potentially between 40 to 50 different actors involved. These commonly fall under 4 categories: Customer, Intermediary, Supplier and Authority (Table 1).

Actor Types	Description	Possible Actors & Roles
Customer	A party acquiring goods or services through trade	Buyer
		Consignee
		Payer
		Importer
Supplier	A party providing goods and services	Consignor
		Payee
		Seller
		Manufacturer
		Exporter
Authority	A statutory body who regulates trade and monitors compliance	Chamber of Commerce
		Consular
		Customs
		Health
		Licensing
		Receiving Authority (Port Authority)
Intermediary	A commercial party providing services within the international supply chain	Bank / Financial Institution
		Broker
		Carrier
		Credit Checking Company
		Credit insurer
		Commission Agent
		Export Agent
		Freight forwarder
		Import Agent
		Insurer
		Receiving authority

Table 1-1 Actors and Roles

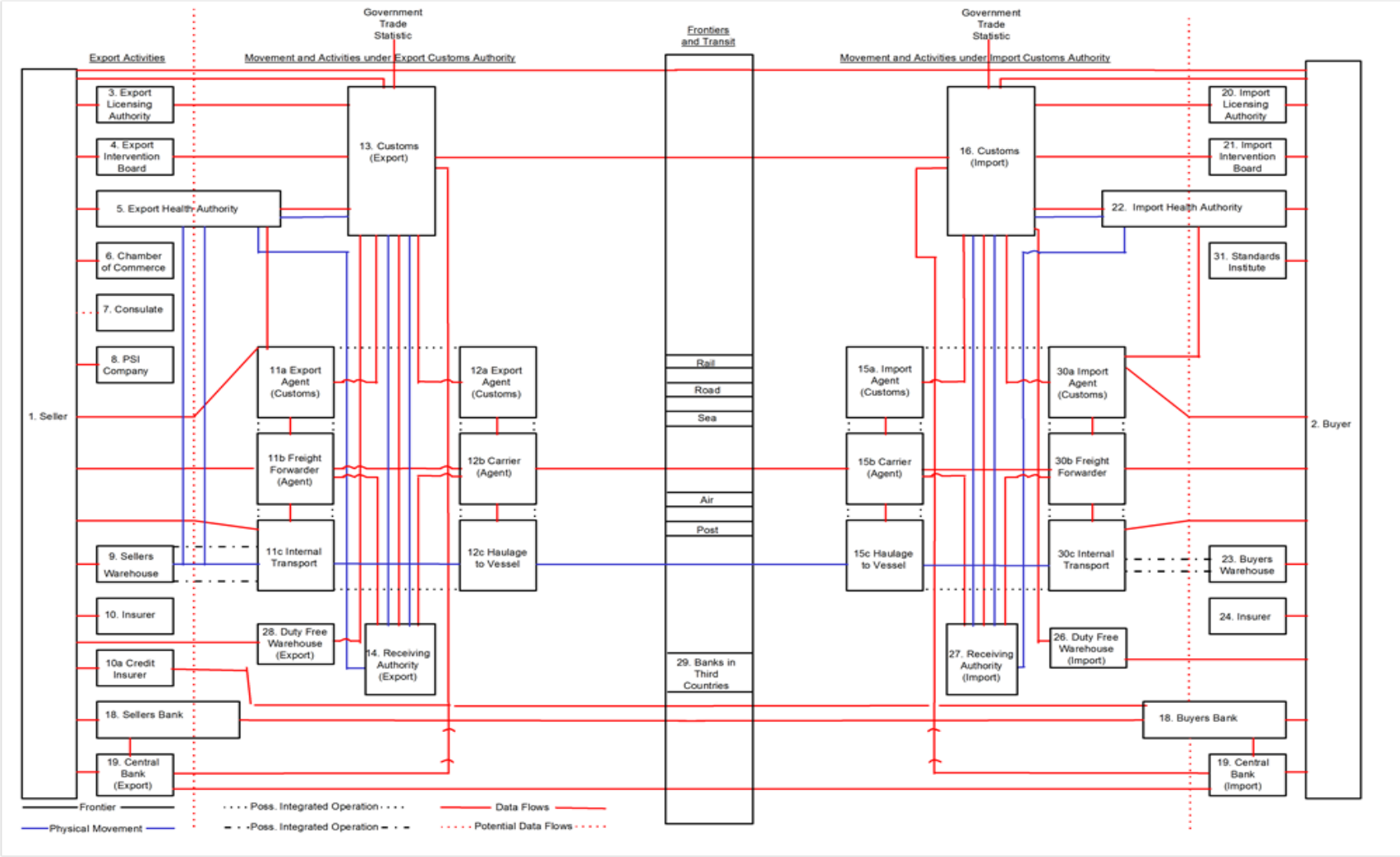

Figure 1-2 Parties and Information Flow in The Supply Chain (CITE)

Global trade involves a lot of paperwork – costing time and money. In trade, the legal instrument which is as old as trade itself is called the Bill of Lading (BoL). A BoL is a legal document issued by the Carrier or agent of the Carrier and has three main attributes:

- Document of Title to the goods: possession of the BoL is equal to proof of legal rights of ownership of goods which can be transferred from one person to another merely by its delivery or endorsement
- Receipt – Provides evidence the Carrier has received the goods in compliance with the Commercial Contract between the parties
- Contract of Carriage - Evidence of the Contract of Carriage (CoC) - that the carrier will transport the goods in compliance with the Commercial Contract.

Paper-based freight documents like the bill of lading are susceptible to loss, tampering, and fraud. Additionally, Letter of Credit as a Financial Instrument is required if the Seller and Buyer do not have a trust relationship. When the goods are shipped using at least two different transportation modes, Letter of Credit will require a standard document which is the Bill of Lading to acknowledge receipt of Cargo. By providing the necessary transparency and consensus, the risk of documentary fraud can be mitigated resulting in the reduction of reconciliation transaction cost between and within the participating parties.

Paper-based Bill of Lading the standard document for trade are causing difficulties, costs, discrepancies and counterfeit products.

Counterfeit goods and products is a growing problem for parties of the supply chains. Counterfeits and pirated goods have a major impact on world market. It is estimated the imports of counterfeits are work half a trillion dollars a year amounting to 2.5% of global

imports (OECD/EUIPO, 2016). On the other hand, reports indicate that the counterfeit market today including online piracy generates returns of up to $600 billion annually. This amounts to $600 billion losses for businesses from across the world. This has major adverse influence on the sales and profits of firms as well as on revenue, security economy, health, safety and environment. This is a major concern for governments, businesses and consumers. Fake goods reaching consumers and markets are a global problem. Counterfeiting produces copies that endanger lives: faulty products or parts, medicines that make people sick, harmful toys, zero nourishment baby formula and instruments delivering false readings. Parties have to make sure authentic goods are sold and delivered to the consumers and can identify authentic products and avail to consumers where they can obtain them. Improving traceability of physical goods by creating an auditable and tamper-proof record of the journey behind all products across the supply chain. By preventing the selling of fake goods and counterfeits many benefits will be realized by businesses, society and the environment.

In the trade supply chain, identifying the origin of goods and products is a challenge for authorities. They have to get a quick and accurate information on where the goods originated or came from and which are affected and have to be removed from the stores. Failure in determining the origin of products is contributed to inefficient border procedures which lead to loss of revenue for governments and increased cases of smuggling. For example, the diamond trade market could potentially use blockchain for authenticity. Specific data about each diamond including its country of origin and the mine where it was recovered, is permanently recorded on a blockchain so it can be viewed by potential buyers who may want to check its credentials prior to completing a transaction. Goods Traceability

within a blockchain platform could theoretically provide guarantees about the authenticity of products in the supply chain.

1.2. Blockchain

Blockchain technology has emerged as a promising approach to ensuring the traceability and integrity of data. Blockchain technology is typically used to establish a decentralized system where, as a rule, such a system is implemented through the use of smart contracts. Similar to traditional legal contracts, smart contracts encapsulate the logical rules of the system and assure their enforcement through automation (Alzahrani & Bulusu, 2018).

Using blockchain technology, each of the participating entities has an identical copy of the entire transaction history, known as the ledger. The ledger consists of several blocks, and each block has a set of transactions. Blocks are connected together through hashing. A block hash value is obtained through the use of a hash function. One of the well-known hash function is the SHA-256, which regardless of the input size always returns 256 bit as a unique hash value. Each block stores the hash values of itself and the previous block (Figure 1-3). Therefore, at any time, changing the data of one block will result in changing the hash value of the block, and therefore it will no longer match the hash value stored in the next block. Through the use of hashing, we can ensure the integrity of the data (ledger), since it simplifies the process of detecting any manipulation in the data.

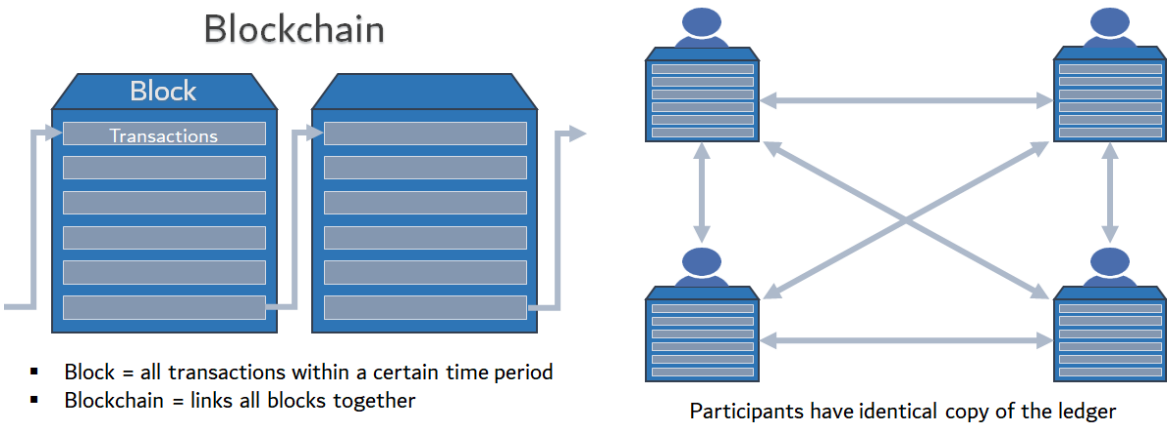

Figure 1-3 Blockchain and Ledger Architecture

By employing the concept of group consensus, the integrity of the data can be ensured. Each of the participants writes new transactions on a temporary block, and whenever a participant proposes a new block, the group consensus mechanism is triggered to validate the proposed block. Once the validity is confirmed, using this mechanism, each participating entity adds the new block to its ledger. To confirm the correctness of a given block, using group consensus, the majority of the participants must vote that it is identical to its local copy. If the correctness of the new block is not confirmed, it is deleted, and no participant will include this block in its ledger. The size of the block, the number of the transaction, is predetermined based on the application requirements. Blockchain solutions can be categorized into two main types: public blockchains and private blockchains.

1.2.1. Public Blockchains

Public blockchains e.g., Ethereum (Wood, 2018) are typically described as a permissionless blockchain, whereas anyone has permission to write new transaction (record) to the blockchain. Having the ability to interact with the blockchain in permissionless fashion introduce significant pressure on the consensus mechanism.

Therefore, strong consensus mechanism such as Proof-of-Work (PoW) and Proof-of-Stack (PoS) (Zheng, et al., 2018) are required to ensure the privacy and integrity of the data. Additionally, to establish some trust between the participants, all participants in this type of blockchain, must have the same authority (privileges). This decentralization of the authority privileges is crucial since in such environment no participant(s) should be able to control the blockchain.

1.2.2. Private Blockchains

In a private blockchain, e.g., Hyperledger Fabric (Cachin, 2016), only a subset of the entities (participants) have permission to write new records to the blockchain, and such a blockchain type usually is described as a permissioned blockchain. The identities of the participants in a private blockchain are known to each other, where we expect to have a single participant with administrative privileges. In this type of blockchain, the administrative participants register the other participants and determine their blockchain access permission. The presence of the administrative entity results in categorizing a private blockchain as centralized in terms of authority privilege since the entity with the administrative right can control the blockchain.

Additionally, having administrative participant(s) reduces the security pressure, as a rule, to be followed by each participant on the blockchain is pre-determined and the administrative participants monitor the flow of information in the blockchain. Therefore, a simplified consensus mechanism such as Proof-of-Authority (PoA) (Zheng, et al., 2018) can be implemented here. A consortium blockchain is similar to a private blockchain; however, in this blockchain, a consensus mechanism is performed by a pre-determined approved set of participants.

1.2.3. Scalability

In this work, scalability is defined as the ability to scale up the size of the network (number of transaction) without any interruption to the business process. Private blockchain solutions are considered more scalable compared to public blockchains. The difference between these two types of in this work, scalability is defined as the ability to scale up the size of the network, in terms of number of transaction without any interruption to the business process. Private blockchain solutions are considered more scalable compared to public blockchains. The difference between these two types of blockchain in terms of speed is related to the rule the nodes play in the network. In public blockchains, all nodes are identical regarding responsibility. All nodes perform the task of building consensus, managing the ledgers, and interacting with the user (client). In private networks, these tasks are assigned to different nodes, and this improves the performance in private blockchains compared to public blockchains. play in the network. In public blockchains, all nodes are identical regarding responsibility. All nodes perform the task of building consensus, managing the ledgers, and interacting with the user (client). In private networks, these tasks are assigned to different nodes, and this improves the performance in private blockchains compared to public blockchains (Guo & Liang, 2016).

In this section, we presented the general categorizations, which usually are used to describe any blockchain solution. However, these categorizations do not represent absolute values. In other words, being a permissioned or permissionless blockchain is not a 0-1 value. For instance, if we describe a blockchain solution as a permissioned blockchain, this means that the overall solution architecture has a permissioned behavior. In this solution, small

components might have permissionless behaviors, but they do not influence the overall behavior.

1.3. Blockchain-based Trade Supply Chain

In this section, to clarify the complexity of the international trading process in terms of information sharing, we discuss the importation process from the rest of the world to the local market. The employed importation process at Dubai Customs will be used throughout this discussion, and we will focus on the sea channel. Then, we briefly discuss the advantages of employing a blockchain solution to optimize the international trade supply chain.

1.3.1. Importation

Figure 1-4 presents the steps of the importation scenario by sea; other methods of transportation (air and land) follow relatively the same steps. In this trading domain, a large number of documents are exchanged between the trade supply chain entities. The figure shows the identity of the participants for this international trade supply chain. Once the importer and the exporter have agreed on the payment method, the exporter provides the importer with the following documents:

- Original bill of lading: it acts as a contract, which confirms the receipt of the cargo by the carrier (freight forwarder).
- Original commercial invoice.
- Certificate of origin: it shows where certain shipments of goods are manufactured and are proceeding to a specific country.

A few days before the shipment arrives, the importer submits the original bill of lading to the shipping agent, who obtains a delivery order to the importer. The importer is also required to submit the import declaration application to Dubai Customs to start the shipment clearance process. This process proceeds to assess the risk associated with this declaration. In situations where the declaration has failed the validation process, it will be rejected, and the customers will be informed. If the shipment is identified as not risky, the charges will be collected, and the clearance will be issued. In situations where the shipment is declared as risky, the declaration will be further analyzed. The output of this analysis process can be (1) clear without an inspection, (2) clear with inspection, (3) seek additional information from client, or (4) seek opinion. Clear with inspection refers to the requirement of physically inspecting the shipment by the customs agents to issue the clearance. Also, seek opinion refers to the process of involving customs agents to investigate several components of the declaration, such as valuation and tariff[1].

[1] That is, duty to be paid for importation and exportation.

Figure 1-4 The International Trade Supply Chain (Sea Transportation)

1.3.2. Customs Clearance and Blockchain

From the description, it is clear that validating the received documents is the most crucial step to ensure the completion of the importation business process. This step relies mainly on human judgment since there is no direct communication between the supply chain participants, and this increases the possibility of falsified documentation not being detected. This step can be optimized by establishing a secure information-sharing mechanism that ensures the integrity of the information exchanged between the supply chain participants.

Such an objective can be achieved by establishing blockchain-based information-sharing mechanism between the trade supply chain participants. In such a domain, a private blockchain network can be used to connect the (international) trade supply chain participants (Pawczuk, et al., 2019; Loklindt, et al., 2018; Smartz, 2018; Macedo, 2018) Thus, the involved participants (stakeholders) for any shipment can have direct access to the exchanged document. In such a network, using smart contracts, we can automate the process of validating and authenticating the trade documents. In addition, by connecting all of the involved participants to the network, we can simplify the auditing process, since the correctness of the documents has already been established.

1.4. Aims and Objectives

In this work, the objective is to provide a blockchain-based operating model components that optimizes the entire international trade supply chain. In particular, the components are designed to improve the processes of customs authorities as part of the international trade

supply chain. Typically, the currently employed operating model at customs tries to establish a trade-off between trade facilitation and protecting the public interest. Determining this balance has always been a challenging task, since any applied mechanism is expected to favor one of the factors (facilitation or protecting) more than the other. The aim of trade facilitation is to simplify the trading process to ensure the continued growth of the trading market. On the other hand, the task of protecting the local society and economy requires customs authorities to analyses and inspect the shipments to ensure the lawfulness of the trade. As already mentioned, the task of protecting the public interest involves several processes involving the customs authorities, where performing these processes is time-consuming in most cases. The complexity of the process has a negative influence on the trade facilitation factor, which aims to reduce the time involved in the trade process.

The proposed model addresses this issue by establishing a direct communication mechanism amongst the supply chain participants, and this ensures the receipt of the required documents by the customs authority in a timely manner. This gives the customs authorities the advantage of having enough time to process the shipment before it physically arrives at the port. In addition, through the use of blockchain technology, the operating model components automates the process of authenticating and validating the documents, since this technology ensures the integrity and immutability of the exchanged data between the supply chain participants. Therefore, the objectives of this work can be summarized as follows:

- Develop a blockchain-based approach to address the importation and exportation and ensure information authenticity from customs perspective.
- Develop a lightweight algorithmic method to be used by the blockchain-based approach for the detection of smuggling activities.

1.5. Research Questions

Taking the current complex situation into consideration, blockchain technology has emerged as a promising approach for the optimization of the international trade supply chain. By using this technology, the privacy and integrity of the exchanged information are guaranteed. In addition, blockchain technology comprises an information-sharing mechanism that guarantees data immutability and traceability. This, in turn, can establish a trusted communication model between the supply chain participants and guarantee that the customs authority will receive the required information on time. In addition, the inherent features of blockchain technology help in establishing a direct communication model between the customs authority and other participants in the international trade supply chain. In the customs domain, increasing the transparency of the operating model components increases the optimization space. This contributes towards optimizing the processing time and costs through the removal of redundant functionalities and in the simplification of the authentication and clearance processes.

In this study, the focus is on designing operating model components that deals with the importation and exportation scenarios at Dubai Customs. We consider Dubai Customs as a deployment environment for the proposed components. However, the proposed solution can be easily adopted by any other customs agency. The objective of the proposed

operating model components is to optimize the trading process by reducing the operational time and cost. In addition, the presented components are designed to target the shipment clearance process and all of its related sub processes, which include the risk assessment process, the auditing process, and the information verification and validation processes. Toward this end, this work addresses the following questions:

- Can blockchain address customs challenges relative to import and export information exchange to mitigate authenticity issues?
- Can we develop methods that result in the reduction of smuggling activities and raise risk assessment accuracy as part of a blockchain-based global trade formalities?

1.6. Focus and Key Contributions

This thesis is the combined work of four research papers:

- A Survey on Using Blockchain in Customs-based Trade Supply Chain Solutions (Juma, et al., 2019a)
- Customs-based Blockchain Solution for Exportation Protection (Juma, et al., 2019b)
- Enhanced Customs-based Distributed Risk Assessment Method (Juma, et al., 2019c)
- Customs-based Hybrid Risk Assessment Method

The focus of this thesis is to provide the following contributions:

1.6.1. Develop a Blockchain-based Approach to Address the Importation and Exportation and Ensure Information Authenticity from Customs Perspective

With the information-sharing mechanism currently used by customs authorities, verifying documents to prevent fraud and counterfeiting is an exceptionally costly, time-consuming activity. Because actors in international trade supply chains do not communicate with each other directly, customs authorities may ask customers to provide additional documentation that can verify documents already submitted. Additionally, because customs regulations vary from country to country, whether certain goods are permitted or prohibited by customs authorities also varies, while some goods may be allowed to enter countries provided that they have a special permit from government authorities. In the current operating model, although customers are expected to promptly provide all required permits for processing, delays in submitting the required documents are common and invariably prolong processing and raise shipment costs.

The lack of communication among actors in international trade supply chains reduces the efficiency of the current trade model. In particular, the semi-isolation of actors can result in the failure of customs authorities to identify fraudulent documents, which allows unhealthy products to enter communities and potentially cause harm to society. Such failure can also result in the trade of counterfeit products, which can significantly affect local economies, as well as reduce customs revenue, because documents may have been altered to lessen duties. At the same time, the lack of communication also lengthens

processing times and increases shipment costs, which intensifies pressure placed upon traders and, as a result, can reduce the volume of trade.

In this work, we propose a novel blockchain-based solution to optimize the operating model at Dubai Customs for various importation and exportation scenarios. The solution seeks to simplify the processes entailed in both kinds of scenarios and to establish direct, tamper-proof, information-sharing mechanisms for actors in international trade supply chains. To those ends, the proposed model consists of several computational components that chiefly target the processes of shipment clearance, auditing, and risk assessment.

The proposed computational model is designed to optimize the processing components used in international trade supply chains as a whole. That objective is driven by the need to fully automate customs authority-related processes in order to help customs authorities to facilitate trade while protecting society. The architecture of the model should ensure the simplicity of adding and modifying functionalities, which is possible by virtually dividing the presented model into layers such that each layer contains functionalities corresponding to the specific objective. In that way, any component will be able to be rewritten without significantly affecting the overall architecture.

1.6.2. develop a Lightweight Algorithmic Method to be Used by the Blockchain-based Approach for the Detection of Smuggling Activities

The functionalities of risk assessment encompass the process of analyzing shipment information and tracking shipments in order to identify any suspicious transactions or activities. Risk assessment is typically performed by customs authorities in a centralized

fashion. In that process, whenever information concerning a new shipment becomes available, it is entered into the risk assessment engine to examine the shipment, which involves comparing the shipment's features (i.e. attributes) with available historical data as part of following a learning-based model. Consequently, the accuracy of the assessment depends upon the historical data provided and the number of attributes—up to 120—that can be used to describe each shipment and transaction. In that sense, the model is complex in terms of computational requirements, and any irregularity in shipping activity heightens the pressure on customs authorities to provide and perform reliable services in a timely manner. Moreover, once a shipment is declared to be risky, then several time-consuming manual processes are required to clearly identify the source of the risk.

To address this problem, in the model we propose a lightweight algorithm solution that reduces the complexity of the risk assessment by highlighting factors in the classification of shipments as risky. As an online algorithm, the solution involves performing risk assessment at different stages of supply chain when any actor submits shipment information to the blockchain. For instance, once a manufacture uploads an invoice to the blockchain, then risk assessment can be performed on the information in the invoice (e.g. amount and type of good). Such assessment will return an outlier factor that can be directly submitted to customs authorities via the proposed model to inform their identification of suspicious shipment. In particular, high outlier factors (e.g. 10) increase suspicion about the shipment more than low ones (e.g. 3).

The principal idea of the proposed solution is to divide the space for historical data into safe and risky compartments for each supply chain actor (e.g. manufacturers and shipping

agents). Once new shipment information is received by one of those actors, the algorithmic approach will identify the space with the most similar behavior among past shipments. The outlier factor for the shipment will be calculated to determine whether it should be treated as risky. A major advantage of the approach is that customs authorities will analyses the outlier factors of shipments at early stages of the shipment's life, which will afford authorities more time to perform detailed analyses.

1.7. Researcher Role

The researcher is a director at Dubai Customs with responsibility for shaping and designing the techno-functional procedures of the organization. In this work, the researcher engaged the relevant departments to explain his research intent and verify his findings in comparison to existing operational tools and practices such as measuring the effectiveness and efficiency of the proposed framework as well as measuring the accuracy of the proposed risk assessment methods. Datasets used included previously shared data from other government entities, which did not require the researcher to engage external parties. The domain experts of each concerned business function within the organization verified the research outcomes and presented their feedbacks with the researcher.

1.8. Thesis Structure

The thesis comprises eight chapters.

- Chapter 2 provides a comprehensive literature review on the work done in the area of trade supply chain using blockchain technology.

- Chapter 3 illustrates the research methodology and approach followed to address research objectives and answer the research questions.
- Chapter 4 presents the architecture of the proposed blockchain-based system and prove that the proposed solution will change build the trust the trade supply chain relative to authenticity.
- Chapter 5 tackles a fundamental problem with the trade supply chain relative to risk assessment within blockchain platform using distributed approach to detect the suspicious transactions.
- Chapter 6 extends what was done in Chapter 5 and provides a higher performance algorithm in terms of accuracy using outlier hybrid mechanism to detect the suspicious transactions.
- Chapter 7 discusses the key findings of the thesis and provides answers to the research questions.
- Chapter 8 concludes with the results and recommendations for future works.

1.9. Conclusion

This chapter provided a background about the trade supply chain and various issues that faces this domain from customs perspective. In addition, it tackles the potential of using blockchain technology by illustrating the various features of this technology and the applications in which this technology can be utilized in this domain. This chapter also provide details on the aims, objectives and research questions that form the focus of this thesis and the key contributions.

2. Chapter 2: Literature Review

2.1. Introduction

The trade supply chain represents the required steps to complete the trading process, which eventually results in delivering the goods to the buyer. The process of trade involves a legal bind agreement between the trading parties (seller and buyer), which specifies the conditions that must be addressed by each party for the successful completion of the trade. For instance, these conditions could specify the acceptable transportation method for the goods. The trading process is typically monitored by a third-party that acts as a regulator for the trade. The main task of this entity is to make sure that all parties fulfil the agreement conditions. In case of a dispute between the trading parties, the regulatory entity will act to resolve the issue. For instance, customers who use the Amazon trading platform can inform the platform administration if the received goods do not match the posted description by the sellers. In such a process, the employed information-sharing mechanism must ensure the integrity of the exchanged information to simplify the process of trade between trading parties.

The complexity of the trading process increases significantly in the international trading scenario. International trade involves many parties, mainly including the trading community (importers and exporters), customs agency, shipping agent, port operators, freight forwarders, and customs brokers. The freight forwarders arrange shipments for customers. The shipping agents usually deal with the transportation of cargo. A customs broker usually is responsible for the preparation of the shipment declaration information,

which will be submitted to the customs agency. During the trade, each of the involved entities performs its task based on the documents that are provided by other entities in the trade supply chain. For instance, the customs process the declaration application submitted by the broker, and then send its result, the clearance, to the next entity in the supply chain.

In the international trade supply chain, the employed information sharing mechanism is also a dominant factor in determining the overall efficiency of the supply chain. In this trading domain, several entities require access to the documents from the different participants in the supply chain in a timely manner. A key document's dependent entity in this supply chain is the customs authority, which plays an important regulatory role. Customs authority acts as the gate that protects society and the economy. The protection task is established by monitoring the flow of goods entering the country to detect counterfeit products and smuggling activities. To fulfil this task, customs authority relies on the information provided by several participants in the international trade supply chain. This information is used in the shipment clearance process to examine the shipment under consideration and to determine if a physical examination is required (World Customs Organization, 2018).

The issue of ensuring the integrity of the exchanged information can be addressed by providing a traceable secure system that allows the trade participants to gain access to the data (document) in a timely manner. In this system, once a document is submitted, participants gain access to this document based on their role in the trade model. Additionally, the system must be able the provide the users with the ability to trace the status of the shipment through the entire trade supply chain model. Towards this end,

several proposals (Allen, et al., 2019; McDaniel & Norberg, 2019; Belu, 2019; Chang, et al., 2019; Xu, et al., 2018; Engelenburg, et al., 2017; Rauchs, et al., 2019) have investigated the use of blockchain technology to optimize the (international) trade supply chain. Blockchain technology has revolutionized the manner in which trust can be established between entities. Thus, the participants of the trade supply chain can share their information without any privacy concern. Blockchain is Distributed Ledger Technology (DLT) in which records (data) are stored in block format, where these blocks are linked (chained) using cryptography (C. Technologies, 2018; Blockchain Training Alliance (BTA), 2018). Blockchain technology can ensure the traceability and integrity of the shared data between the participating entities. These inherited features highlight the potential of optimizing the trade supply chain through the use of blockchain technology.

The main objective of this work is to study and highlight the impact of blockchain technology on simplifying the (international) trade supply chain. As a dominant participant in the international trade supply chain, we discuss the impact of the blockchain technology on simplifying the customs administration-related processes. Towards this end, this work addresses the following questions:

- **RQ1**: What is the impact of the blockchain technology on optimizing the trade supply chain?
- **RQ2**: What are the factors that influence the adoption of blockchain technology in the trade supply chain?
- **RQ3**: Can we improve the customs administration control of international trade through the use of blockchain technology?

2.2. Methodology

To address the research questions proposed in this work, we have conducted a detailed review and discussion about the use of blockchain technology in trade. This review adopts the methodological approach (Tranfield, et al., 2003), which mainly consists of three main steps: planning, execution, and reporting. In the planning step, we determine the search keywords and the protocol for execution. In addition, we determine the databases to execute this search. In the execution step, we follow the planned protocol to obtain the desired articles and information. In the reporting step, we address the presented question in this work, by discussing all factors that influence the question's solutions. Next, we describe the planning and execution steps, where the reporting step is described in the next section.

2.2.1. Planning

The search criteria are designed to help in addressing the research questions presented in this work. Accordingly, the main terms that are used in the research questions have also been used in the search criteria. These terms are "trade supply chain", "blockchain", "customs", "trade monitoring", "counterfeit trade" and "trade facilitation". In any of the performed search, the format of the search words can be represented as follows <blockchain and ANY>, where blockchain as a term must be included in addition to any other term(s). In this work, we have included peer-reviewed papers and working papers. The latter type of papers is normally generated from industrial corporations. In terms of peer-reviewed papers, we have focused the search on the following databases: IEEE, ACM, scientist Direct, Scopus, Springer, and Taylor and Francis. Working papers are included

in this work only if they address customs administration processes or originated from an important industrial company such as IBM (Androulaki, et al., 2018) or Deloitte (Pawczuk, et al., 2019).

2.2.2. Execution

We began by applying the above-mentioned search criteria, which returned 3,910 papers. Then, we have started the filtration process by removing all duplicate publications. This is followed by applying the inclusion/exclusion criteria. The inclusion criteria make sure to include all papers that clearly defined a trade application scenario or optimized a single (or multiple) components of the trade supply chain. All technical papers that address the security component in blockchain technology were excluded from this work. Additionally, general papers that describe blockchain technology were also excluded from consideration. Then, we removed survey papers, and we performed a quality assessment to make that the selected paper contributes to the research questions. These secondary selection criteria returned 105 papers.

We used these selected papers to determine the application categorization presented in the next section. This categorization is performed by reading the abstract section of each of the selected papers to identify the application scope for this work.

Additionally, for each application scenario, we limited the number of papers discussed to five. However, for papers dealing with customs administration-related processes, no limit was applied. This limitation was imposed to reduce the probability of discussing papers that share more or less the same main concept. In addition, proposals that addressed

customs administration-related processes were the only set of proposals that required a full discussion of the objective of the work. Other proposals are presented to fill the gap in terms of blockchain and the trade supply chain. At the end of this selection process, we were focusing mainly on 34 papers.

The analysis process of the selected papers was performed iteratively. In addition, the snowball technique was applied in this work. This technique emerged as a promising approach due to the difficulty of identifying a complete sample from official sources. Through this process, 35 manuscripts from conferences, technical reports, dissertations, and working papers were cited since they supported as well as being mentioned in the 34 selected papers.

2.3. Blockchain and Trade Supply Chain (Reporting)

In this section, we discuss proposals from the related literature that have investigated the use of blockchain technology to facilitate the (international) trade supply chain. In this trading scenario, the type of the employed blockchain solution is usually associated with the application domain. For instance, blockchain-based e-commerce solutions are generally deployed on a public blockchain, since anyone should be able to join the network, and all participants are expected to have the same authority privileges (all participants are equal). On the other hand, blockchain solutions that address the trading of highly regulated goods are expected to be deployed on a private blockchain. This deployment mechanism is crucial since participants in such trade processes are expected to perform several types of confirmation and validation steps. Accordingly, in this situation, the permission of each participant must be pre-determined by an administrative participant. For instance, to

address the food safety problem, a private blockchain architecture is required, since blockchain-based solutions to address this problem usually involve a predetermined set of participants.

Additionally, to ensure the quality of the food, several critical processes must be employed to ensure the authenticity and correctness of the uploaded information. Regarding blockchain solutions which are designed to improve components' supply chain performance, the environment where these solutions are deployed depends on the targeted processes. If the public customers do not interact mainly with the targeted processes, we expect such solutions to be deployed on a private blockchain. For instance, proposals that aim to optimize the information-sharing mechanism between the supply chain participants will be deployed on a private blockchain, since the registration and permission for each participant must be pre-approved by an administrative authority.

In this direction, towards addressing the first research question (RQ1), which is related to the impact of the blockchain technology on the trade supply chain, we start the presented discussion by categorizing the discussed proposals (34 papers) as follows (Figure 2-1 summarizes this classification):

- **Electronic trading solutions:** these solutions normally provide online trading platforms. The characteristics of these platforms underline a public blockchain as a suitable deployment environment since all participants will have the same level of authority.

- **Validation solutions:** These solutions are typically deployed on a private blockchain. In general, they are designed to address highly regulated trading processes. For instance, solutions that are proposed to prevent fake goods trading are normally deployed in a private blockchain, since the participants in such a blockchain are expected to be part of the supply chain, where each participant has predetermined permission.
- **Supply chain management solutions:** These solutions are designed to optimize the overall supply chain management. As for this category, we also discuss proposals that aim to optimize a single functionality in the trade supply chain. In general, we expect such solutions to be deployed on a private blockchain since public customers are not expected to interact with such processes. However, in situations where the target processes are designed to address customer requirements of the general public, a public blockchain could be a suitable deployment environment.

In all of these categories – especially the last two – a consortium blockchain could be a suitable environment for deployment if a predefined set of participants needs to perform the group consensus. This classification aims to identify and highlight the applications' domains of the trade supply chain, where blockchain technology can be used to optimize the trading processes. Accordingly, the presented discussion mainly aims to distinguish between the proposals in term of the following factors:

- Blockchain type (public / private / consortium).

- Authority distribution (centralized / decentralized).
- Accessibility (permissioned / permissionless).
- Scalability (number of transactions).

These factors aim to clarify the requirement of constructed blockchain-based solutions for each of the proposed application domains

2.3.1. Electronic Trading Solutions

This category focuses on trading solutions that are usually performed over a platform hosted on the Internet (or Intranet). The trading supply chain for such solutions consists typically of a small number of participants. These solutions mainly aim to provide users with a secure easy-to-use trading platform. In this trading domain, most of the proposed solutions are mainly designed to address energy trading and e-commerce trading.

2.4. Energy Trading

Several proposals have investigated the use of blockchain for energy trading in Industrial Internet of Things (IIoT) (Li, et al., 2017; Kang, et al., 2018; Mengelkamp, et al., 2017; Su, et al., 2019). Typically, in IIoT, energy trading is performed using one of the following strategies: (1) Microgrids, (2) Energy harvesting networks, and (3) Vehicle-to-grid networks. In microgrids, groups of smart buildings with renewable energy tools construct a grid and trade electricity among the group members in a P2P manner. In energy harvesting networks, nodes with renewable energy sources also charge each other in P2P manner. In vehicle-to-grids networks, vehicles represent mobile electricity storage devices, which can charge other vehicles or the grid itself. In such trading environments, trust and

privacy are major issues, and, in this direction, a blockchain-based secure energy trading system for IIoT was proposed. This system mainly consists of five parties: (1) energy nodes, (2) energy aggregators, (3) transaction servers, (4) wallets, and (5) smart meters. The energy nodes form the network (e.g., smart buildings and electric vehicles in the above examples). Energy aggregators work as brokers to facilitate the trade between the seller nodes and the buyer nodes. The transaction server is used to record the buying request and send them to the nearest aggregator node. Each energy node has a wallet, which stores the number of energy coins that this node owns. In each node, the smart meter is used to calculate the amount of the traded electricity (Li, et al., 2017).

In this system, each energy node determines its role (seller/buyer) based on its energy level. Once a node decides to buy energy, it sends the buying request to the transaction server. Then, the aggregator node determines the current trading price based on the market status. These buying requests are then broadcast to the sellers. The sellers respond by stating the amount of energy that they are willing to sell. At this stage, the aggregator node matches the buyers with the sellers, and electricity is transferred from the seller to the buyer. For each trade, based on the decided price, the buyer sends the required energy coins to the seller's wallet. Periodically, based on the actual number of transactions, the aggregators propose blocks to be written into the blockchain. This system is proposed to establish an efficient energy trading platform. In this proposal, the solution is designed to use a consortium blockchain. In energy trading, the anonymity of the traders' identity depends on the application scenario. Thus, based on the application requirement, energy trading solutions could use private or public blockchain. In this direction, the adoption of private

or consortium blockchain solutions increases the scalability compared to a public blockchain.

To address the problem of determining the trading price, Mengelkamp et al. proposed a conceptual auction-based approach that targets energy trading between smart buildings. To ensure the privacy and integrity of the trades' transactions, the authors employed the blockchain technology to ensure the traceability and privacy of the transactions. To address the trading scenario, the authors employed a bidding mechanism to determine the trading price (Mengelkamp, et al., 2017). Accordingly, this work presented an analytical study to investigate market behavior. Liu et al. focused on the problem of minimizing the fluctuation levels in the grid. Accordingly, they proposed a blockchain-based algorithmic approach to improve the overall charging and discharging strategies. To test their approach, the authors deployed their solution on a public blockchain (Ethereum), where the results showed that the proposed solution could minimize the power fluctuation level (Liu, et al., 2018).

Similar to any other trading platform, data integrity (security) and privacy are major challenges in energy trading. Thus, several proposals have also investigated the optimization of the security mechanisms in this trading domain (Aitzhan & Svetinovic, 2018; Laszka, et al., 2018). In situations where an identification process is applied to identify the energy nodes before commencing the trade, the actual trading process will be done in a relatively semi-private manner, which reduces the security challenge because all parties are known as a priori. Additionally, in such trading domain, employing a fairness

mechanism by exploring the traceability feature of the blockchain technology is expected to improve the stability of the system.

In energy trading domain, regardless of the employed trading strategy, the presence of the energy supply nodes can control the overall hierarchy of the solution architecture. Eventually, the energy buyer has to be physically connected to the energy source. Thus, for any energy trading platform, we can divide the entire targeted network into zones and assign traders to their nearest zone. Combining this with the fact that in this trading domain, the anonymity of the traders' identity is application-driven highlight the demand of increasing the scalability. Thus, the use of blockchain technology is expected to advance the development of this domain, since anonymity and data integrity using traditional centralized or distributed technologies is not a straightforward task.

2.5. E-commerce

Similar to energy trading, e-commerce trade involves typically three parties: the seller, the buyer, and the trading platform. In this type of trade, the platform aims to ensure that the trading agreements' conditions are satisfied, where the agreements' validation process in e-commerce trading is more advanced than the validation process in energy trading platforms. This is because the energy trading platform deals with one type of commodity (electricity), whereas in e-commerce platforms, any good can be traded. E-commerce trading can be categorized mainly into the following (Gupta, 2014): (1) Business-to-Consumer (B2C), (2) Consumer-to-Consumer (C2C), (3) Business-to-Business (B2B), and (4) Business-to-Government (B2G). Compared to B2C and C2C, the number of trades on a daily basis is expected to be relatively smaller in B2G and B2B. In addition, in B2G and

B2B, the identity of the traders is expected to be confirmed before commencing the trades. This is established, as in these trading scenarios, the seller company (business) typically provides the company (or government department) that acts as a buyer with credential information (user-name and password) to its platform.

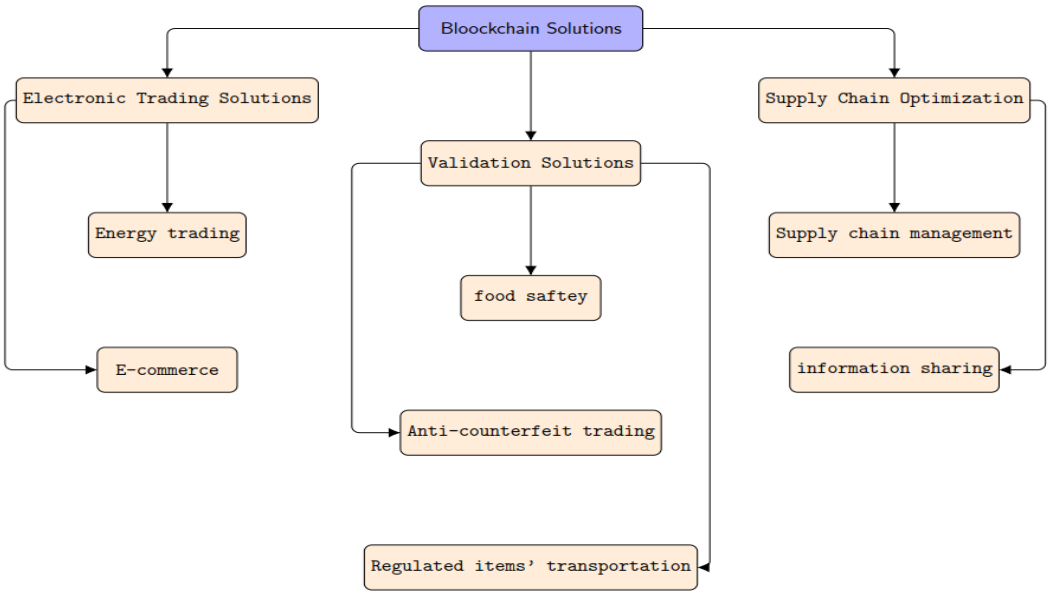

Figure 2-1 Classification for Blockchain Solution in the Trading Domain

In contrast, in B2C and C2C, there is no actual precise mechanism to identify the traders, and, typically, any public user should be able to access the trading platform. Therefore, in B2C and C2C, scalability and privacy are a fundamental challenge. In B2B and B2G trading domains, the focus is typically on optimizing the trading process to improve the trading experience. Usually, blockchain-based e-commerce solutions consist of three types of participants: verifier, participant, and supervisor (Li & Wang, 2018). A verifier is responsible for ensuring the correctness of the transactions before they are written on the

blockchain. A participant represents the sellers and buyers. A supervisor is a trusted third-party node that ensures that the trade conditions are satisfied.

Pittl et al. presented a trading platform termed as Bazaar-Blockchain, which is an improved version of Bazaar-Extension (Pittl, et al., 2016; Pittl, et al., 2018). This trading platform can be recognized as an e-commerce platform designed for cloud environments, and it allows the customer and the cloud service provider to negotiate the price and the terms of deals. Generally, the status of an offer between the customer and the cloud service provider can be advisory, solicited, accepted, or rejected (Hung, et al., 2004). Offers that are flagged as advisory require further negotiation, and solicited offers are fully specified. Acceptable offers become binding after both parties sign their agreements. Using blockchain technology, Bazaar-Blockchain is implemented as an extension of the CloudSim simulator. Bazaar-Blockchain aims to increase the scalability and the data integrity of the negotiation process. However, in such a market, any proposed approach should address the scalability requirement, as demand and supply can vary significantly over time.

To address the privacy concerns in e-commerce trading, Min et al. proposed the Peer Blockchain Protocol (PBP). This protocol uses several types of blocks to ensure overall system security. First, the transaction is written on peer micro-blocks. Once validated, these peer-blocks are aggregated to construct peer key-block. In any interval of time, the number of the generated peer key-blocks is significantly lower than the number of generated peer micro-blocks. The objective of this division is to reduce the bandwidth requirement, as the peer key-block contains the hash values for the peer micro-blocks. Additionally, peer key-blocks are validated before they are aggregated to construct global blocks. Having three

types of blocks that follow different types of validation strategies is expected to improve security. Due to the inherited characteristics from the blockchain technology, traceability and security concerns in the e-commerce trading platform can be easily addressed. However, in e-commerce trading system, two main issues of user identification and scalability must be addressed. In such a system, the user identification process must ensure and validate the identity of the user to ensure that all the transaction is lawful. In blockchain technology, this can be performed by using a third-party validator node. Regarding the scalability, the blockchain solutions must not include any expensive computational process, which is essential, as the expected volume of online trades is large. This volume of trade suggests that the consensuses mechanism that is employed must adopt a "light" strategy to establish an upper bound for the expected running time (Min, et al., 2016). A multi-level architecture has also been adopted by (Xie, et al., 2018) to establish a trusted blockchain-based e-commerce framework. In this framework, based on the type of performed validation, blocks are categorized into three different types: undecided, valid, and invalid. The main intention of this division is to support the storage of a massive number of transactions.

In the e-commerce trading domain, the impact of using blockchain technology depends on the challenges and the requirements for each trading category. In B2B and B2G, the identity of the traders is known and confirmed, and this reduces the pressure on the applied consensus mechanism. In such trading categories, blockchain technology can be used to optimize the trade supply chain by monitoring the trading process. In B2C and C2C, the identity of the users is not expected to be always confirmed. Accordingly, traders are

expected to have the same level of authority (privileges); thus, it is expected that such trading solutions to be implemented using a permissionless decentralized public blockchain. In addition, by using permissionless blockchain, the design must focus on the scalability and data privacy issues to reduce the pressure on the consensus mechanism. The scalability concerns highlight the importance of employing efficient, lightweight mechanisms to address privacy and data integrity issues.

2.6. Validation Solutions

This category discusses proposals that aim to automate the validation of certain trading constraints and processes of international trade supply chain. Based on the trading domain, these proposals aim to address the anti-counterfeit trading problem, the transportation of regulated items, and food safety.

2.6.1. Anti-Counterfeit Trading

Trading counterfeit goods have a significant negative, damaging impact on society and the economy. For instance, trading fake medicines not only has a dangerous outcome on people's health and, thus, on their life but also costs the economy millions of dollars (Mori, et al., 2018; Blackstone, et al., 2014). Thus, establishing an efficient mechanism for anti-counterfeit has always been a priority for the public and private sectors. To effectively address this problem, the information-sharing platform between the trade supply chain participants should guarantee the immutability, integrity, and privacy of the information. In this direction, blockchain technology has emerged as a promising technology to address this problem.

Toyoda et al. proposed a blockchain-based product ownership management system, where its primary objective is to use the traceability feature in the blockchain to avoid trading of counterfeit products. This is established by providing customers with the ability to trace the product from the manufacturing stage through the entire supply chain until it reaches them. This system comprises of two chains: (1) RFID-enabled supply chain and (2) post supply chain. The RFID-enabled supply chain connects the retailer to the manufacturer through the distributor, and the post-supply chain connects the retailer to the customer via the shops (or online sales) (Toyoda, et al., 2017).

In the RFID-enabled supply chain, which uses the Electronic Product Code (EPC), the manufacturer enrolls its unique prefix in order to identify its ownership of the products in any future transactions. Then, the manufacturer registers the EPC of each product that he owns. Once the shipment reaches the distributor, the distributor uses the product's EPC for validating the product's genuineness, following which, these products can be shipped to any shop (small retailer) while keeping their ownership and EPC information in the information flow. Once a customer chooses a specific product, the EPC of the product can be used to identify the manufacturer to the customer in order to establish the genuineness of the product. In addition, the blockchain is used to identify the seller as the owner of the product. Using the EPC with the ability to trace the ownership, we can correctly decide whether a specific product is genuine. However, as the author mentioned, this system requires an administrative node (server) that validates and performs the registration of the manufacturer and the products' EPCs. In the supply chain presented here, none of the entities (participants) in the supply chain enjoys the total trust of all other entities or

participants. Thus, a public blockchain (Ethereum) is used as a suitable environment to validate the proposed system performance. Using a public blockchain environment challenges the scalability of the presented system since strong group consensus is required to be performed. In addition, in the case of multi-ownership, all manufacturers who produce the same product must be a part of the blockchain. This creates additional pressure on the manufacturers in terms of creating the required infrastructure.

Similarly, Alzahrani et al. also investigated the problem of the trade of counterfeit goods. In this research, the authors proposed a blockchain-based solution that utilizes the benefits of Near Field Communication (NFC) in detecting and avoiding counterfeit goods. The main aim of this work is to authenticate transactions using two types of authentication mechanisms, namely, the local authentication and global authentication. The local authentication is used to ensure that the tag and the information about the products have not been altered at any stage during the trade-process. In the global authentication, the main idea is that the validator nodes trace the entire series of transactions of each shipment to make sure that the current transaction is correct and as expected. In this work, in order to validate the current block, the consensus protocol selects a subset of the nodes as validators, and by reducing the number of validators, it aims to reduce the energy consumption of the system. These two authentication mechanisms work together to validate the trade. Using simulation experiments, the authors validated the performance of the presented approach in terms of consensus latency and detection rate (Alzahrani & Bulusu, 2018). To address the problem of trading counterfeit products in the food supply chain, Baralla et al. (2018) presented an authentication blockchain-based framework that can be used by the public to

authenticate that the goods are made in, for instance, Sardinia. Other industrial initiatives to use blockchain for anti-counterfeit in food and e-commerce trades are presented in (Xiao, 2017; Seal, 2018; UCOT, 2018; Roberts, 2017).

Addressing the counterfeit goods trading problem requires commitment from all supply chain parties. This limits the practicality of using the blockchain technology, as we cannot enforce all companies that represent the supply chain participants to be part of the blockchain. Thus, any anti-counterfeit blockchain-based solution should be designed to overcome this issue. This can be established by integrating the blockchain solution with systems that can be used to authenticate the transactions' documents in an offline manner. Such systems can be based, for instance, on machine learning or deep learning methods. In this scenario, as the participants' identity are pre-determined, we expect this type of solutions to be implemented on permissioned blockchain. In addition, in such scenarios, the participants are expected to have different levels of trust. Therefore, either private or consortium blockchain is expected to be used in this type of application.

2.6.2. Food Safety

To ensure the quality of the distributed food, several measures are typically applied across the food supply chain. These steps work to monitor the surrounding environment of the goods at all stages of the supply chain. In addition, these measures typically involve several laboratory tests performed at pre-determined points in the supply chain. To increase the confidence of the employed food safety measures, techniques to ensure the uploaded information integrity and data immutability must be applied. In this direction, several proposals (Tian, 2017; Malik, et al., 2018; Cui & Idota, 2018; Hepp, et al., 2018; Kamath,

2018) have integrated these food safety methods with blockchain technology to optimize these methods.

Tian et al. presented a blockchain-based system to address the problem of food safety in the supply chain, which provides a reliable real-time traceability of the food supply chain by combining the benefits of the blockchain, the Internet of Things (IoT), and Hazard Analysis and Critical Control Points (HACCP) methods. In this system, blockchain is used to address the traceability requirement, and IoT is used to capture the required information about the shipment environment (for instance, temperature and light). The HACCP approach is a well-known method that is used to avoid hazards in the food supply chain. This method consists of several tests that must be performed at different points during the passage of the food along the supply chain. The overall objective of this system is to increase the efficiency of the HACCP through the use of the blockchain and IoT technologies (Tian, 2017).

In this work, the author presents an application scenario to describe the entire process, where the author assumes that the traded food is harvested crop plants. All the required information about the environment where these plants grew (for instance, light, and temperature) is stored in the blockchain. Any participant in the food supply chain can access this information. In addition, through the use of the IoT infrastructure, we can monitor and store important information about the warehouse environment and distribution. Regarding the performance of the presented approach, the authors did not present any technical details, and therefore the performance of the presented approach needs to be validated.

The problem of food safety has also been investigated by (Malik, et al., 2018). To address this problem, the authors proposed permissioned consortium blockchain-based framework. By using the consortium mechanism, the authors aimed to increase the trust of the customers by avoiding having a single node with high authority. This framework deals with four types of members: (1) non-participating, (2) participating, (3) governance board, and (4) validators. Non-participating members (such as customers) can only query the blockchain. Participating members are the food supply chain entities, and they are the source of transactions. The governance board members consist of several government agencies, and they are responsible for determining the read and/or write access rules for the participating members.

To increase the scalability of the network, the author adopted the sharing mechanism, where the blockchain data is divided between several shards. Using this mechanism, the task of validating the transactions is performed by several nodes simultaneously. Additionally, the network is divided into geographical zones, where a validating node processes the transactions originated inside its zone. Once they are verified, the participating members' transactions are stored in their local ledgers. To improve the privacy of the data, a transaction is not shared with other participating members, and it is only submitted to the validator nodes. A valid transaction must contain a pre-determined set of fields and must satisfy the rules determined by the governance board. For each shard (local ledger), a set of predetermined validators are identified, where, in each validation round, one of these validators will be selected to process the current block under consideration. Local ledgers are duplicated and continuously submitted to the global

validator to update the product ledger, which is accessible by customers using query manager.

Cui et al. presented a case study analysis, where Dentsu's blockchain-based system was used in Japan for the sale of organic vegetables. In this experiment, each vegetable was equipped with a chip that carried the required information about the status of the vegetable. The recorded information was used to generate information for vegetable batches. This information was uploaded to the blockchain. During the production life-cycle, the results of the performed laboratory tests on the vegetables were uploaded to the blockchain. In addition, IoT devices were used to monitor the storage and distribution environment, and the information recorded by these devices was periodically uploaded to the blockchain. In this study, an e-commerce trading platform was used to facilitate trades, where the actual trading was also stored in the blockchain. Customers were provided with an application to inquire about the historical data of the vegetables. In this work, the authors did not provide enough information about the implementation details. However, giving the inquiring capability to customers suggests that the entire solution must be implemented on a public blockchain (Cui & Idota, 2018).

Similarly, Kamath et al. described the blockchain system solution proposed by Walmart Inc. to trace the production of food. Tracing the production of mangoes from trees to shelf is one of the pilot studies performed by Walmart. In this study, blockchain technology combined with IoT devices was used to provide the customers with the ability to trace the production and transportation of the traded mangoes (Kamath, 2018).

Along the same lines, Hua et al. proposed a blockchain-based conceptual framework for the agriculture domain. This framework discussed the benefits of blockchain technology and how it can be applied in agriculture to increase the trust level between the customers and the distributors. This framework consists of three types of activates: (1) registration, (2) verification, and (3) tracing. The administrative node performs the registration of the participating entities. Smart Contracts handles the verification of the uploaded data. Tracing is usually performed by the end-user to trace the historical information of the goods. This work achieves its objective of highlighting the advantages of adopting the blockchain technology in the agriculture domain (Hua, et al., 2018). However, this work did not address the technical requirements to implement the proposed framework. In (Kumar & Iyengar, 2017), a similar conceptual framework has been presented for the rice supply chain. A study presented a quantitative analysis approach to clarify the importance of employing a blockchain-based technological solution for the coffee supply chain in Burundi (Thiruchelvam, et al., 2018). A case study that explores the benefits of employing a blockchain solution in the agriculture domain is also presented by. (Casado-Vara, et al., 2018).

Westerkamp et al. proposed a blockchain solution to trace the origin of the raw material used in the production of goods. This system uses recipe-based architecture, where raw materials are represented as tokens, and during the manufacturing process, the token of the final product is constructed based on the input tokens (consumed materials). Such traceability mechanism highlights the presented system as a suitable approach to add the food safety problem. By using this strategy, the authors aimed to trace the final product

and the raw materials. In this system, smart contracts handle mainly three types of tasks: (1) tokenization, (2) recipes, and (3) certified goods. Regarding tokenization, a single, smart contract is responsible for creating and maintaining the token for each type of goods. Other types of smart contracts (recipes) handle the transformation of the raw material to the final product, where the token for this product is determined. During the manufacture of products, certain materials could be used to replace others, and the certified goods contract is responsible for identifying the equality relationship. In the evaluation section of this work, one of the highlighted factors is the benefit of relying on events to transform information in terms of cost compared to storing all of the information in a smart contract (Westerkamp, et al., 2018).

Food safety trading is typically highly regulated and monitored by several government organizations. Thus, we expect such a process to benefits from adopting blockchain technology as a secure information hosting platform. In addition, the demand for monitoring the environments and the goods highlights the requirement of integrating the application with other types of technologies such as IoT. The information accessible by public users can be deployed on the public blockchain. In these proposals, the end-users (public user) have only query access privileges, and only the trade supply chain participants have the privilege of uploading information to the blockchain, where these settings of smart contracts are used to validate the uploaded information.

2.6.3. Regulated Items' Transportation

In this category, we focus on proposals that mainly use blockchain technology to fulfil the trade and transportation agreements, which are typically implemented as smart contracts.

Furthermore, trading restricted items such as pharmaceutical goods are highly regulated (Kumar & Jha, 2016). Bocek et al. Another study proposed a traceability system termed Modum.io for pharmaceutical supply chain, which combines the benefits of IoT and blockchain. In this system, sensors (IoT) are used to monitor the temperature of each parcel during the shipment, and this is used to ensure the satisfaction of the government regulations. The architecture of this system consists of the back-end, front-end, and IoT sensor devices. The back-end consists of the blockchain (Ethereum network) and a server node, where this server is responsible for monitoring the blockchain and the deployment of the smart contracts (Bocek, et al., 2017).

Furthermore, any sensitive data can also be stored on this server. The front-end consists of Android clients (phones) that communicate with the server in the back-end. Using these clients, the user can register a new shipment and specify the regulations that these shipments must satisfy. In addition to phones, the back-end server can be accessed via the website to initiate the shipment. IoT sensors are carefully placed inside the package to record the temperature. Clients access the sensors to initialize and end the monitoring process.

To initiate the monitoring process, the sensor node has to be placed within the Bluetooth communication range of the Android phone. Then, the user has to associate the tracking number of the package with the MAC address of the selected sensors. Once this association is established, the tracking number of the package and the associated MAC address for the sensors are stored in the back-end server. Then, the client initiates the temperature monitoring process, where the sensors that are placed inside the packages start the

periodical temperature recording process. After receiving the shipment, the client uses the tracking number of the package to request the MAC address of sensors from the server. The client then connects to the sensor to download the temperature readings. To test the performance of the presented system, the authors have run a pilot project lasting nearly one month with a pharmaceutical company, where 52 shipments have been successfully tracked using the proposed system.

Tseng et al. proposed a blockchain-based conceptual model for the drug supply chain, where they discussed the benefits of employing this technology to monitor the shipment and distribution of the drugs (Tseng, et al., 2018). Imeri et al. applied a relatively similar concept to address the problem of transporting dangerous goods. They presented a conceptual framework that aims to provide the required traceability information for the participating entities. These entities are the goods provider, transport operator, regulatory authority, customers, and emergency institutions. In this framework, smart contracts are used to define the path of the shipment and to notify certain entities whenever a specific event occurs (Imeri & Khadraoui, 2018). Additionally, the authors claimed that all participating entities are equal, and no administrative node is required. However, the process to achieve this equality assumption must be clearly stated.

A real-world blockchain traceability system termed OriginChain is presented in (Tseng, et al., 2018; Xu, et al., 2019). OriginChain aims to automate the process of ensuring that the shipment satisfies the regulations and rules. This system deals with three types of users: (1) service user, (2) traceability providers, and (3) blockchain administrator. Examples of service users are retailer, consumer, and supplier. Traceability provider represents a

company that provides several types of traceability services such as product examination, loading monitoring, lab tests, and yard examination. Blockchain administrator generates and deploys smart contracts that capture the traceability requirements. In this system, the process starts with the supplier submitting a registration application to the traceability provider, which validates the application and registers the supplier company. Then, to start the traceability service for a specific trade, the supplier must provide all the paperwork such as invoices, trade agreements, and contracts. Once the traceability provider validates these documents, the supplier and traceability provider have to sign a legal agreement that specifies the services that must be used (lab tests, yard inspection, etc.). The service starts once the supplier calls the factory contract from the web application. This contract creates service, registry, and data contracts. Service contract shows the traceability services that must be employed, and the legal information of the agreement is captured in the registry contract. Data contract deals with data storing and accessing. Information is stored either on-chain or off-chain. Information required for traceability is stored on-chain, and raw information (certificate files) is stored off-chain. OriginChain is implemented using the Ethereum blockchain.

Similar to any other crucial natural resource, sand trading follows government regulations, which ensure that the local trading budget is not exceeded and any illegal mining activities are detected. In this direction, Pour et al. presented a framework to regulate sand trading. The framework presented by the authors authenticate all of the mining activities and use the available information to analyses if a new mining request should be approved based on the available budget (Pour, et al., 2018).

Mao et al. presented a blockchain-based trading system for the food supply domain. Accordingly, they presented a dynamic programming algorithmic approach that aims to establish a match between sellers and buyers that optimize their trading returns (Mao, et al., 2019).

Based on the addressed scenario, private or public blockchains can be used to optimize the monitoring component in this application domain. If a public blockchain is used, a suitable credential scheme must be implemented, since the source of information on the blockchain must be clearly identified.

2.7. Supply Chain Optimization

In this category, we take a close look at the proposals that optimize parts of the supply chain components. The proposals discussed in this section can be divided into supply chain management and information-sharing proposals. Supply chain management proposals aim to provide an entire framework that facilitates the entire supply chain responsibilities. Information sharing proposals address the optimization of the communication model between the participants to simplify certain supply chain processes.

2.7.1. Supply Chain Management

Wu et al. presented multi-ledger tracking framework to simplify the process of supply chain management. This framework consists of several private sub-ledgers and a single centralized public ledger. Each sub-ledger represents a single shipment, and they can be accessed privately by the trading partners. The centralized public ledger represents the global tracking information that can be seen by public users. This framework consists of

the following components: (1) index server, (2) peer, (3) administrative node, and (4) external monitoring nodes. The index server has the addresses of all nodes that are parts of the network. Peers represent the participating entities (for example, customs authority and shipping agents). The administrative node keeps track of all activities in the network. External monitoring nodes are third-party monitoring nodes that validate and track the status of this shipment. Furthermore, these nodes post their validation results on the blockchain. All of these components submit the shipment-related transactions to either the private sub-ledgers or the public ledger (Wu, et al., 2017).

The proposed framework supports three types of events: (1) shipment initialization, (2) custody, and (3) monitoring. The administrative node starts the shipment initialization process and broadcasts the event to all involved participants. The custody event is used to identify (and change) the current owner of the transaction. The monitoring events identify the current geographical location of the shipment. In this framework, any node can propose a new block. The proposed blocks are validated using the traditional PoW consensus mechanism. By supporting the two types of ledgers, this framework aims to provide traceability for the public users and the participating entities. However, adding a public ledger may increase the load on the consensus mechanism.

Chen et al. (Chen, et al., 2017) also proposed a conceptual framework that aims to improve supply chain management by using a blockchain-based solution. In this framework, the authors proposed a system architecture that consists of several layers: (1) IoT sensors layer, (2) data layer, (3) contract layer, and (4) business layer. The idea of dividing the system architecture into four layers is to group the functionality components according to the

services that they provide. In the sensor layer, the authors proposed employing technologies that can be used to track the goods (for example, GPS and RFID). The data layer has the blockchain and the ledger, and smart contracts are executed inside this layer to ensure the quality of the data. The contract layer has the responsibility of executing some of the functionalities that can support the decisions made by the business layer, which includes the main business activities (Wu, et al., 2017).

Similarly, Meng et al. proposed a conceptual framework termed DeliveChain, which can be used to gather the required information to analyses the expected delivery performance for a given company. DeliveChain is designed to capture the status of the production and delivery in the supply chain, and this information is used to support the business decision. DeliveChain consists of five layers: (1) data input layer, (2) transaction layer, (3) smart contract layer, (4) ledger layer, and (5) business intelligence layer. The data input layer determines the acceptable data input methods by the system (GPS, staff, IoT). In the transaction layer, the data gathered by the data input layer is represented in specific pre-determined formats based on the type of the input source. The logic of the business is mainly implemented in the smart contract layer. In this layer, critical data and events are tracked to ensure the reliability of the system (Meng & Qian, 2018).

Additionally, in this layer, the obtained data from the previous layers are processed to help quantify and predict the production or delivery performance. The ledger layer stores the actual transactions. The business intelligence layer performs business analysis functionalities. Furthermore, the proposed system aims to help businesses in the process of making short-/long-term decisions.

Blockchain is an ideal tool to ensure the integrity and security of the data. In these two frameworks (Chen, et al., 2017; Meng & Qian, 2018), the authors assigned unspecified computational tasks to the smart contracts. However, the computational capability of smart contracts is limited, and this should be taken into consideration during the designing of smart contracts.

To optimize trading in agriculture domain, Leng et al. proposed blockchain solution, which employs double chain architecture. This solution is designed to establish a secure, trustworthy trading system, where enterprises aim to increase their share of the market wealth (rent-seeking). The two chains that form the architecture are termed as the user information chain and transaction chain. Information related to users' agriculture businesses or enterprises are stored in the user information chain, and all of the details of the transactions are stored in the transaction chain. Using two chains increases the privacy of the proposed solution. For instance, any member of the system can check the businesses' resource details on the user information chain without knowing the enterprises' details. The actual transactions are stored in the transaction chain using the Merkle Tree structure. To address rent-seeking, the system uses smart contracts that aim to establish the minimum total equity value among the traders (Leng, et al., 2018).

To optimize supply chain management, the proposed solutions must be application-driven. Applications have different requirements, which result in having different deployment constraints. Therefore, proposing a generic framework to improve the supply chain management reduces the optimization space.

2.7.2. Information Sharing

In the international trading domain, customs authorities' rule of protecting society by detecting smuggling and fake products is a challenging task. To fulfil this task, customs requires detailed information from businesses to monitor the flow of goods. Naturally, businesses are unwilling to share information, where the reason behind this is to avoid liability and protect confidant private information related to businesses strategies. To address this problem, Engelenburg et al. proposed a software architecture for business-to-government information sharing. They addressed these issues by proposing the designing of an information-sharing system that can be acceptable to businesses. In this direction, they highlighted the importance of maintaining the data confidentiality to avoid liability caused by sharing information as the main requirements for the businesses. These requirements are established in the proposed architecture through the use of blockchain technology. Besides the blockchain technology features of data immutability and data integrity, this architecture itself employs a context-based information sharing strategy. Using this strategy, a participating member can determine the logic of accessing certain information provided by his/her company. Therefore, if any other member would like to access this data, a request will be sent to the decision component, where it will be evaluated based on the owner's sharing strategy. In permissioned blockchain, we can pre-determine the information accessible by each member. Therefore, this architecture can be categorized as an extra level of privacy (Engelenburg, et al., 2017).

Additionally, to improve the process of international trade, Vos et al. presented DEFEND, a secure and privacy-preserving decentralized system for freight declaration. DEFEND is

a blockchain-based solution that aims to simplify and support the collaboration between the economic operators and the customs agencies. The author assumes that the participating entities in this system are: (1) the economic operators, (2) customs agencies, (3) containers, and (4) packages. A container contains several packages, and a unique identification number identifies each container. Additionally, in this system, the economic operators trust the customs agencies, whereas the customs agencies do not trust the economic operators or each other. By supporting traceability, this system aims to ensure that the customs agency is fully aware of the status of all packages inside the containers (Vos, et al., 2018).

The process flow of this system starts when the economic operator submits the container, and the package claims to the blockchain. These claims contain information about the shipment and the path that it will follow. Then, the customs agent in the operator country runs the validation protocol to make sure that participating entities are authorised. In this system, the customs authorities have the right to add new operators to the blockchain. Additionally, they can also remove operators if they misbehave. This system addresses the relationship between economic operators and customs authorities. However, this relationship does not capture the main concept of international trade. In most situations, the customs authority may ask other government authorities to process the shipment. For instance, if the shipment contains food, the health department might be involved to test the safety of the food.

Adopting blockchain technology is expected to have a significant impact on optimizing the information-sharing component in the international trade supply chain. Using such a secure platform, the participants must be able to identify and authenticate the source of

information. Additionally, using blockchain-based information-sharing mechanism, participants can control the type of information that they are willing to share with other participants, and this significantly helps them in protecting their business strategies.

2.8. Findings and Discussion

Table 2-1 summarizes the proposals that have been investigated in this work in terms of the following features: validation platform, application domain, type, authority distribution, integrated technologies, and accessibility. In this section, the discussion aims to clarify the factors behind the selection of each design criterion. This discussion contributes towards answering the second research question (RQ2), which states "What kind of factors influence the adoption of the blockchain technology in the international trade supply chain?" We conclude this section by discussing the practicality of using blockchain technology from a customs perspective, and this helps in answering the third research question (RQ3), which states "Can we improve the customs administration control of international trade through the use of blockchain technology?"

2.8.1. Type of Blockchain (public/private/ consortium) (RQ2)

The type of employed blockchain in the trading domain depends on the targeted business processes and the trade market. Business processes (services) can be divided based on their visibility to the public customers into front-end and back-end. Normally, customers interact with front-end processes, where back-end processes are internal processes (not visible to customers) that support the front-end processes.

In local trade, where the objective is to establish and regulate the trading market, it is more likely to use a public blockchain, as any user should be able to access the trading platforms without any restriction. Blockchain solutions for only the supportive processes can be deployed on a private blockchain, as the public customers are not part of these processes. A private blockchain can also be suitable for the local trading environment when the targeted market is restricted in nature and pre-authorisation is required. For instance, trading restricted items that require special permeate is more likely to occur in private blockchain. A consortium blockchain is suitable when one of the traders (or both) are several personals. For instance, when a government department is part of the trade, it is expected that several pre-determined employees have to agree on the trading conditions. Additionally, these points also apply to international trade. For instance, solutions that propose using blockchain to increase the customer visibility of the trade flow is expected to use public blockchain (e.g., (Malik, et al., 2018; Kamath, 2018)). However, if the solution is proposed to implement critical business processes such as issuing banks letter of credit (Guo & Liang, 2016) (back-end processes), we expect that the deployment will occur on a private blockchain. In international trade, consortium blockchain is expected to be used when several participants have to validate the trade transaction.

From the customs perspective, the trading activities are performed between a pre-determined set of participants among whom a level of trust already exists. Thus, to ensure the practicability of the proposed system, and, as, in most scenarios, the data is not accessible to the public customers, the system is more likely to be deployed in private blockchain. Consortium blockchain can be used for application scenarios that require the

validation of several government entities. For instance, if permits authorities such as health administration and department of defense are integrated with the application architecture, it is more likely to use consortium blockchain to make sure that restricted items obtain the appropriate permits. Public blockchain can be used to host general descriptive information for public users. Compared to the public blockchain, using private blockchain (and consortium blockchain) reduces the pressure on the employed security mechanism because the network participants are pre-determined. Thus, using this type of blockchain in the design of the system has the advantage of simpler security requirements. In addition, in such a trading solution, certain participants (customs authority) are expected to play an administrative role to regulate the trade. Having such an administrative node that monitors the participants' activities helps in securing the trading process.

2.8.1.1. Application Domain Integrated Technology (RQ2)

In situations where the application scenario requires combining the benefits of blockchain technology with other technologies such as IoT, the solution architecture becomes vital in determining the overall performance. In this solution, we expect most of the processing to occur outside the blockchain, as the computational power of smart contract is limited (Muzammal, et al., 2019). Hosting the computational functionalities outside the blockchain and the interaction with these functionalities should be carefully planned at the designing stage to ensure the reliability of the final solution.

In customs domain, implementing the main processes that are related to the task of examining the shipment under consideration and issuing the clearance requires integration with several existing technologies. Currently, at Dubai Customs, the process of importation

and exportation uses several machine learning-based technologies to validate the documents, the calculated duties, and trace the containers. These technologies require high computation and storage capabilities, and implementing them using smart contracts is not applicable. Thus, the blockchain-based processing model must take into consideration the issues that may arise because of this integration.

2.8.1.2. Validation (RQ2)

To validate the performance of the proposed blockchain architectures, the discussed proposals have used several types of validation mechanisms such as simulation, Proof of Concept (POC), and the numerical experiments. The validation mechanism depends on the main idea of the proposal. For instance, proposals that investigate simplifying certain processes (e.g., (Engelenburg, et al., 2017; Vos, et al., 2018)) are more likely to establish a PoC using a real implementation. In this case, the selected deployment environment depends on the required accessibility strategy. For instance, the Ethereum environment is generally used for public permissionless application scenarios, and IBM Hyperledger Fabric is typically used for private permissioned application scenarios. Simulation is typically used when the objective is to validate the behavior of certain network-related components (e.g., (Xiao, 2017; Tseng, et al., 2018)). In such a scenario, quantifying the behavior of these components requires relatively a considerable number of transactions over a long period of time, and, therefore, simulating their behavior is the most efficient validation method. Proposals that present conceptual frameworks normally support their claims through logical arguments without any evaluation methods. Some of these conceptual framework proposals sound efficient; however, without proper

experimentation, their expected performance will always be unclear. Other experiment methodology, such as quantitative analysis can be used to validate the acceptance level of the proposed approach (Thiruchelvam, et al., 2018).

In customs domain, all of these validation methods are expected to be used through the process of solution development. Quantitative analysis can be used to test the user acceptance level at an early stage of development. In addition, simulating the proposed architecture behavior is expected to be performed before performing a real implementation and lunching the developed solution.

2.8.1.3. Scalability and Number of Transactions (RQ2)

Both public and private blockchains priorities security over performance. In terms of the number of transactions, public blockchains, such as Ethereum, currently support around 15 transactions per second (Etherscan, 2019; Perboli, et al., 2018), whereas private blockchains, such as Hyperledger Fabric, support around 3,500 transactions per second (Androulaki, et al., 2018; Perboli, et al., 2018). Thus, in terms of scalability, blockchain solutions that are built based on Hyperledger Fabric are expected to scale-up more efficiently compared to Ethereum-based blockchain solutions. However, private and public systems are both slow compared to Visa, that supports 25,000 transactions per second (Perboli, et al., 2018; Blocksplain, 2018).

This difference between Ethereum and Hyperledger Fabric in terms of scalability is related to the architecture that supports each of them. The Ethereum blockchain is a permissionless solution, where all nodes are identical and perform the same tasks. In Hyperledger Fabric,

on the other hand, the nodes are not equal, and tasks are distributed among the nodes, which can be mainly categorized into peers, ordering, and client nodes. Peer nodes are mainly responsible for performing the consensus mechanism. Ordering nodes make sure that all nodes that have a copy of the ledger store information in the same order. Client nodes host the end-user application and communication with the rest of the blockchain.

From the classification provided for the blockchain applications in trade, the electronic trading solutions (especially e-commerce trade) are the most likely to have scalability challenges. The number of transactions generated by solutions of this type can reach into the millions. Thus, the architecture of the proposed solutions must be designed well to ensure the continuous growth of this type of solution.

In the validation category, the solutions normally consist of two parts, the query engine part and the validation part. The validation part represents the process that must be implemented between the participants to perform the examination (validation) task. The query engine part is used by the user to check the validation results. Compared to electronic trading solutions, the number of participants in each process is relatively high. However, the number of transactions generated in these types of solutions on a daily basis is expected to be lower compared to electronic trading solutions. Although the number of participants in the supply chain of this category is higher than the electronic trading solution category, the validation solution is expected to have fewer scalability issues compared to the electronic solutions since the number of transactions is lower.

The supply chain optimization category normally targets improving the performance of a single (or multiple) processes. In information-sharing solutions, the scalability of the solutions is mainly related to the amount of data exchanged between the participants and the number of expected transactions. In these solutions, we expected to have a single node (e.g., customs administration) with a ledger that has the complete list transaction. Therefore, the number of transactions that this node must record may create a scalability issue. Regarding supply chain management solutions, the scalability of such a solution depends mainly on the targeted processes and the overall solution architecture.

2.8.1.4. Accessibility and Authority Distribution (RQ2)

Accessibility and administrative privileges are mainly associated with the type of used blockchain. Private and consortium blockchain is typically permissioned networks, as they involve a pre-defined set of participants with clear rules. In terms of authority, in private blockchain, based on the application scenario, a single participant may have administrative authority, and, therefore, such blockchain can be described as centralized in terms of authority, as the administrative participant has advanced privileges. The same concept relatively applies to the consortium blockchain. In this type of blockchain, a pre-determined approved subset of the participants performs the group consensus, where they can control the flow of information in the blockchain. Public blockchain is typically permissionless, as it is normally used for applications, where any public user should be able to access and use the network without any restriction. In public blockchain, users are expected to have the same privileges, and, therefore, public blockchain is decentralized in nature.

Centralization and decentralization are not absolute values. In a decentralized blockchain, it might be the case that certain participants are required to have higher authority, for instance, trade regulators in e-commerce platforms. However, in such an application scenario, the task of controlling and validating the ledger is not delegated to these entities. In customs domain, several of the processes that are considered critical such as the process of validating the documents and assessing the shipments. Such processes are expected to be performed in a controlled environment, where customs have a high administrative rule. Therefore, we expect these processes to be automated using centralized permissioned blockchain

2.8.1.5. Customs Administration and Blockchain (RQ3)

Overall, from customs administrative perspective, several factors influence the efficiency of automating the international trade supply chain through the use of blockchain technology. These factors can be mainly participants and their rules as well as integration with existing technologies. In international trade, the trade supply chain consists typically of a relatively high number of participants. The number of participants and their activities plays a major role in determining the overall practicality of the system. In this direction, the cost and benefits of joining the blockchain network are not the same for all participants (Perboli, et al., 2018). Therefore, we cannot assume the willingness of all participants in the international trade supply chain to be part of the proposed blockchain solution. Accordingly, we expect that the registration of some of the manufacturers, freight forwarders, or even shipping agents as active participants in the blockchain may be barred. For this purpose, the system design should allow for “skipping” the expected input from

such a non-priority participant(s). For example, if the freight forwarder for a given trade is not part of the blockchain, the shipping agent, on receiving the goods from the freight forwarder, can resume the process of interacting with the blockchain. The identity of the non-priority participants depends on the targeted process. For instance, in the importation scenario, the priority of the participants is associated with the importance of the documents that they provide for the shipment clearance process.

Additionally, at customs, typically, several systems are used to target critical processes. These systems cover several technological trends such as IoT, augmenting reality, virtual reality, and Robotic Process Automation (RPA). For instance, at Dubai Customs, we have RPA systems that are currently used to automate the process of filling the shipment declaration application and authenticating the provided information. Another example is an IoT-based system, which we are currently using in the process of scanning and monitoring the cargos. Integrating these systems with blockchain-based architecture should be carefully designed. Some of these systems require mainly online access to the information-sharing platform and based on the blockchain architecture, this might not be a straightforward task, as blockchain technology focuses on security more than performance.

Eventually, blockchain technology can be used to simplify the international trade supply chain. However, as several of these participants are actually located overseas, agreements between the countries' customs administration should be established to support the deployment of cross-border blockchain solutions.

Table 2-1 Summary of the Investigated Proposals

Proposal	Validation	Application domain	Type	Authority distribution	Integrated technologies	Accessibility
Engelenburg [7]		Importation declaration	Private	Decentralised		Permissioned
Vos [65]	Hyperledger Fabric	Freight declarations	Private	Centralised		Permissioned
Bocek [54]	Ethereum	Medical products	Public	Centralised	IoT	Permissioned
Toyoda [36]	Ethereum	Anti-counterfeit	Public	Centralised		Permissioned
Lu [6], Xu [51]	Ethereum	Product traceability	Consortium	Centralised		Permissioned
Mengelkamp [22]	Simulation	Energy trading	Public	Decentralised	IIoT	Permissionless
Li [20]	Simulation	Energy trading	Consortium	Decentralised	IIoT	Permissioned
Liu [24]	Simulation	Energy trading	Public	Decentralised	IIoT	Permissionless
Li [28]	Ethereum	Transaction privacy	Public	Decentralised		Permissionless
Pittl [29] [30]	Simulation	Cloud market negotiation	Public	Decentralised		Permissionless
Xie [33]	Simulation	E-commerce	Public	Decentralised		Permissionless
Alzahrani [37]	Simulation	Anti-counterfeit	Private	Centralised	NFC	permissioned
Tian [43]		Food safety	Private	Decentralised	IoT	Permissioned
Malik [44]	Simulation	Food supply chain	Consortium	Centralised	IoT	Permissioned
Kamath [47]	Hyperledger Fabric	Food safety	Public	Decentralised	IoT	Permissionless
Cui [45]		Food traceability	Public	Centralised	IoT	Permissionless
Hua [48]		Agriculture	Private	Decentralised		Permissioned
Kumar [49]		Rice supply chain management	Private	Decentralised		Permissioned
Thiruchelvam [50]	Quantitative analysis	Coffee supply chain trade				
Vara [51]		Supply chain management	Private	Decentralised	IoT	Permissionless
Westerkamp [52]	Ethereum	Traceability	Public	Decentralised		Permissioned
Tseng [55]	Gcoin	Drug supply chain	Public	Decentralised		Permissionless
Imeri [56]		Dangerous goods	Private	Decentralised		Permissioned
Poor [59]	Simulation	Sand trading	Public	Decentralised		Permissionless
Mao[60]	Ethereum	Food trading	Consortium	Decentralised		Permissioned
Wu [61]	Simulation	Supply chain management	Private	Decentralised		Permissioned
Chen [62]		Supply chain management				
Meng [63]						
Kaigunl [64]	Simulation	Agriculture	Public	Decentralised		Permissioned
Min [32]	Simulation	E-commerce	Public	Decentralised		Permissionless

2.9. Conclusion

Blockchain technology has the advantage of optimizing the trade supply chain by simplifying the monitoring component and ensuring the integrity of the exchanged information. The data integrity and traceability features of this technology underline the benefits of using this technology in trading highly regulated goods such as pharmaceutical goods. Such features can help in detecting counterfeit goods and monitor the transportation environment. Blockchain technology can contribute significantly to the optimization of the international trade supply chain compared to the local trade supply chain. In international trade, the number of participants is very high in contrast to the local trading scenario. Compared to the local trading domain, in international trade, a high number of rules and conditions must be applied to ensure the lawfulness of the trade. These factors highlight the significance of employing blockchain technology in the international trading domain.

The adoption of the blockchain technology in the trading domain is mainly influenced by the scalability (number of transactions), the willingness of the participants, and the cost. Blockchain technology prioritizes security over performance, and this limits the scalability of blockchain-based systems. Additionally, we cannot assume the willingness of all participants to join a blockchain-based trading solution, and this also limits the growth of employing this technology in the trading domain. Also, the cost of joining a blockchain solution in terms of infrastructure might challenge the adoption of this technology in the (international) trade supply chain.

As part of the international trade supply chain, customs administrations play an essential role in protecting the local society and economy. Accordingly, from a customs authority

perspective, the data integrity and traceability features of the blockchain technology have a significant impact on simplifying the goal of protecting the society and economy. Accordingly, joining blockchain-based information-exchanged mechanism is expected to optimize the processing model of customs authority to facilitate international trade further.

3. Chapter 3: Research Methodology

The work in this thesis aims to introduce a novel blockchain-based solution that aims to optimize the operating model at Dubai Customs for the cars exportation scenario as a use-case. This involves simplifying the processes applied in both scenarios and establishing direct tamper-proof information-sharing mechanisms between the international trade supply chain participants. Toward this end, the proposed framework consists of several components that mainly target the shipment clearance and risk assessment.

In this thesis, a blockchain-based solution with a plugin to empower the solution with risk assessment capabilities is proposed. To build this solution, a proof of concept (PoC) approach is followed using the IBM Hyperledger fabric and Python programming language. The PoC comprises two stages; building the solution architecture and integrating the online risk assessment capabilities. The evaluation of the proposed framework components involved experimenting with various parameter settings that result in the best achieved results.

3.1. Background

The trade supply chain consists of several participants, one of whom, the customs authority, naturally must have access to certain information submitted by a subset of the participants. For instance, traders have to submit the original invoices (from the manufacturer) to the customs authority in order to calculate duties. As part of the targeted processes, measurements are applied to ensure the authenticity of the submitted information by the trade supply chain participants. This is established, since to a certain extent, information

provided by the customers and other participants cannot be totally trusted. This highlights the importance of providing trusted information in the exchange mechanism between the trade supply chain participants, where the process of authenticating the submitted information is automated. In addition, the isolation between the supply chain participants in the current model results in increasing the possibility of having redundant processes and increasing the overall processing time. This emphasizes the important of establishing direct communication mechanisms between the supply chain participants, where participants can communicate with each other in a timely manner.

Several proposals have investigated the use of blockchain technologies to automate the trade supply chain. Some of these proposals focused on improving the traceability and visibility of the supply chain (Kamath, 2018; Toyoda, et al., 2017; Cui & Idota, 2018; Hua, et al., 2018) so that customers can access information related to the origin and flow of goods. Other proposals have focused on optimizing the processes related to the requirements of certain trading scenarios, such as medicine transport (Bocek, et al., 2017) and food safety (Tian, 2017). Most of these proposals have indirectly addressed sections of the customs authority's processes and tasks. For instance, an anti-counterfeit model was presented to contribute towards protecting the society and economy and this is one of the primary responsibilities of the customs authority (Toyoda, et al., 2017). Another example is the medicine monitoring platform (Bocek, et al., 2017). This platform's objective is to monitor the conditions of the environment during the entire shipping process. Such information is typically required by customs during the processing of the shipment. Although these proposals have partially helped in addressing customs-related processes,

they were not designed to optimize them, and their application to the customs domain requires significant changes to their process framework.

A proposal for structural outlines that target customs processes (Engelenburg, et al., 2017; Vos, et al., 2018). Moreover, an information-sharing framework was proposed, which aimed to establish a context-based data-sharing mechanism for the supply chain participants (Engelenburg, et al., 2017). By using this mechanism, whenever a specific participant requests access to information, they will have the ability to grant or deny this request. This framework aims to increase the confidence of the participants in sharing information. However, it can be used as a secondary privacy mechanism, as the visibility criteria of each attribute stored in the blockchain can be predetermined. A structural idea that aims to optimize the communication processes between the freight forwarder and the customs authority was demonstrated (Vos, et al., 2018). It achieves its goal of improving the information flow between these two participants. However, the critical processes, such as the ones involving the validation and authentication of the submitted documents, requires the involvement of several supply chain participants such as the shipping agent, the broker, the freight forwarder, and the manufacturer.

In this work, the proposed model aims to optimize the overall international trade supply chain processing components. This optimization is driven by the requirement to fully automate the customs authority-related processes in order to help the customs authority to achieve its goal of facilitating trade and protecting the society.

We also aim to establish an accurate risk assessment method, which utilizes the inherited features of blockchain-based information sharing mechanism to achieve its goals. The proposed method consists of two steps of assessments, (1) decentralized and (2) centralized risk assessment steps. The decentralized step classifies shipments to safe, risky, and undecidable. The undecidable shipments are re-classified using the centralized risk assessment step at the customs administration using the Random Forest Classifier. In the proposed method, shipments declaration information is represented as points in multi-dimensional spaces. The Local Outlier Factor (LOF) is a density-based method that relies on nearest neighbor's search (Gan & Zhou, 2018). It is an unsupervised anomaly detection method which computes the local density deviation of a given data point with respect to its neighbors. Once each risk assessment is performed, the result of this assessment is submitted to the customs administration via the blockchain system. Such a strategy provides the customs administration with real-time assessment of shipment during the international trade supply chain stages. The outlier factor values must be taken into consideration to determine the riskiness factors of the shipments and indicate cases of fraud.

3.2. Conceptual Framework

The architecture of the proposed novel model ensures the ease of adding and modifying any functionalities. This can be achieved by virtually dividing the presented model into layers, in such a way that each layer contains functionalities that share some similarity in terms of its objective. Thus, any component can be rewritten without a major effect on the overall architecture. The presented model consists of four layers: (1) the ledger layer, (2)

the smart contracts layer, (3) the verification layer, and (4) the interaction layer. Figure 3-1 shows the architecture of the presented conceptual framework. The last three layers interact with an external server, which store the original documents submitted by the supply chain participants. Additionally, the external server is used to host the computationally expensive functionalities and risk assessment components. This is done due to the processing limitations of the smart contracts (Muzammal, et al., 2019), and, therefore, all the algorithmic components that require extensive computations are located outside the blockchain. Each of the presented layers consists of several processes, where the processes of a single layer interact only with the layers located directly below and above this layer.

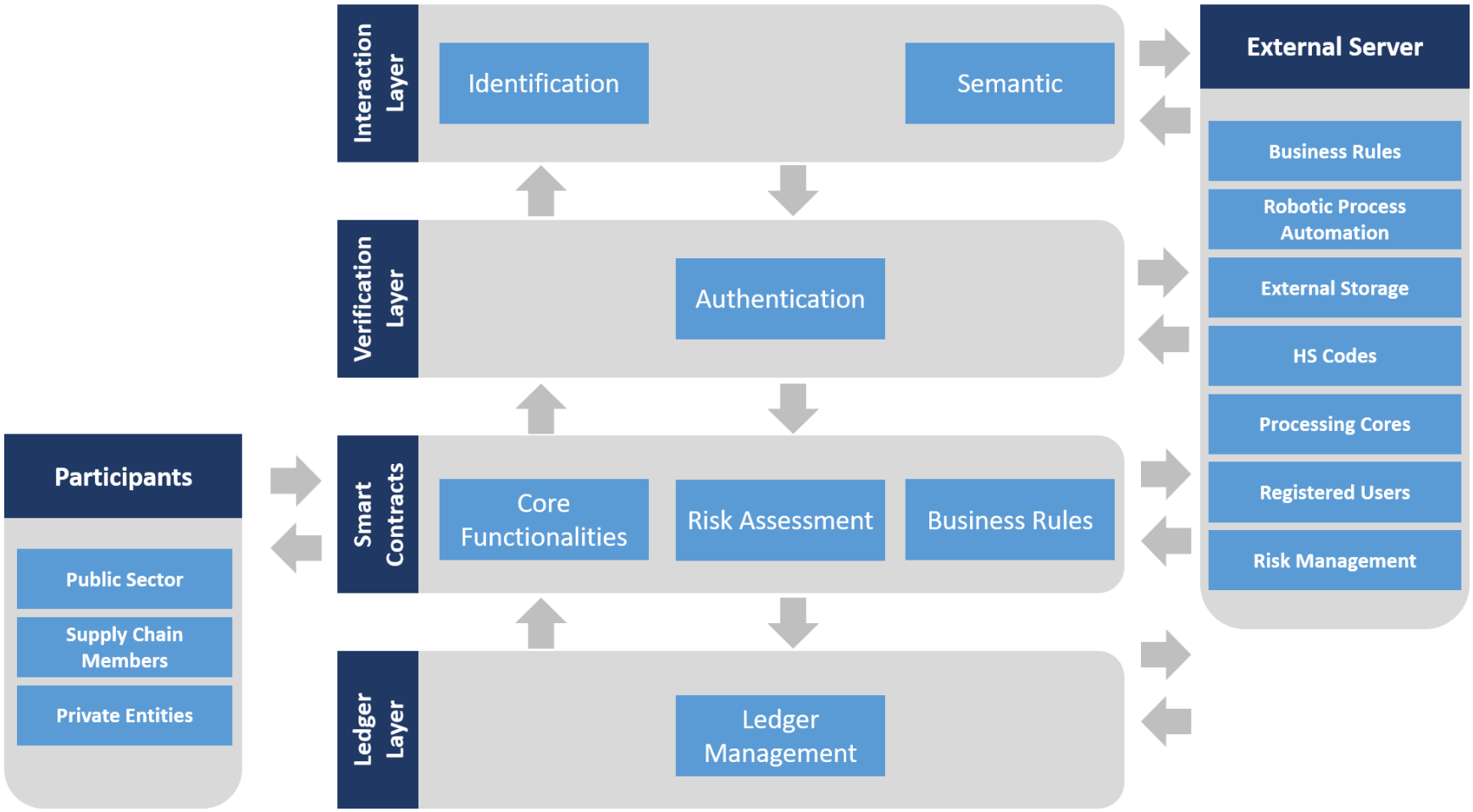

Figure 3-1 Conceptual Framework

At the customs authority, the processes of the interaction layer are triggered once a transaction is submitted by any trade supply chain participant to the blockchain. This layer contains the processes that define the mechanism of interaction between the supply chain participants and the model. In this layer, processes that confirm the identity of the participants are implemented to make sure that only the registered user can access the platform. In addition, in this layer, a semantic process is also implemented to define the type of information expected from each participant in the trade supply chain. The registered users' data are stored on the external server, and therefore the identification process implemented in this layer accesses the external server to confirm the users' identity.

The verification layer hosts several processes that authenticate the information provided by the participants. For instance, in this layer, we confirm and authenticate the correctness of the submitted Harmonized System (HS) code for the type of goods included in the shipment under consideration. Each traded item in the market has a worldwide predefined HS code, which is used during the process of calculating duties. In addition, the HS code for a given item defines the procedure that the customs authority must follow to process this item. For instance, certain HS codes directly indicate that a special permit from the health ministry must also be submitted by the trader. In the presented model, the HS code table is hosted on the external server. In situations where the functionalities of this layer determine that the information provided by the customer is false, the Customs Declaration Management (CDM) Department is informed to take the necessary actions. For instance, if the participant has provided fraudulent information, the Police Department will be informed. Additionally, CDM is also informed if physical inspection of the shipment is needed before issuing the clearance.

The smart contracts layer contains the core functionalities, the risk-assessment functionalities and the administrative business rules. The sources of these business rules are typically several government authorities, and it is mainly motivated by political and economic factors. For instance, the government could restrict the importation of certain goods types to support local businesses. Additionally, for security purposes the government could ban importation from certain entities or sources. These business rules are stored in the external server, since we expect that they require relatively large storage space.

The risk-assessment functionalities handle the process of analyzing and tracking the shipment information to identify any suspicious transactions or activities. This risk assessment is typically performed at the customs agency in a centralized fashion. Normally, whenever information concerning a new shipment becomes available, it is entered into the risk-assessment engine to examine the shipment. This involves comparing the features of the shipment under consideration with the available historical data. This comparison is normally performed using a behavioral analysis model. The accuracy of this assessment depends on the provided historical data and the number of features (attributes) that can be used to describe each shipment transaction, which could reach 120, while any irregularity in shipping behaviors increases the pressure on the customs agency to perform and provide reliable services in a timely manner.

In the proposed model, to reduce the complexity of the risk-assessment component, it will be performed at different stages of the supply chain. The risk-assessment functionalities can be described as computationally expensive. Thus, they will be located on the external server. In a situation where the shipment failed to pass the risk assessment, the CDM Department will be informed to perform an inspection.

The ledger layer stores the actual ledger. However, each participant in the supply chain (except customs) only stores a subset of the transactions in its ledger. Each participant ledger contains only transactions which are either submitted to this participant or submitted from this participant. The proposed conceptual framework is designed to work in a distributed fashion along the trade supply chain. Thus, each component (functionality) will be triggered once the required input data for the component becomes available on the blockchain. Performing these processes in a distributed fashion aims to reduce the operational time and costs.

The presented model can be designated as a privately permissioned blockchain solution. In the proposed framework, we assume that all trade supply chain participants trust the customs authority. However, customs authorities do not trust the supply chain participants. Additionally, at the current stage, we do not assume that any overseas government authority is part of the blockchain, since this would require a change to government legislation. This assumption can be dropped at a later stage, if mutual agreements are signed with these countries. In terms of authority privileges, this model can be described as centralized, since the customs authority has administrative rights over the blockchain. This is an expected assumption, since the information submitted to the blockchain by the supply chain participants is typically provided to the customs authority using different communication mechanisms. Therefore, in the proposed model, the relationship between the supply chain participants represents what has been adopted in reality for centuries.

To evaluate the performance of the proposed operating model components, we are planning to perform an extensive set of experiments. These experiments will be designed to investigate the robustness, accuracy, and scalability of the presented model. The

experiments are to be performed in a simulated network environment, where the simulation tools are selected based on each experimental objective. For instance, the common open research emulator (CORE) (Ahrenholz, et al., 2008) can be used to test and evaluate the scalability and robustness of the network dependent components. Furthermore, proof of concept (PoC) will be implemented using IBM's Hyperledger Fabric, a permissioned blockchain infrastructure. The inputs for the experiments are shipment declaration information, provided by Dubai Customs, for the year 2018. This contains all the required information from the international trade supply chain participants and will be used to simulate the actual behavior of these participants.

3.3. Risk Assessment Methods

3.3.1. Data Collection

The efficiency of the presented method is evaluated using several sets of experiments. The input data used in these experiments are obtained from the service innovation department at Dubai Customs. The used data consists of two different datasets; the first one consists of 12,221 shipment declaration applications and the second one consists of the used data consists of 500,000 shipment declaration applications submitted to Dubai Customs. These applications are already labelled as either risky or safe based on the outcome of the inspection performed by the customs administration. These declaration applications consist of 0.5% risky shipments. Each shipment declaration consists of more than 120 field. However, not all of these fields are used in the designing of the methods proposed in this work. To determine the features that we will use in this work we have investigated the correlation between the declaration fields and the classification label (Safe and Risky). In this work, we have used the following shipments declaration fields:

- Value: represents the total amount of money paid by the importer to the manufacturer.
- Goods HS-code: The HS-code is used to define a unique number for each item category and by customs to calculate the amount of duties the traders are expected to pay as well as determine whether the shipped items can enter the country, with or without permits.
- Duty value: the duty value amount calculated by the custom administration for the shipped goods.
- Country of origin: the manufacturing country of the shipped goods.
- Cost, Insurance and Freight (CIF) value: this value represent the total cost of the shipment including the insurance and freight forwarder charges.
- Original port of loading,
- Shipping agent identification number and last port of loading in the shipping route.

Table 3-1 show a sample of the used fields. However, we did not show the Shipping agent identification number due to privacy constraints.

Table 3-1 Summary of used declaration fields

ValueTable 1-1 Actors and Roles	**HS-Code**	**Duty**	**Country of origin**	**CIS**	**Original port**	**Last port**
9500	57024210	1827.666	TR	36553.31	41224	41224
18512.09	87087000	3452.44	CN	69048.8	91535	91535
24703	87087000	4561.409	CN	91228.18	91535	91535
22258	87087000	4109.94	CN	82198.79	91535	91535

37524	85076000	6928.807	CN	138576.13	9400	9400

3.3.2. Data Preparation

In the presented experiments, 70% of the applications are used to represent the historical data. Whereas, the rest 30% of the applications are used for testing purposes. To capture the impact of the threshold (t) on the proposed method performance, we performed these experiments while varying the value of this threshold. The data should be split randomly to have measure the efficiency for the performance of the data model.

3.3.3. Performance Evaluation for the Algorithmic Methods

To calculate the accuracy of the presented method on the shipment level, the entire shipments must be classified to either risky, safe, or undecidable. Shipments are labelled as risky if any of the two risk assessments stages (manufacturer or shipping agent) identify the shipment as risky. A shipment is identified as undecidable if both risk assessments stages labelled the shipment as undecidable. In other cases, the shipments are classified as safe.

In addition to accuracy, the used performance metrics in these experiments are precision, recall, and F1-score. If the attention is on the risky classification results. Precision is defined as the percentage of correctly classified risky shipments, and it is calculated as follows:

$$P = \frac{TP}{TP + FP}$$

Where TP (true positive) refers to the number of correctly classified risky shipments, and FP (false positive) refers to the number of safe shipments that are wrongly classified as risky shipments. As a performance metrics, precision evaluates the capabilities of the presented methods in term of capturing the distinct features of the risky shipment.

Recall is defined as the percentage of correctly identified risky shipment over the total number of risky shipments. The recall is calculated as follows:

$$R = \frac{TP}{TP + FN}$$

Where FN (false negative) represents the number of risky shipments that are not correctly classified. In line with precision, recall evaluates the capabilities of the presented methods in term of capturing the distinct features of the risky shipment. F1-score is used to determine the accuracy of the test, and it is calculated as follows:

$$F1 = 2 \times \frac{R \times P}{P + R}$$

The value of this score range from zero to one, where the best accuracy occurred when the value of this score is one. Therefore, the overall efficiency of presented methods can be represented by the value of the F1 score.

3.4. Ethical Considerations

To a certain extent, the data that we used had critical information about the trade supply chain participants. Thus, it had been processed by the Dubai Customs authority to remove the identity information of the supply chain participants. This was done to ensure the privacy of their business strategies. All the data originated from the same and associated

with a unique key to clarify their same source origins. In addition, the proposed solution was submitted to the Dubai customs authority for publication approval. This was crucial, as some of the processes contain critical business information strategies (for instance the mechanism of detecting counterfeit goods).

3.5. Conclusion

This work aims to build a blockchain-based solution with a plugin to empower the solution with risk assessment capabilities that aims to optimize the operating model at Dubai Customs. The cars exportation scenario has been selected as a use-case that aims to optimize the operating model for various importation and exportation scenarios. To build this solution, an experimental PoC approach is followed using the IBM Hyperledger fabric and Python programming language. The implementation of the PoC includes two stages. The first stage is building the solution architecture and the second stage is integrating the online risk assessment capabilities.

4. Chapter 4: Customs-based Blockchain Solution for Exportation Protection

4.1. Introduction

Customs Administrations around the globe are tasked with a major role of combating criminal cross-border activities conducted by small and large criminal networks. The main objective of these networks is illicit financial gain and fortune. One threat of particular concern comes from the sophisticated organizations responsible for the theft and export of stolen vehicles. Thousands of vehicles are stolen or carjacked across the globe in order to be illegally exported through various marine terminals located around the world heading to different destinations. The success of identifying, degrading and disrupting these criminal networks depends on many things, with document verification, analytics and risk assessment right at the top of the list. Leveraging the data pool and analytical abilities, coupled with close collaboration with partners, customs has a higher chance of dismantling these networks.

By operating in a data-driven collaborative fashion, participants will be able to confirm the integrity of the documents exchanged throughout the cross-border transactions. Ensuring data immutability is essential and must be guaranteed. Traditional approaches to fulfil these requirements were difficult and costly tasks. Getting the right data to concerned authorities using traditional means will create a connectivity maze and raise new challenges to the different authorities. A more Complex algorithms-based must be applied to ensure that each participant has the latest version of the data, and no participant can actually manipulate the shared information. With advances in technology, this task is more feasible

and achievable granted certain standards and rules are put in place. With solutions like this in action the mission of customs to safeguard borders is within reach. Thereby protecting the public from criminals and materials while enhancing economic competitiveness by enabling legitimate trade and travel.

4.2. Related Work

The inherited features of the blockchain technology have underlined its potential to optimize several application domains such as health (Jiang, et al., 2018), agriculture (Hua, et al., 2018), and trade (Casado-Vara, et al., 2018). Blockchain is known for ensuring data immutability and integrity, where these characteristics result in increasing the trust among the participants in any application scenario. This revolutionizes the way we address traditional problems such as food safety, trade traceability, and information exchange. In (Tian, 2017; Kamath, 2018; Cui & Idota, 2018; Hepp, et al., 2018), the authors proposed blockchain-based solutions to address the problem of food safety in the food supply chain. Using these solutions, users can gain access to the required information to authenticate food quality and storage environment. For instance, to support the concept of trees to shelf information visibility, Walmart Inc. solution publishes all the information gathered during the production of food to a public blockchain. Food safety solutions typically involve the use of IoT sensor devices to monitor the surrounding environment of foods, where the collected sensor data and any lab test performed are uploaded to the blockchain (Kamath, 2018).

To ensure the quality of the available pharmaceutical goods, the authors proposed blockchain-based solution to trace the status of goods storage environment along the pharmaceutical supply chain. This proposal employs IoT devices to monitor the status of

pharmaceutical goods (Bocek, et al., 2017). In a relatively similar concept has been applied to trace and monitor the transportation of dangerous goods (Imeri & Khadraoui, 2018). In other researches, the authors presented a traceability solution termed OriginChain, which aims to increase the transparency of the trading process and to ensure that the shipped goods satisfy the trade regulations and rules. Three types of parties interact in this solution: service user, traceability provider, and blockchain administrator. Service users represent companies and retailers. Traceability provider is responsible for performing the test requested by the service user. Blockchain administrator generate smart contracts, which will implement the responsibilities of traceability providers (Lu & Xu, 2017; Xu, et al., 2019).

An industrial platform termed TRACER is presented as a traceability solution to authenticate the diamond ownership information (Tracr, 2019). This platform aims to increase trade confidence by ensuring the integrity, traceability, and immutability of the trade transaction. A similar concept has also been adopted by the TrustChain platform (Trust Chain, 2019). Additionally, several other proposals have investigated the use of the blockchain in the context of anti-counterfeiting measures. A study proposed a blockchain-based solution, which uses the traceability feature of the blockchain technology to detect fake products. In this solution, starting from the manufacturer, all the participants in the trade supply chain have to be registered users on the blockchain. In this direction, once a participant uploads information to the blockchain, this participant has to digitally sign the information using his/her public/private keys. Therefore, the end-user can authenticate the origin of the goods, since the source of each transaction on the blockchain can be determined easily (Toyoda, et al., 2017).

Several proposals have also investigated the use of blockchain technology to simplify the Customs Authority processing model. In another research, the researchers presented a context-aware information sharing solution, in which each of the participants can control the visibility of information on the blockchain. In this solution, whenever a participant requests access to specific information, the participant who owns this information can accept or deny this request. This strategy aims to increase the participants' confidence in sharing the information (Engelenburg, et al., 2017). Vos et al. presented a blockchain-based decentralized system for freight declaration. This system aims to simplify and automate the collaboration between the economic operators and the Customs agencies. By digitizing the shipment containers through the use of IoT technology, this system aims to increase the awareness of the Customs Authority about the shipped goods and their shipping path. These two systems target the international trading scenario, where participants are located both inside and outside the country. The applicability of such solutions is restricted, since the willingness of the participants to join the network is a major issue (Vos, et al., 2018).

In this chapter, we propose a solution that has wide economic impact across the globe in which multiple parties covering different industries can potentially suffer consequences of malicious activities involving cross-border trade. The same solution can present much needed opportunities in reducing operations risks and challenges. This will become more evident as part of this chapter in which we uncover the impact of illegal export of vehicles by non-owners which amounts to an aggregated multi-billion dollars annually across the globe (UNODC, 2018). The proposed solution spans various businesses and organizations such as loaning banks, car rental agencies, insurance companies, police, road and transport authorities, Interpol and customs authorities all of which may be impacted by the addressed

use-case. Thus, we aim to resolve the global problem by adopting blockchain technology to determine whether vehicles crossing borders are considered legitimate or not at the origin country.

4.3. The Export Cars Blockchain System

The Export Cars Blockchain (CarChain) system aims to establish a communication mechanism among the participants, such that the privacy and integrity of the data are guaranteed. Participants that use the CarChain system are (1) banks, (2) car rental companies, (3) Dubai Police Department, (4) Road and Transportation Authority (RTA), and (5) Dubai Customs. Generally, building a typical distributed system that connects these participants is impractical, since such system is expected to raise several significant privacy and security concerns. Blockchain has emerged as a suitable technology for establishing such system, since using this technology, we can ensure the privacy of the information exchanged.

4.3.1. Overview

In this system, only three participants are expected to have complete visibility of the information stored in the ledger, viz., Dubai Customs, Dubai Police Department, and RTA. By nature, these participants are expected to use the stored historical information in the ledger for their internal processes only. They are also expected to maintain the ledger and create the consensus. Regarding the other two types of participants (banks and car rental companies), each of them can access only its own information on the ledger.

In the CarChain system, the main process starts once Dubai Customs submits an inquiry. This inquiry is represented as a smart contract, with information about the car being

exported. Accordingly, this smart contract checks the information stored in the ledger to identify whether this car is owned by a rental company or is currently charged to a bank. Additionally, this smart contract checks with the Police Department and RTA, to determine the legal and ownership status of this car. In situations where there is an active case against the car in the Police Department, or the car is rented from a car rental company, the exportation process will be stopped. This will also occur if the loan that with which the car is purchased is not repaid in full, or the car ownership information in RTA does not match the information provided in the declaration. In such a case, the customs declaration management department will be informed for investigating the exportation further.

4.3.2. Architecture and Processes

Figure 4-1 shows the required modification for the car exportation business process model notation after deploying the CarChain system. Once the declaration is validated, the process continues with invoking the CarChain system. In this step, a smart contract will be triggered to process the current inquiry. This contract will check the information stored in the ledger. In addition, it will check with RTA and the Police Department databases, through the use of external web services. The RTA and the Police Department records are kept off-chain, since they are expected to be significantly large.

If any of the participants has an issue with the exportation, the process will be stopped, and the customs declaration management will be informed. In situations of fraud, the legal authority will also be informed.

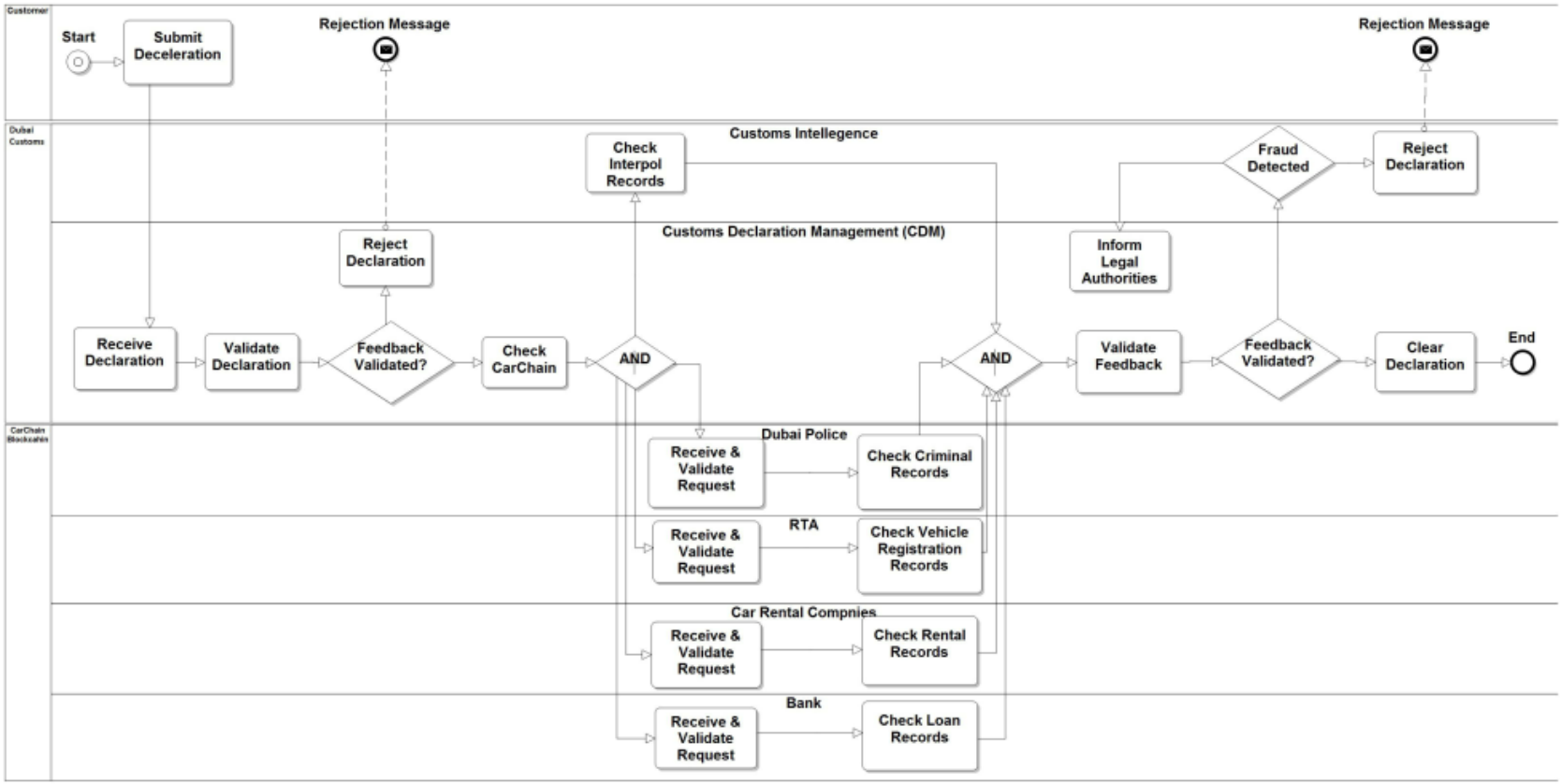

Figure 4-1 The Car Exportation Business Process (with CarChain)

This examination is performed from the perspective of each participant. Dubai Police Department checks whether there is an active case against this car. RTA validates the car ownership and the clearance information. Cars rental companies check whether they rented the car. Banks check whether the car is bought using a loan, which remains unpaid.

Fig. 8 presents the architecture of the CarChain system. This architecture is divided into three layers, viz., the interface layer, the smart contracts layer, and the ledger layer. The interface layer defines the processes that the participants can use to interact with the system. The next layer consists of several smart contracts used to store information on the ledger and to perform the inquiry process. The ledger layer represents the actual blockchain. Each participant uses functionalities related to their rule in the system. Dubai Customs performs participant registration, and this functionality deals with the process of registering banks and car rental companies. Banks and car rental companies can trigger functionalities related to loans and vehicles status. These functionalities deal with processes of updating the vehicle or loan status on the ledger. Dubai Customs typically initiates an inquiry with the objective of determining the status of the car being exported.

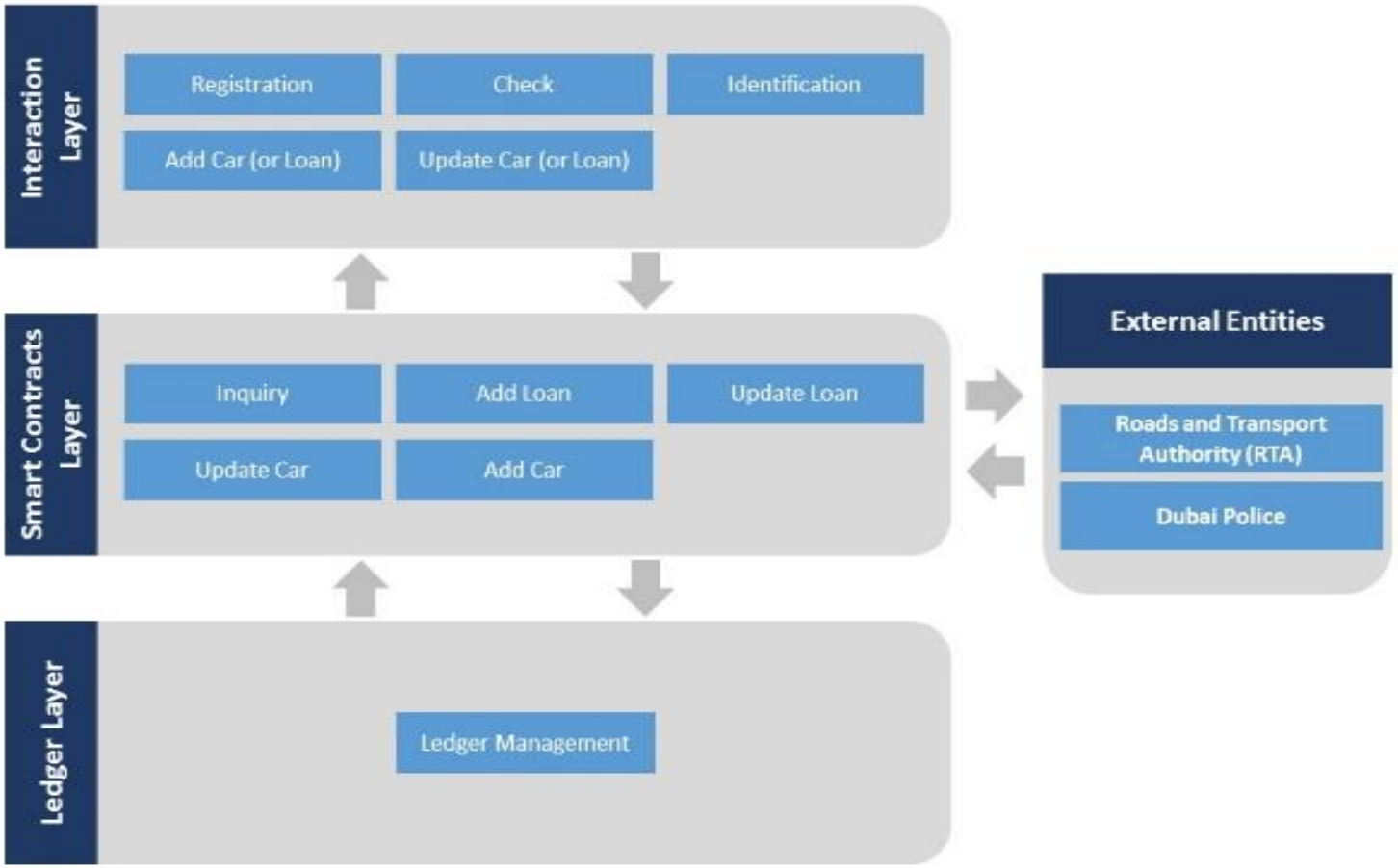

Figure 4-2 The CarChain System Architecture

4.3.3. Banks and Car Rental Companies

To interact with the CarChain system, car rental companies and banks have to be registered users. The registration is done through Dubai Customs, where each bank and car rental company is assigned a unique identification number. Each bank or car rental company has access to the ledger transactions originated by this participant. Once they register with the system, car rental companies and banks can start recording their cars and loan activities on the ledger.

The type of transaction (activity) recorded on the ledger depends on the participant type. Transactions originated by car rental companies are related to the ownership status of their cars. Accordingly, a car rental company is allowed to register a new car under its name, or change the status of any of its cars to indicate for example that the car had been sold, and is no longer part of this company's fleet of vehicles. Banks use the system to record the cars that are bought using loans. In the proposed system, once a car loan is repaid, the bank has to record a new transaction to indicate the repayment. For privacy purposes, banks do not store the car owner's name on the ledger, which records only the plate number and the chassis number.

4.3.4. Police Department and RTA

Dubai Police Department and RTA have different types of interaction with the system. These two participants use the transactions stored in the ledger for their internal processes. For instance, the Police Department can use the ledger information to track the movement of the vehicle from/to Dubai. In addition, once these two participants receive an inquiry about a car, each performs an examination based on its role in the system. RTA checks and

validate the car ownership information, and Dubai Police Department checks whether there is any active case against this car in its database.

These participants start their examination processes once they receive the car's information using the Inquiry smart contract. If RTA examination determines that the car ownership information provided with the declaration does not match its records, Dubai Customs would be informed to stop the exportation. Dubai Customs would perform the same action if Dubai Police Department records indicate the existence of a case against the car. Dubai Police Department and RTA records are stored off-chain.

```
async function Inquiry(vquery) {
1   const REG = await getAssetRegistry('org.carchain.vehicle');
2   let onLoanResults = await query('selectVehicleonloan');
3   if (onLoanResults.length > 0)
4       console.log(' Vehicle is on active loan');
5   else
6       {let onRentResults = await query('selectVehicleonrent');
7       if (onRentResults.length > 0)
8           console.log('Vehicle is on active rent');
9        else{
10          const RTA = await
            request.get({'http://RTAJUSTFORTEST/vstatus?chno=vquery.chassisnumber&eid=vquery.emiratesid
            ',JASON:true});
11          const POLICE = await
            request.get({'http://POLICETEST/vstatus?chno=vquery.chassisnumber',JASON:true});
12          if (RTA.results > 0)
13              console.log(' Vehicle is registered to correct person');
14          if (POLICE.results > 0)
15              console.log(' Vehicle has registered Police case');}}
```

Figure 4-3 Code for the inquiry smart contract

4.3.5. Dubai Customs

Dubai Customs interacts with the system mainly by starting the car inquiry process. Additionally, it is responsible for registering the banks and car rental companies. The inquiry process is established by passing the car information to the smart examination contract. This contract validates the declaration information by checking the transactions stored in the ledger, as well as by contacting the Police Department and RTA. Where fraudulent activity is detected, the legal authority is informed for handling the case.

4.4. Proof of Concept (PoC)

To validate the performance of the CarChain system, we have implemented a Proof-of-Concept (PoC) for the proposed architecture, using the IBM Hyperledger Fabric blockchain framework. Hyperledger fabric is designed for private permissioned network, where the identity of the participants and their roles in the network are known. The objective of this PoC is to test the efficiency of the proposed architecture, mainly in terms of integration. The system is designed to be eventually deployed as part of Dubai Customs operating model. Thus, it should be easily integrated with other deployed systems, without any interruption to the business processes. In this section, we describe the PoC implementation details in terms of assets, transactions, and smart contracts.

4.4.1. Assets

In blockchain terminology, assets could be anything having value, and in the CarChain system, these represent cars and loans. In this system, the ledger-stored information consists of cars bought with loans, or cars belonging to rental companies. Thus, two kinds of assets are established in the proposed system, viz., the CLoan and the RCar. CLoan assets refer to the bank loans availed for buying cars. The banks manage CLoan assets, and loans are identified by their numbers. Each loan is associated with a Boolean variable (true/false), which represents the current status of the loan. If this variable value is false, it indicates that the loan has been repaid. RCar refers to cars, which are currently owned by rental companies. The rental companies manage RCar assets, where cars are identified using their chassis numbers. Each car asset is also associated with a Boolean variable, which represents the renting status of the car. If this variable value is true, this means that the car is currently rented to a customer.

4.4.2. Transactions

Banks, Dubai Customs, and car rental companies are the only participants that submit transactions to be written in the ledger. Banks submit two kinds of transactions to the ledger, representing the initialization of a new car loan and the status update of an existing loan. The status of a loan is changed to false when the customer fully repays. Car rental companies can perform two kinds of transactions: car registration and ownership update. Car registration transaction is used to register a new car with the system, and an ownership update is used to change the ownership information for the registered car. For a car exportation declaration, Dubai Customs can submit to the ledger two types of transactions, viz., clear for exportation and involve customs management department.

4.4.3. Smart Contracts

In the CarChain system, smart contracts are responsible for managing the assets and performing the inquiry, which is triggered by Dubai Customs. Managing the assets is performed mainly through the use of four contracts, which perform the processes of registering new bank loans, updating the status of existing loans, adding a car to a rental company's fleet of vehicles, and changing the ownership information for a car that belongs to a car rental company.

The inquiry smart contract examines the ledger to obtain any available information about the car being exported and also, using web service; the smart contract contacts the RTA and Dubai Police Department to check the status of this car. This examination process can result in either clearing the exportation or blocking it. Fig. 9 presents the main components of this smart contract. This smart contract starts by checking whether the car is bought using a loan, and the whether the loan is repaid (lines 2-4). Then, the contract proceeds to

determine whether the car is rented from a rental company (lines 6-8). To examine whether the declared ownership information matches RTA records, a web server hosted by the RTA must be invoked to validate the ownership information. In this work, for testing purpose, we have created a local service for testing (line 10). In the official deployment, this triggered functionality must be a service hosted at RTA. The same process must be applied to trigger the Dubai Police department service (line 11).

4.5. Evaluation

The traditional formalities are cumbersome and lack efficiency and effectiveness. The time it takes to clear goods results in financial loss for all parties involved. The proposed blockchain-based solution contributes drastically to raising both efficiency and effectiveness throughout the whole supply chain. Additionally, it will increase the level of satisfaction for all participants. The proposed solution will eliminate the cost associated with the data sharing, integration, compliance assurance, validation and conformance to the laws and regulations. The efficiency of the proposed solution is measured by capturing the before and after situation using Activity Based Costing approach (ABC) (Innes & Falconer, 1995).

To determine whether a vehicle can be legally allowed to cross-borders, multiple parties are required to share or exchange information with each other to prevent the possibility of cross-border car theft. Traditional solutions would involve complex integration infrastructure that costs time and money. Furthermore, these parties will incur high maintenance costs. At the same time, the security of this solution is not guaranteed as each entity uses different levels and approaches of security and data may be susceptible to manipulation or hacking. The more parties and business purposes organizations try to

serve, the more complex this integration mechanism may become which may end up in spaghetti of connectivity which is difficult and costly to handle.

The end-to-end process depends on multiple parties with multiple systems which are in-large paper-based that consume time and money. Authentication of produced documents is also hard to guarantee with the traditional architecture. Therefore, the need to provide easy integration, authentication and immutability features without disruption to existing technology architecture investments is essential.

The distributed nature and immutability features available in blockchain made it feasible for organizations and businesses to deliver services end-to-end in collaborative fashion. The PoC conducted indicates how we can shift from negative economic and administrative dip to a fully positive outcome for all participating parties.

The proposed PoC resulted in substantial decrease in number of reported cases in cross-border luxury cars theft in the city of Dubai by 88.65% in 2018 according to the statistics provided by Dubai Customs. This amounted to time saving of 99% and cost saving of 69% by shifting to the proposed solution and adopting the features that come with it.

4.6. Conclusion

In this chapter, we presented a blockchain-based system called CarChain. This system is designed at Dubai Customs to simplify and automate the process of exporting luxury cars. CarChain aims to establish a direct and secure communication mechanism among the supply chain participants. By employing the blockchain technology, the proposed system ensures the integrity and immutability of the exchanged data.

This solution targeted export vehicles in one city and can be expanded nationwide and involve key international stakeholders to protect both export and import of stolen luxury vehicles. Furthermore, the proposed solution can be used to cover other commodities such as fake or stolen goods to protect and support and comply with the global intellectual property rights.

5. Chapter 5: Enhanced Customs-based Distributed Risk Assessment Method

5.1. Introduction

In general, customs administration aims to establish a trade-off between facilitating trade and protecting the public interest (World Customs Organization, 2018). Of course, both of these objectives necessarily conflict, for the increased facilitation of trade increases risks for local economies and societies. At the same time, applying strong measures to ensure the protection of public interest can reduce the ease of trade. At customs administration, the process of risk assessment is expected to serve the objective of protecting local interests by, for example, confirming the authenticity of trade documents and detecting all forms of suspicious activities. For a given shipment, risk assessment involves validating available information about the shipment to determine whether it should be cleared with or without physical inspection. Although applying such risk assessment processes can further facilitate trade, optimizing the accuracy of the risk assessments process remains a major challenge.

From the perspective of customs administration, shipment risks can be categorized into either value manipulation risks or undeclared goods risks. Value manipulation risks occurred when the trader falsified the trade documents in order to reduce the expected amount of duties. Undeclared goods risks occur when traders attempt to smuggle restricted or prohibited goods into a country. Whereas restricted goods such as pharmaceutical items and weapons require special permits from government authorities to enter the country. Prohibited goods represent all products not allowed to enter the country under any

circumstances. The impact of shipment-related risks on local societies and economies underscore the importance of the protections provided by the customs administration.

To realize the objective of protection, customs administration offices perform risk assessments during not only the importation but also the exportation of goods. In both scenarios, however, risk assessment entails roughly the same steps to ensure the lawfulness of the trades involved. Typically, risk assessment is performed in a centralized fashion at the customs administration, where information provided on import and export declaration applications are analyzed for risk factors related to the shipments being assessed.

Once the employed risk assessment process identifies a shipment as being risky, if the risk relates to suspected smuggling activity, then a customs inspection agent is expected to perform a physical inspection to determine the riskiness of the shipment. Based on the shipment volume, that inspection could take hours to perform, especially in the case of sea channel shipments. Customs administration starts processing a shipment once it receives the declaration application from the trader, although that submission may occur only once the shipment physically reaches the local port. If so, then customs administration has a limited window of time to analyses and inspect the shipments, since the overall processing time for any shipment is bound by a predetermined time constraint to ensure the ease of trade. All of these factors must be taken into consideration during the design of customs-based risk assessments solution.

In this chapter, to boost the efficiency of risk assessments performed by customs administration, we propose a lightweight distributed risk assessment method. The objective of the method is to provide customs administrations with real-time feedback about risk

assessments at different stages in the international trade supply chain. The proposed method is designed as a secondary-level assessment that complements existing risk assessments processes performed by customs administrations. By using the method, customs administrations can have significantly more time to investigate shipments labelled as risky.

The main idea of the proposed distributed method is to perform risk assessments for shipments at two stages of the international trade supply chain—at the manufacturer and at the shipping agent—both of which can allow the capture of value manipulation risks and undeclared goods risks. Risks related to value manipulation can be assessed by analyzing the manufacturer's information (e.g. invoice and country of origin), while undeclared goods risks can be assessed using information related to the shipment's path and type. For each type of risk assessment, the proposed method represents the shipment's information as points in multi-dimensional space consisting of two kinds of subspace: safe and risky. Risky subspace encompasses shipments whose risks have been identified and confirmed, whereas safe subspace encompasses ones without any identified risks. The dimensions of each space represent the parameters used to analyses the type of risk. For instance, for value manipulation risk, assume that the parameters are the invoice value ($), goods type, and country of origin. Figure 5-1 illustrates this dynamic, with the subspaces for value manipulation risk highlighted.

For each shipment, the method represents the shipment's information as points in the value manipulation and undeclared goods spaces. For each space (i.e. risk category), the primary

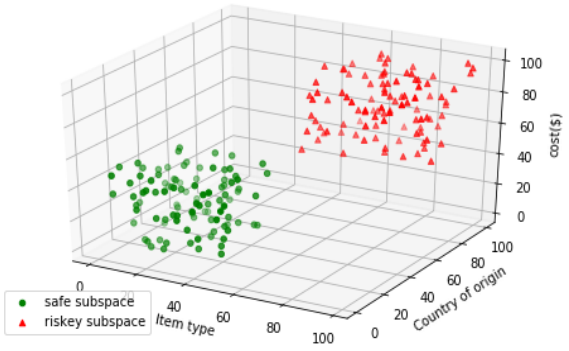

Figure 5-1 the value manipulation transaction space

objective is to determine whether the shipment (i.e. a point) is risky or safe based on its locality. As part of the classification step, the method employs the well-known local outlier factor (LOF) algorithm proposed by (Breunig, et al., 2000), which can determine whether a given point is an outlier by comparing its density against the density of points located in its neighborhood. The algorithm returns an outlier factor (≥ 0) that can be used to determine where the new point (i.e. shipment) is an outlier compared to its neighbors. Next, using the obtained outlier factor for each subspace, the method allows determining whether the new shipment should be labelled as safe or risky. The results show that the method can provide classification that is 83% accurate on average.

Once an assessment stage has processed a shipment, the result is sent to the customs administration in an online manner. If the result is that the shipment is risky, the proposed method gives the customs administration the advantage of having a significant amount of time to investigate the shipment. The proposed method uses the information provided by participants in the international trade supply chain. Thus, to ensure the accuracy of the method's classifications, we need to establish a secure, trusted information-sharing mechanism for all supply chain participants. Such a mechanism can be built by using

blockchain technology. Blockchain is distributed ledger technology (DLT) that can ensure the traceability and integrity of data shared between entities. Several proposals (Engelenburg, et al., 2017; Vos, et al., 2018; Toyoda, et al., 2017; Xu, et al., 2019; Smartz, 2018; Macedo, 2018; Pawczuk, et al., 2019; Loklindt, et al., 2018) have highlighted the potential of optimizing (international) trade supply chains by using blockchain technology. However, using the blockchain-based information exchange mechanism is not mandatory; the method can be integrated with any information-sharing mechanism that can ensure the integrity of the information used.

In this chapter, we have assumed that the proposed method is deployed with a customs-based blockchain that handles importation and exportation in the supply chain. We have focused on a sea channel importation scenario, although with minor modifications the proposed method can be used for any importation channel.

5.2. Trade Supply Chain and Blockchain Technology

In this section, we describe the participants of the international trade supply chain in term of their responsibilities, and we highlight the type of documents exchanges between these participants. Additionally, we briefly describe the main mechanism of blockchain technology.

5.2.1. International Trade Supply Chain

In this work, the focus is on the sea transportation channel; other channels follow relatively the same steps. Figure 1-4 presents the steps of the international trade supply chain (sea channel). In general, this supply chain consists of several parties that include the trading community (importers and exporters), customs agency, shipping agent, port operators,

freight forwarders, and customs brokers. The importation and the exportation scenarios are mainly distinguished by the flow direction of goods and documents in the supply chain.

The responsibilities of the international trade supply chain participants can be described as follows. Freight forwarders communicate directly with the exporter and the shipping agent, where it is responsible for arranging the customers' shipments. Shipping agents deal with the ports and the freight forwarders, where it is responsible for the cargo's transportation. Customs brokers communicate mainly with the customs administration and the trading community. Customs brokers responsible for the preparation of the shipment declaration information, which will be submitted to the customs administration. During the trading process, each of the involved participants performed its tasks based on the documents, which are received from other participants in the trade supply chain. For instance, the broker uses documents received from the trading community and the shipping agents to prepare the declaration form, which is then submitted to the customs administration.

As part of the clearance process, the importer has to submit the following documents to customs administration: (1) commercial invoice, (2) certificate of origin, (3) detailed packing list, and (4) bill of lading. Commercial invoices describe the cost of the shipped items, and it could also show the insurance and shipping cost. Certificate of origin shows the goods manufacturer (or processing) country. The packing list describes the method of packing for each item included in the shipment. Bill of lading acts as a contract that confirms the receipt of the cargo by the freight forwarder.

At customs administration, the risk assessment process has to be performed in a relatively short time window, and therefore, customs administration may not be able to perform

advanced customer and shipment risk assessment, which may require the participation of other external parties. This introduces significant pressure on the customs administration since the authenticity of the documents must also be validated by the customs administration.

5.2.2. International Trade and Blockchain Technology

Using a blockchain-based information sharing mechanism, each of these supply chain participants will have a copy of the transaction history (ledger). The ledger is represented as several blocks, where each block contains a set of transactions (figure 1-3). The connection of the blocks is established using hashing. A block hash value is calculated by using a hash function, which receives the entire block as an input and returns a fixed-length value. Besides the transactions, each block stores the hash value for the previous block. Thus, changing the data stored in any block results in changing the hash value of this block, and therefore it will no longer match the hash value stored in the next block. Using hashing, we can detect any manipulation in the data. In blockchain-based systems, the rules of the system are implemented using smart contracts. Similar to traditional legal contracts, smart contracts encapsulate the logical rules of the system and assure their enforcement through automation.

5.3. Method

The objective is to establish a distributed risk assessment method, which utilizes the inherited features of blockchain-based information-sharing mechanism to achieve its goals. In this work, we assume that a blockchain solution to facilitate the importation scenario is constructed to cover the international trade supply chain participants. We also assume that the blockchain solution is designed and deployed via the customs administration. Thus,

several procedures (smart contracts) are deployed to authenticate the submitted transactions (information) by the supply chain participants.

5.3.1. Overview

The proposed risk assessment method is triggered at two stages in the trade supply chain; namely the manufacturer and the shipping agent stages. In the manufacturer stage, the risk assessment is performed once the manufacturer uploaded the details of the importer requested order to the blockchain. This information includes manufacturer location, invoice details and, the goods country of origin. Assessing the transaction submitted by the manufacturer is expected to help in detecting the valuation risk. On the other hand, the shipping agent risk assessment stage is triggered once the shipping agent related information has also become available on the blockchain. This shipping agent risk assessment stage uses information such as the path of shipment and the trade details to detect undeclared goods risk.

For each of these two stages, the analysis (assessment) is performed at two levels: personal and global. In the personal level, the proposed method analyses the shipment under consideration by using the same importer historical transactions for benchmarking purposes. The efficiency of this level is related to the number of transactions (shipments) performed by the importer in the past. The behavior of importers with relatively long trading history is easier to predicate compared to traders with small trading history. In the global step, the entire available transactions (all importers) is used for benchmarking purposes.

In each stage, the assessment is performed by combining the results of both levels to determine whether the current shipment can be considered risky. Toward this end, in each stage, the available shipments historical information is represented as points in multi-dimensional space. Each stage space is divided into risky and safe subspaces. Risky subspace is used to represent shipments, where the presence of risk is confirmed. Safe subspace represents shipments that did not have any risk issues. In each assessment stage, the outcome of the two assessments levels is represented as two outlier factors sets (personal and global). These factors are then processed to determine whether the current shipment can be considered as risky from this assessment stage perspective. Beside risky, a shipment could be classified as safe or undecidable. Undecidable shipments are expected to be reclassified by the centralized risk assessment process located at the customs administration. The introduction of classification label aims to improve the accuracy of the distributed classification mechanism. Accordingly, a threshold is used by the method to establish a minimum required difference (gap) between the obtained outliers' factors (safe and risky) to classify the shipments. This threshold is introduced since shipments with a relatively small gap between these outliers do not have clearly unique classification features.

Next, we describe the transactions representation, the Local-density Outlier Factor (LOF) algorithm, and the classification process.

5.3.2. Transactions Representation

The shipment information is in two spaces; the manufacturer, and the shipping agent spaces. Both of these spaces contain a subset of the information that is included in the importation declarations form, which is normally submitted to the customs administration.

The information that will be encoded in each space depends on the category of risk associated with each space.

To detect the value manipulation risk, information (parameters) related to the manufacturing detailed and price are required to detect the presence of any value manipulation risk. These parameters represent the dimensions of the manufacturer space, and can be described as follows:

- **Cost**: represents the total amount of money paid by the importer to the manufacturer.
- **Location**: represents the country of the manufacturer.
- **The shipped goods Harmonized System code (HS-code)**. This system is used to define a unique number for each item category. HS-code is used by customs to calculate the amount of duties; the traders are expected to pay. In addition, the HS-code is used to determine whether the shipped items can enter the country with or without permits.

Once the manufacturer space is constructed, historical shipments information is represented as points in this 3-dimensional space. Each point has three coordinates values $(c: \text{cost}, l: \text{location}, h: \text{HScode})$. Beside these coordinates, the importer identification number and a unique number to identify the shipment will be also encoded on the point. The selection of these coordinates in the value manipulation risk assessment aims to establish a relationship between the goods cost, manufacturer location, and HS-code. This relationship can be used to analyses whether the importer manipulated the manufacturer information in order to reduce the amount of duty.

The shipping agent space consists of four dimensions that represent the shipping agent identification number, the goods HS-Code, port of loading, and trading volume. These parameters (coordinates) aim to clarify whether the selection of a specific agent for the shipment under consideration is expected. Additionally, it clarifies whether such goods are expected to be delivered from the declared port. In this space, historical shipment information is represented as points in 4-dimensional space. Similar to the representation in the manufacturer space, each point contains the coordinates, the importer identification number, and the subspace identification number.

By having two subspaces, this representation aims to simplify the problem of detecting risky shipments, since each risk category can be addressed separately.

5.3.3. The Local-density Outlier Factor (LOF)

In this section, for the sake of completeness, we describe the mechanism of the LOF algorithm. For a given point A, this algorithm takes into consideration the density of the points located inside point (A) neighbourhood to determine whether this point is an outlier. By considering the local density, this algorithm can be used to capture the scenarios where the characteristics of an outlier point might change over time. Once a point is processed, this algorithm returns an outlier factor (≥ 0). In situations where the value of this factor is greater than one, the point will be considered as an outlier. In other situations, the point will be handled as a normal point.

This algorithm starts by calculating the distance between each point (transaction), and its k-nearest neighbor (KD). For each point, we then calculate the reachability distance (RD) between this point and all points located inside its neighborhood. The reachability distance

of point A from point B is the maximum between the actual distance between these two points or the k-nearest distance of point A ($RD\ (A,B) = max\{KD(B), d(A,B)\}$).

Then, the algorithm proceeds to calculate the points Local Reachability Density (LRD). For a given point A, the local reachability density is calculated by taking the inverse of the average reachability distance of all points in A neighbourhood to itself. The local reachability density for point A is calculated as follows:

$$LRD(A) = \frac{1}{\sum_{B \in N(A)} RD(A,B)/|N(A)|}$$

Where $N(A)$ refers to the neighbors of point A. of point Lastly, the LOF of a point A is calculated by dividing the average ratio of the local reachability density of point A neighbours over that local reachability density of point A itself. The LOF for point A is calculated as follows:

$$LOF(A) = \frac{\sum_{B \in N(A)} LRD(B)}{|N(A)| \times LRD(A)}$$

Using this calculation it is clear that the lower the local reachability density of point A, the higher the LOF. This captures the situations when the distances between a point and its neighbours are relatively large (sparse). The value of this factor (LOF) determines whether the point under consideration can be considered as an outlier. The higher the LOF value ($\gg 1$), the more likely that this point is an outlier.

5.3.4. The Classification Process

The triggering of this process is associated with the submission of the manufacturer and shipping agent transactions to the blockchain. The submission of the commercial invoice

details by the manufacturer triggers the value manipulation risk assessment. On the other hand, submitting the shipping agent transaction to the blockchain triggers the undeclared goods risk assessment. Once each risk assessment is performed, the result of this assessment is submitted to the customs administration via the blockchain system. Such a strategy provides the customs administration with real-time assessment of shipment during the international trade supply chain stages. Additionally, providing such information in advance gives customs the ability to investigate the shipment in more details. This assessment process is designed to complement the risk assessment performed at the customs administration.

For each risk category, the riskiness of a point (shipment) is obtained by analyzing the locality of this point in the risky and safe subspaces. For each subspace, the assessment process determines whether the new point can be categorized as normal or outlier point. This categorization is established by considering the density of the points around the new point location, and it is performed using the LOF algorithm. The objective of using both subspaces in this risk assessment process is to provide a more accurate risk assessment.

In situations where the new point (shipment) is only considered as an outlier in one of the subspaces (safe or risky), it is easy to determine the riskiness factors of this shipment. For instance, if the new shipment is considered as an outlier in the safe subspace, and normal in the risky subspace, this point (shipment) is considered as risky. However, in situations where the new shipment is considered as an outlier in both subspaces, the outlier factor values must be taken into consideration to determine the riskiness factors of the shipments. For instance, consider the example shown in figures 5-2, where points p_1 and p_2 represent two shipments. Both of these points are expected to be outliers in the safe and risky

subspaces. The safe and risky outliers' factors for point p_2 is expected to be relatively the same, since this point is located in the middle between the two subspaces. However, point p_1 is located closer to safe subspace than the risky subspace, and therefore it might be considered as safe point.

Any point with relatively the same safe and risky outlier factors is considered as an undecidable point (shipment). Figure 5-3 highlights the steps of the risk assessment process. This process performs risk assessment at the personal and global levels. Personal risk

assessment uses only the same importer historical transactions in the assessment process (line 3), where the global risk assessment uses all importers historical transactions (line 4).

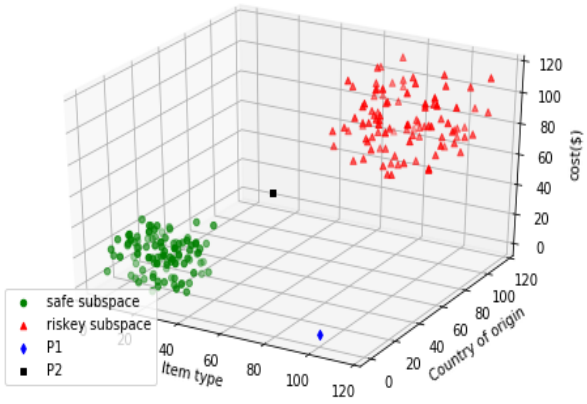

Figure 5-2 Points Classification Example

The outcome for each risk assessment level is represented using two variables; namely; (1) the safe outlier factor (s_f), and (2) the risky outlier factor (r_f). The number of points in the personal assessment history might be relatively small. Additionally, the global assessment does not precisely capture the importer behavior. Thus, both of these level factors are taken into consideration during the assessment of the shipments. In this work, we use the personal

assessment level factors (Ps_f and Pr_f) to tune (increase or/and decrease) the global assessment level risk factor (Gr_f). This tuning (lines 5-8) only occurs when the value of the personal factors suggests that the current shipment is risky, and this occurs when $Pr_f \leq 1$ and/or $Ps_f > 1$.

In situations where the personal risk factor is less than or equal to one (line 5), the global risk factor is updated by subtracting $\left((1 - Pr_f) \times \frac{|P|}{|G|}\right)$ from its value, where $|P|$ is the number of points in the personal history, and $|G|$ is the global history size. In other situations where the personal safe factor is greater than one, the global safe factor is updated by adding $\left((Ps_f - 1) \times \frac{|P|}{|G|}\right)$ to its value (line 7). These updates occur to emphasis the situation where the personal risk assessment considers the shipment as risky.

To start the assessment part of the process, we begin by rounding the resultant global factors with value less than one to one, since we treat inlier points as normal points (line 9). Then, we calculate the absolute difference between the global risk and safe factors (g) (line 10). As part of this process, we use a threshold (t) to determine the minimum possible acceptable gap between these two factors in order to classify the shipment. In situations where the gap is less than or equal to the threshold ($g \leq t$), the point is considered undecidable, since in this situation the global assessment factors do not clearly identify the riskiness status of the shipment.

To label a point (shipment) as safe, the gap must be greater or equal to the threshold, and the global safe factor must be smaller than the global risk factor. A shipment is labelled as risky when the global safe factor is greater than the global risk factor by at least t value.

The threshold is introduced as a controlling parameter, were increasing the value of this threshold is expected to reduce the number of misclassified shipments. Furthermore, increasing this threshold increases the number of undecidable shipments. However, in this method, we are mainly concerned with reducing the percentage of misclassified shipments, since the undecidable shipments are expected to be re-classified using the centralized assessment strategy deployed at customs administration.

5.4. Evaluation

classificationProcess $(p(c,l,h), type, t)$
    input: $p = point\ to\ examine, t = threshold$
        $type = risk\ categoey$
    output: $label\ (u: undecidable, r: risky, s: safe)$
1 $P_h \leftarrow getImporterHistory(p, type)$
2 $G_h \leftarrow getGlobalHistory(type)$
3 $Ps_f \leftarrow LOFSafe(P_h, p), Pr_f \leftarrow LOFRiskey(P_h, p)$
4 $Gs_f \leftarrow LOFSafe(G_h, p), Gr_f \leftarrow LOFRiskey(G_h, p)$
5 **If** $Pr_f \leq 1$ **then**
6 $Gr_f \leftarrow Gr_f - \left((1 - Pr_f) \times \frac{|P|}{|G|}\right)$
7 **If** $Ps_f > 1$ **then**
8 $Gs_f \leftarrow Gs_f + \left((Ps_f - 1) \times \frac{|P|}{|G|}\right)$
9 $Gs_f, Gr_f \leftarrow RoundLowerThanOne(Gs_f, Gr_f)$
10 $g \leftarrow |Gr_f - Gs_f|$
11 **If** $g \leq t$ **then**
12 $label \leftarrow u$
13 **Else If** $(Gr_f > Gs_f)$ **then**
14 $label \leftarrow s$
15 **Else**
16 $label \leftarrow r$
17 **Return** $label$

Figure 5-3 The Classification Process

The efficiency of the presented method is evaluated using several sets of experiments. The input data used in these experiments are obtained from the service innovation department at Dubai Customs. The used data consists of 12,221 shipment declaration applications submitted to Dubai Customs in 2018 (sea channel). These applications are already labelled as either risky or safe based on the outcome of the inspection performed by the customs administration. These declaration applications consist of 11% risky shipments and 89%

safe shipments. The declaration applications are pre-processed to extract the required information for the value manipulation and undeclared goods risks assessments. In the presented experiments, 70% of the applications are used to represent the historical data, where the rest of the applications (30%) are used for testing purposes.

To capture the impact of the threshold (t) on the proposed method performance, we performed these experiments while varying the value of this threshold. To determine the value of k in the LOF algorithm, we have performed sensitivity analysis, where we incremented the value of k by one until the algorithm performance becomes stable. The stability is achieved when $k = 10$, and therefore in the presented experiments, the value of k is set to ten.

To calculate the overall accuracy of the presented method (shipment level), the entire shipments must be classified to either risky, safe, or undecidable. Shipments are labelled as risky if any of the two risk assessments stages (manufacturer or shipping agent) identify the shipment as risky. A shipment is identified as undecidable if both risk assessments stages labelled the shipment as undecidable. In other situations, the shipments are classified as safe.

Besides accuracy, the used performance metrics in these experiments are precision, recall, and F1-score. These metrics are measured for each main classification class (safe and risky). In situations where we focus on the risky classification results, precision is defined as the percentage of correctly classified risky shipments.

Where TP (true positive) refers to the number of correctly classified risky shipments, and FP (false positive) refers to the number of safe shipments that are wrongly classified as

risky shipments. In this work, since undecidable shipments are assumed to be re-classified at the customs administration, shipments with undecidable status are not considered during the calculation of the accuracy, precision, recall, and F1-score.

Recall is defined as the percentage of correctly identified risky shipment over the total number of risky shipments.

Table 5-1 Performance Measures

	Precision	recall	F1-score
Risky	73%	85%	79%
Safe	90%	81%	85%

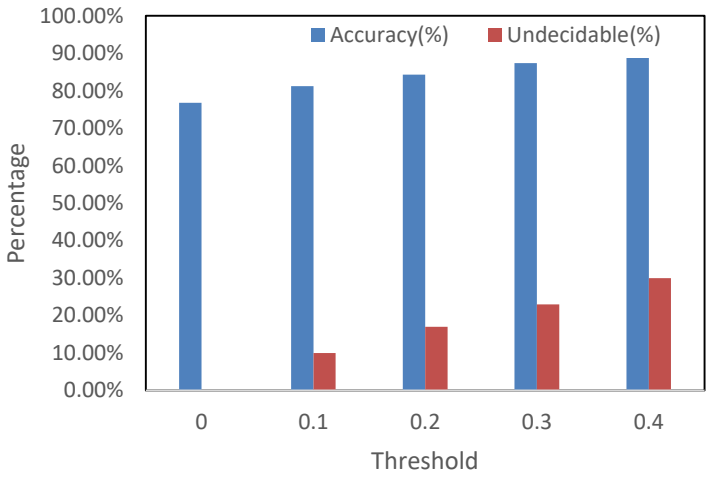

Figure 5-4 Threshold Value Against the Accuracy and the Undecidable Shipments Percentages

The value of this score ranges from zero to one, where the best accuracy occurred when the value of this score is one.

5.4.1. Results

To investigate the impact of the threshold value on the accuracy and the percentage of the undecidable shipments, we ran the experiment, while varying the value of the threshold. Figure 5-4 shows the results of these experiments. The result shows that increasing the threshold value increases classification accuracy. This is expected, since increasing the threshold results in increasing the percentage of shipments, which are labelled as undecidable, and this increases the probability of correctly classifying the rest of the shipments. Additionally, increasing the threshold value results in increasing the acceptable gap between the shipments safe and risked outlier factors, and therefore the shipments that will be examined are expected to have more distinct features that simplify the classification process.

Next, to clarify the percentage of truly risky shipments detected by each risk assessment stage, we ran the experiment while varying the threshold values (Figure 5-5). The results show that the shipping agent assessment stage (undeclared goods risk) is always able to detect a higher percentage of risky shipments compared to the manufacturer risky assessment stage (value manipulation). This highlights the relationship between the two risk categories. To clarify this relationship, let us consider the objective of each risk assessment stage. Manufacturer risk assessment stage aims to detect any manipulation in the original invoice that is submitted by the manufacturer (value manipulation risk). Shipping agent risk assessment aims to detect any suspicions in term of shipping path and the traded goods. In this direction, shipment declarations that are labelled by the shipping

agent risk assessment as risky are more likely to be also labelled as risky by the manufacturer risk assessment. This is established since the shipments with undeclared goods risk is more likely to use fraudulent manufacturer documents. On the other hand, shipments declarations with value manipulation risk are not necessarily expected to have undeclared goods risk, since most cases of this risk type deal with manipulating the information to avoid paying duties.

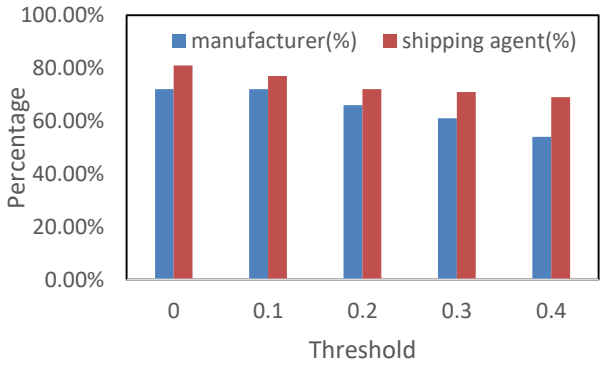

Figure 5-5 Threshold Value Against the Percentage of Risky Shipments Captured by the Manufacturer and the Shipping Agent Assessment Stages

To investigate the performance of the proposed method in term of accuracy factors (precision, recall, and F1-score), we ran the experiments for threshold value equal to 0.2. In these experiments, we calculate the performance factors for both the risky and safe classifications. The results of these experiments are shown in Table 2. From the results, we can see that the precision score for the safe shipment classification is significantly higher compared to the risky shipments classification. In this scenario, the shipments with risky classification label are further examined by the centralized risk assessment process at customs administration, whereas shipments with safe classification label are expected to be quickly cleared by the customs administration. Thus, achieving a high precision score

for the safe shipments' classification is desirable in this situation. About the risky shipment classification precision, from the results, we can see that 27% of the risky classified shipments were safe shipments. This occurs because the distance between these safe shipments and the risky subspace is expected to be relatively small. In this direction, the proposed method labelled these shipments as risky to be re-classified by the centralized risk assessment functionality located at the customs administration.

The performance of the proposed methods depends mainly on the threshold value, and the employed risk assessment stages. One of the main advantages of this method is that new risk assessment stages can be designed and deployed without interrupting the rest of the stages. In addition, since we assume that the method is implemented on top of a blockchain solution for international trade, any risk assessment stage can be modified by deploying a new smart contract (newer version of the code) to replace the current active one. The mechanism of adopting the threshold strategy aims to take advantage of the fact that regardless of the deployed distributed risk assessment method, a centralized risk assessment strategy is also required to be deployed at the customs administration. Beside re-examining risky classified shipments, the centralized risk assessment process is designed to capture the intelligence information provided by external departments (Interpol and police department). Therefore, the proposed method works well in situations where it is employed as a secondary assessment level to provide real-time feedback about the shipments risk assessment at different stages in the trade supply chain.

5.5. Related work

The use of outlier detection algorithms has advanced the detection of abnormal activities in different application domains such as network traffic intrusion (Huang, et al., 2013;

Huang, et al., 2015), money laundering (Gao, 2009; Chen, et al., 2007), and fraud detection (Sharmila, et al., 2019; Malini & Pushpa, 2017; Badriyah, et al., 2018).

In computer network domain, the detection of abnormality in network traffic is performed by analyzing the network traffic periodically to capture any irregularity in traffic flow. To address this problem, Gan et al. proposed an improved version of the LOF algorithm that attempts to capture the irregularity in the traffic pattern, where network traffic is represented as points in multi-dimensional space. In this improved version, the authors combined LOF with clustering approach to optimize the identification of the neighborhood (Gan & Zhou, 2018).

Based on the application domain, traffic pattern may change-over-time, and therefore the threshold that determines whether a certain point is an outlier may change over time. In this direction, Huang et al. proposed adoptive outliers detection method that employs a knowledge-based component as part of the outlier detection mechanism. In this component, the identity of the points that are used to capture the data behavior is updated periodically (Huang, et al., 2013). To improve the adaptivity, the authors use an incremental majority learning approach to optimize the size of the time window used in the training of the model (Huang, et al., 2015).

To address the money laundering problem, Gao et al. proposed a LOF-based mechanism that applies a clustering approach to reduce the complexity of the outlier detection problem. In this solution, the distance between any two transactions belong to the same cluster must be less than or equal a pre-determined threshold. In this context, threshold is used as a measurement of similarity between transactions. Once clusters are established, the

proposed solution apply LOF algorithm to identify outliers (Gao, 2009). Larik et al. have adopted the same concept, where clustering is used to group the individuals' financial behaviors (Larik & Haider, 2011). Statistical methods are used to determine if a given cluster's transaction can be considered as an outlier (Larik & Haider, 2011).

In an attempt to study the financial behavior of Taiwanese companies, the authors applied the LOF algorithm to capture the abnormality in these companies' behaviors. As part of the results, the authors suggested that outlier detection algorithms such as LOF can be used to establish a warning system about companies' abnormal activities (Chen, et al., 2007).

In the credit card domain, several proposals have addressed the importance of using outlier detection algorithms (such as LOF and k-Nearest Neighbors) to detect fraudulent activities. In these papers, the authors show that the behavior of the transaction can be efficiently determined, and therefore fraud detection mechanism can be established using outlier detection algorithms (Sharmila, et al., 2019; Malini & Pushpa, 2017).

Badriyah et al. have applied the k-Nearest Neighbors outliers detection mechanism to identify frauds in cars insurance application domain. To identify fraud, this mechanism compares the features of the new transaction (attributes) against the features of its k-nearest neighbors. In this direction, if a transaction does not share similarity with the majority of its neighbors, it is considered as an outlier (Badriyah, et al., 2018). In another research, the authors presented an empirical study that aims to quantify the applicability of using outlier detection algorithms such as LOF and k-Nearest Neighbors to detect health insurance fraud. This study highlighted that in this domain, the LOF algorithm has relatively reasonable performance (Bauder, et al., 2018).

In this work, as part of the proposed risk assessment method, the LOF algorithm is used to detect whether a given point can be considered as an outlier. Other outlier detection mechanisms could also be used for this purpose. However, the LOF algorithm is selected since the density of the trade transactions is expected to change over the financial year. Therefore, employing local density-based outlier detection mechanism such as LOF is expected to capture the variation in the data pattern over time.

5.6. Conclusion

In this chapter, we proposed a distributed risk assessment method that employs the well-known LOF algorithm to detect whether the new shipment can be considered risky (outlier). The proposed method is designed to reduce the pressure on customs administrations by performing an early-stage risk assessment. This gives the customs administration the advantage of investigating the shipment in more detail if required. By considering the safe and risky historical shipment information, the proposed method attempts to improve its classification accuracy. Using this method, points are classified as either safe, risky, or undecidable. The undecidable point (shipments) are required to be investigated further (re-classified) by the customs administration. The results show that the proposed method can achieve around 83% accuracy.

6. Chapter 6: Customs-based Hybrid Risk Assessment Method

6.1. Introduction

Customs Administrations globally are tasked with safeguarding local borders thereby protecting their respective society from dangerous people and materials while enhancing global economic competitiveness by enabling legitimate trade and travel (World Customs Organization, 2018). Their role includes combating criminal cross-border activities conducted by small to large criminal networks. The main objective of these networks is illicit financial gain and fortune. The success of identifying, degrading and disrupting these criminal networks depends on many things, with document verification, analytics and risk assessment right at the top of the list. Leveraging the data flows and analytical abilities, coupled with close collaboration with local and international partners, customs has a higher chance of dismantling these networks.

Customs Authorities put a lot of emphasis on being proactive and the strict enforcement of trade laws to protect national economic security, facilitate trade, protect the health and safety of local society, and ensure a level playing field for local industry. To guarantee seamless cross-border trade flow the process of risk assessment is considered a critical process that aids in confirming the authenticity of trade documents and detecting all forms of suspicious activities. From Customs administration perspective, shipments related risks can be mainly categorized into value manipulation and undeclared good. Risk in term of value manipulation occurs when the trader falsified the trade documents in order to reduce the expected amount of duties, he/she is expected to pay. Value manipulation causes lost in revenue, and has a damaging effect on the local economy. On other hand, undeclared

good risk occurs when the trader manipulates the trader documents in order to smuggle restricted or prohibited goods to the country. Restricted goods such as pharmaceutical items and weapons require special permits from governments authorities to enter the country. Smuggling restricted goods (without permits) to the country has a major impact on the society, since the objective of obtaining the permit is to make sure that the shipped goods and recipients satisfy the country standard and rules. Prohibited goods represent all products that are not allowed to entre to the country under any circumstances. The identity of such products varies between the countries; however, illegal drugs and fake could be considered as example of prohibit goods. The presented risk types emphasize the importance of the protection rule performed by the customs administration

Cross-border trade transactions involve multiple parties, including the trading community (importers and exporters). Throughout the cross-border trade process a number of documentary requirements are produced. Each of the involved entities performs its tasks based on some or all of these documents. For instance, customs process the declaration application submitted by the broker, and then send the outcome - the clearance - to the next entity in the supply chain. A major issue facing customs authorities and other parties with this process is ensuring the integrity of the exchanged information. This information sharing mechanism and documentary exchange are a dominant factor in determining the overall efficiency of the end-to-end process in the supply chain. Customs authorities is one of the primary parties in the chain and has a role to play in protecting local society and developing economic prosperity. The protection task is established by monitoring the flow of goods entering the country to detect counterfeit products and smuggling activities. To fulfil this task, customs authority relies on the information provided by the various

participants in the international trade supply chain. This information is used in the shipment clearance process to examine the shipment under consideration and to determine if a physical examination is required (World Customs Organization, 2018).

The complexity of the centralized risk assessments functionalities if we can establish a secure trusted information sharing system between the entire international trade chain participants. Using such system, proposing decentralized risk assessment functionalities become desired objective. Trusting the exchanging information can be guaranteed by employing blockchain information sharing mechanism between the international trade supply chain participant. Blockchain is Distributed Ledger Technology (DLT) that can ensure the traceability, integrity, and immutability of the shared data between the participating entities. Several proposals (Engelenburg, et al., 2017; Vos, et al., 2018; Bocek, et al., 2017; Toyoda, et al., 2017; Xu, et al., 2019; Smartz, 2018; Macedo, 2018; Pawczuk, et al., 2019; Loklindt, et al., 2018) have highlighted the potential of optimizing the (international) trade supply chain through the use of the blockchain technology.

In this chapter, we propose a hybrid two-stages risk assessment method This method consists of two steps; the decentralized and the centralized risk assessment steps. In this work, we focus on the sea channel importation scenario, with minor modification, the proposed method can used for any importation channel. The method presented in this work significantly extend the method (Juma, et al., 2019c). This extension included the addition of the centralized risk assessment step, and the restructuring of the decentralized risk assessment step. In this work, we assume that the trade supply chain solution is implemented using blockchain solution. Therefore, the exchanged information can be trusted.

In the distributed risk assessment step, the main idea is to divide the risk assessment functionalities into several components that are performed at different stages in the international trade supply chain. The proposed method performs two types of risk assessments; value manipulation and undeclared goods. Once a shipment has been examined using the distributed risk assessment step, this shipment will be classified to either safe, risky, or undecidable. Safe shipments will not be physically examined at the customs administration. Risky shipments will be physically inspected. Shipments that could not be clearly classified to safe or risky, will be classified as undecidable, which will be sent to the centralized risk assessment step for classification.

In the distributed risk assessment step, risk related to value manipulation is assessed by analyzing the manufacturer related information, such as invoice and country of origin. Undeclared goods risk is assessed using information related to path and type of shipment. For each type of risk assessment, the proposed method divides the historical space into "safe" and "risky" subspaces. The risky subspace contains all shipment information where the risk is identified and confirmed. Safe subspace represents shipments where no risks are identified. For each subspace, historical information is represented as points in multi-dimensional space. Whereas, the dimensions of each space represent the parameters that are used to analyses the risk type. For instance, for value manipulation risk, assume that the parameters used during risk analysis are the invoice value ($), goods type and country of origin. In this example, each of these parameters will be represented as a dimension in the value manipulation space. Figure 6-1 illustrates this such representation, where the subspaces are highlighted.

Using similar representation, for each new shipment, the method works by representing the shipment information as two points in the value manipulation and undeclared goods spaces;

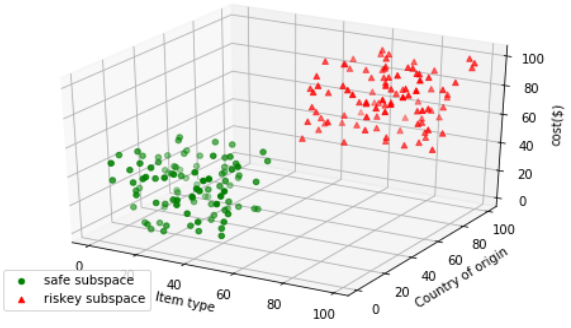

Figure 6-1 An Example to Illustrate Shipment Representation Using Multidimensional Space

respectively. Then, for each risk type, the method works to determine whether the new shipment (point) is closer to its risky or safe subspace. In situation where the new shipment is relatively located at the same distance from the safe and risky subspaces (Breunig, et al., 2000), this shipment will be considered as undecidable. Any shipment with undecidable label will be send to the centralized risk assessment step for reclassification. The centralized risk assessment step employs the well-known Random Forest Classifier (Ho, 1995), where the entire labelled historical data is used train this classifier. The results show that the accuracy of the presented method is around 90%.

6.2. Related Work

Outlier detection is a density-based algorithm (also known as anomaly detection). Outlier detection is also known as unsupervised anomaly detection. It is used to capture exceptional cases that deviate substantially from the majority of patterns. It is the process

of finding data objects with behaviors that are very different from expectation. Such objects are called outliers or anomalies.

Outliers can be of two kinds: univariate and multivariate. Univariate outliers are used for looking at a distribution of values in a single dimensional space. Multivariate outliers are used for a n-dimensional space (of n-features). Models are trained to look at distributions in n-dimensional spaces since it can be very difficult for the human brain to do it.

Outlier detection algorithms has advanced the detection of abnormal activities in many application domains such as network traffic intrusion (Huang, et al., 2013; Huang, et al., 2015), money laundering (Gao, 2009; Chen, et al., 2007) and fraud detection (Sharmila, et al., 2019; Malini & Pushpa, 2017; Badriyah, et al., 2018), fake news and misinformation, healthcare analysis, security and surveillance and more.

Density-based approaches to outlier detection have been proposed, Local outliers are the objects that differentiate or differ from their neighborhood in a dataset. In computer network domain, periodic analysis for the detection of abnormality in network traffic is performed to capture any irregularity in traffic flow. To capture the irregularity in the traffic pattern, Gan and Zhou (2018) proposed an improved version of the LOF algorithm with network traffic represented as points in multi-dimensional space. In this improved version the clustering approach was combined with LOF by the authors to optimize the identification of the neighborhood. Outlier detection was combined with clustering analysis because the two are highly related tasks. Clustering finds the majority of patterns in a data set and organizes the data accordingly.

Based on the application domain, the threshold that determines if a certain point is an outlier may change over time because traffic patterns can possibly change-over-time. With this in mind, Huang, et al. (2013) proposed adoptive outlier's detection method that employs a knowledge-based component as part of the outlier detection mechanism. In this component, periodic update of the identity of the points used to capture data behavior. To optimize the size of the time window used in training the model, the authors use an incremental majority learning approach to improve adaptivity (Huang, et al., 2015).

To address the money laundering problem, Gao et al. proposed a LOF-based mechanism that applies a clustering approach to reduce the complexity of the outlier detection problem. In this solution, distance between two transactions are clustered together must be less than or equal a pre-determined threshold (Gao, 2009). In this context, threshold is used as a measurement of similarity between transactions. The proposed solution starts with the clustering approach to establish clusters, then apply LOF algorithm for the identification of outliers. A study have adopted a similar concept in which clustering is used to group the individuals' financial behaviors then employ statistical methods to determine if a given cluster's transaction is an outlier (Larik & Haider, 2011).

LOF algorithm to discover behavioral abnormalities as part of a study relative to the financial behavior of Taiwanese companies was used by the authors. This study resulted in the authors suggesting that outlier detection algorithms such as LOF is a good mechanism to establish a warning system about companies' abnormal activities (Huang, et al., 2015).

In the credit card domain, a number of proposals (Sharmila, et al., 2019; Malini & Pushpa, 2017) have stated the importance of using outlier detection algorithms (such as LOF and

k-Nearest Neighbors) in the detection of fraudulent activities. In these papers, the authors determined that fraud detection mechanism can be established using outlier detection algorithms to show that the behavior of the transaction can be efficiently determined.

Badriyah et al. have applied the k-Nearest Neighbors outliers detection mechanism to identify frauds in cars insurance application domain. To identify fraud, this mechanism compares the features of the new transaction (attributes) against the features of its k-nearest neighbors. From this perspective, if a transaction does not share similarity with the majority of its neighbors, it is considered as an outlier (Badriyah, et al., 2018). An empirical study that aims to quantify the applicability of using outlier detection algorithms such as LOF and k-Nearest Neighbors to detect health insurance fraud by (Bauder, et al., 2018). This study highlighted that in this domain, the LOF algorithm has relatively reasonable performance.

In this chapter, as part of the proposed risk assessment method, we use the LOF algorithm to detect whether a given point is an outlier. Other outlier detection mechanisms could have employed in the proposed method. However, the LOF algorithm is selected since the density of the trade transaction is expected to change over the financial year. Therefore, employing local density outlier detection mechanism such as LOF is expected to capture the variation in the data behavior over time.

6.3. Method

The objective is to establish an accurate risk assessment method, which utilize the inherited features of blockchain-based information sharing mechanism to achieve its goals. The proposed method consists of two steps of assessments, (1) decentralized and (2) centralized

risk assessment steps. The decentralized step employed a light-weighted process that aim to detect any risk at early stages in the trade supply. Based on the available information though the supply chain, this step classifies shipments to safe, risky, and undecidable. The undecidable shipments will be re-classified using the centralized risk assessment step at the custom administration. This step is performed using the Random Forest Classifier. In this work, we assume that a blockchain solution to facilitate the importation scenario is constructed to cover the international trade supply chain participants.

6.3.1. Overview

Starting from the manufacturer (exporter), once a shipment transaction is performed, each participant broadcasts the performed transaction to the rest of the participants using blockchain-based information sharing. In this work, we assume that the blockchain solution is designed and deployed via the customs administration. Thus, several procedures (smart contracts) are deployed to authenticate the submitted transaction by the supply chain participants.

The functionalities of the distributed risk assessment step are triggered at two stages in the supply chain; namely (1) the manufacturer and (2) the shipping agent stages. Manufacturers submit information that describe the details of the requested order by the importer. This information includes manufacturer location, invoice details and the goods' country of origin. Performing assessment on the transaction submitted by the manufacturer is expected to help in detecting valuation risk. On other hand, shipping agents submit information related to path of the shipment, where this information can help in detecting undeclared goods risk. Once each of these participants submit their transaction via the information sharing mechanism, the distributed risk assessment smart contract is triggered

to analyses the shipment details. For each of these two participants, the analyses use all historical transactions conducted by all importers for benchmarking purposes.

Historical trade transactions in both stages (manufacturer and shipping agent) of the assessment are represented as points in multi-dimensional space and grouped into risky or safe subspaces. In the event that the presence of risk is confirmed, the shipment is categorized and placed in the risky subspace. Otherwise, it is placed in the safe subspace. Outcome of each assessment stages is represented as outlier factor. The factor obtained by each assessment stages is then processed to determine whether the current shipment can be considered risky from this assessment stage perspective. In addition to a shipment being both equally risky and safe, another category of undecidable is introduced. Undecidable shipments' reclassification is handled by the centralized risk assessment step, held at the customs administration. This step uses more shipment declaration features in order to re-classify the undecidable shipments. In this work, the centralized risk assessment stage is modelled as random forest classifier.

The introduction of the undecidable classification label aims to improve the accuracy of the distributed classification mechanism. Accordingly, a threshold is used by the method to establish a minimum required difference (gap) between the obtained outliers' factors (safe and risky) to classify the shipments. This threshold is introduced since shipments with a relatively small gap between these outliers, do not have clearly unique classification features.

Next, we describe the distributed and centralized risk assessments steps.

6.3.2. Distributed Risk Assessment Step

The main idea of this step is to represents the shipments declaration information as points in multi-dimensional space in order to apply the outlier detection mechanism

6.3.2.1. Transaction representation

In the proposed method, shipments declaration information is represented as points in multi-dimensional spaces. Each risk assessment stage is associated with the information representation space. In the manufacturer risk assessment stage, the following shipments are represented in 5-dimensional space, where the dimensions are describing as follows:

- Value: represents the total amount of money paid by the importer to the manufacturer.
- Goods HS-code: The HS-code is used to define a unique number for each item category and by customs to calculate the amount of duties the traders are expected to pay as well as determine whether the shipped items can enter the country, with or without permits.
- Duty value: the duty value amount calculated by the custom administration for the shipped goods.
- Country of origin: the manufacturing country of the shipped goods.
- Cost, Insurance and Freight (CIF) value: this value represents the total cost of the shipment including the insurance and freight forwarder charges.

Besides these coordinates, the classification label (risky or safe) and a unique number to identify the shipment is also stored in the shipment point. The selection of these coordinates

in the value manipulation risk assessment aims to establish a relationship between the selected dimensions. This relationship can be used to analyses whether the importer manipulated the manufacturer information in order to reduce the amount of duty.

The shipping agent space consists of six dimensions – the shipping agent identification number, the goods HS-code, the CIF value, the original port of loading, the last port of loading and the country of origin. These parameters (coordinates) aim to clarify whether the selection of a specific agent for the shipment under consideration is expected. Additionally, it clarifies whether such goods are expected to be delivered from the declared ports. In this space, each point contains the coordinate parameters, the classification label (safe or risky) and the shipment identification number.

With two subspaces, this representation aims to simplify the problem of detecting risky shipments, since each risk category can be addressed separately.

6.3.2.2. The Local-density Outlier Factor (LOF)

In this section, we begin by providing a simplified explanation of the mechanism of the LOF algorithm. Local outlier factor is a density-based method that relies on nearest neighbor's search. The Local Outlier Factor (LOF) algorithm is an unsupervised anomaly detection method which computes the local density deviation of a given data point with respect to its neighbors. It considers samples that have a substantially lower density than their neighbors as outliers. For a given point *A*, the algorithm looks at the neighbors of

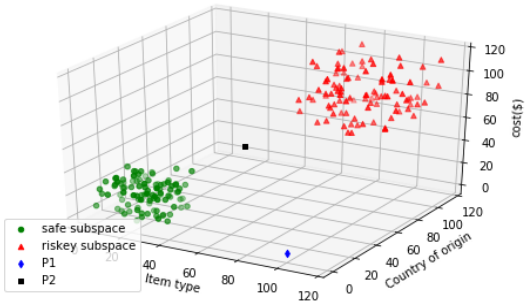

Figure 6-2 Points Classification Example

point (*A*) to find out its density and compare this to the density of neighbor points to later on decide whether this point is an outlier. By considering the local density, this algorithm can be used to capture the scenarios where the characteristics of an outlier point might change over time. This algorithm returns an outlier factor (≥0). In cases where the value of this factor is greater than one, the point will be considered as an outlier. In other cases, the point will be handled as a normal point.

Nearest neighbor based outlier detection techniques require a distance (or similarity measure) defined between two data instances. Distance (or similarity) between two data instances can be computed in different ways.

This algorithm starts by calculating the distance between each point (transaction), and its k-nearest neighbor. For each point, we then calculate the reachability distance between this point and all points located inside its neighborhood. The reachability distance of point *A* from point *B* is the maximum between the actual distance between these two points or the k-nearest distance of point *A*.

Then, the algorithm proceeds to calculate the points local reachability density. For a given point *A*, the local reachability density is calculated by taking the inverse of the average

reachability distance of all points in *A* neighborhood to itself. Lastly, the LOF of a point *A* is calculated by dividing the average ratio of the local reachability density of point *A* neighbors over that local reachability density of point *A* itself Using this calculation it is clear that the lower the local reachability density of point *A*, the higher the LOF. This captures the situations when the distances between a point and its neighbors are relatively large (sparse). The value of this factor (LOF) determines whether the point under consideration can be considered as an outlier. The higher the LOF value ($\gg 1$), the more likely that this point is an outlier.

6.3.2.3. The Classification Step

The triggering of this step is associated with the submission of the manufacturer and shipping agent transactions to the blockchain. The submission of the commercial invoice details by the manufacturer triggers the manufacturer risk assessment stage. On the other hand, submitting the shipping agent transaction to the blockchain triggers the shipping agent risk assessment stage. Once each risk assessment is performed, the result of this assessment is submitted to the customs administration via the blockchain system. Such a strategy provides the customs administration with real-time assessment of shipment during the international trade supply chain stages.

For each stage, the riskiness of a point (shipment) is obtained by analyzing the locality of this point in the risky and safe subspaces (Engelenburg, et al., 2017). For each subspace, the assessment process determines whether the new point can be categorized as normal or outlier point. This categorization is established by considering the density of the points around the new point location, and it is performed using the LOF algorithm. The objective

of using both subspaces in this risk assessment process is to provide a more accurate risk assessment.

In situations where the new point (shipment) is only considered as an outlier in one of the subspaces (safe or risky), it is easy to determine the riskiness factors of this shipment. For instance, if the new shipment is considered as an outlier in the safe subspace, and normal in the risky subspace, this point (shipment) is considered as risky. However, in situations where the new shipment is considered as an outlier in both subspaces, the outlier factor values must be taken into consideration to determine the riskiness factors of the shipments. For instance, consider the example shown in figure 6-2. For the sake of simplicity, in this example we assume that the space consists of only three dimensions. In this example, points p_1 a nd p_2 represent two shipments. Both of these points are expected to be outliers in the safe and risky subspaces. The safe and risky outliers' factors for point p_2 is expected to be relatively the same, since this point is located in the middle between the two subspaces. However, point p_1 is located closer to safe subspace than the risky subspace, and therefore it might be considered as safe point.

Any point with relatively the same safe and risky outlier factors is considered an undecidable point (shipment). Figure 6-3 highlights the steps of the risk assessment process. This process starts by calculating the safe outlier factor (s_f), and (2) the risky outlier factor (r_f) for the new point (p) (lines 2-3). Then, we calculate the absolute difference between the global risk and safe factors (g) (line 4). This gap is used to determine if the new shipment (p) has enough distinct features to be classified as safe or risky, by the current assessment stage (manufacturer or shipping agent). This analysis is performed by comparing this gap (g) against the threshold value (t). This threshold represents the

minimum possible acceptable gap between these two factors in order to classify the shipment. In situations where the gap is less than or equal to the threshold ($g \leq t$), the point is considered undecidable (line 5), since, in this situation, the global assessment factors do not clearly identify the riskiness status of the shipment. To classify this shipment as safe, this gap must be greater or equal to the threshold, and the safe factor must be smaller than the risk factor. A shipment is classified as risky when the safe factor is greater than the risk factor by at least *t* value.

The threshold is introduced as a controlling parameter, where increasing the value of this threshold is expected to reduce the number of misclassified shipments. Furthermore, increasing this threshold increases the number of undecidable shipments. However, in this method, we are mainly concerned with reducing the percentage of misclassified shipments, since the undecidable shipments are expected to be re-classified using the centralized assessment strategy deployed at customs administration.

classificationProcess $(\boldsymbol{p}, \boldsymbol{type}, \boldsymbol{t})$

input: $\boldsymbol{p}$ $(point\ to\ examine)$, $\boldsymbol{t}(threshold)$
type(Manufacturer or shipping agent)
output: ***label*** $(u: undecidable, r: risky, s: safe)$

1 $h \leftarrow History(type)$
2 $s_f \leftarrow LOFSafe(h, p)$,
3 $r_f \leftarrow LOFRiskey(h, p)$
4 $g \leftarrow |s_f - r_f|$
4 **If** $g \leq t$ **then**
  $label \leftarrow u$
5 ***Else if*** $r_f > s_f$ ***then***
  $label \leftarrow s$
6 ***Else***
  $label \leftarrow r$
8 **Return** *label*

Figure 6-3 The Classification Process

6.3.3. The Centralized Risk Assessment Step

Once a shipment is classified as undecidable, the information will be sent to the centralized risk assessment step for further analysis. In this step, since the basic shipment features selected by the distributed risk assessment step was not able to clearly classify the shipment, additional shipment features will be considered during the analysis. In this step, each shipment is represented using the following features: (1) HS-code, (2) original port of loading, (3) value, (4) CIF value, (5) shipping agent identification number, (6) country of origin, (7) the last port of loading the shipping route.

The centralized risk assessment step employs the well-known Random Forest Classifier (Macedo, 2018). This classifier is an ensemble learning technique that work by establishing several decision trees. In this classifier, each decision tree will produce a label for the new shipment (safe or risky), where eventually the label that has been selected by the majority of the trees will be confirmed as the shipment label.

6.4. Evaluation

The efficiency of the presented method is evaluated using several sets of experiments. The input data used in these experiments are obtained from the service innovation department at Dubai Customs. The used data consists of 500,000 shipment declaration applications submitted to Dubai Customs (sea channel). These applications are already labelled as either risky or safe based on the outcome of the inspection performed by the customs administration. These declaration applications consist of 0.5% risky shipments. The declaration applications are pre-processed to extract the required information for the value manipulation and undeclared goods risks assessments. In the presented experiments, 70% of the applications are used to represent the historical data. Whereas, the rest 30% of the

applications are used for testing purposes. To capture the impact of the threshold (t) on the proposed method performance, we performed these experiments while varying the value of this threshold.

Beside accuracy, the used performance metrics in these experiments are precision, recall, and F1-score. If the attention is on the risky classification results. Precision is defined as the percentage of correctly classified risky shipments.

Where TP (true positive) refers to the number of correctly classified risky shipments, and FP (false positive) refers to the number of safe shipments that are wrongly classified as risky shipments. In this work, since undecidable shipments are assumed to be re-classified at the customs administration, shipments with undecidable status are not considered during the calculation of the accuracy, precision, recall, and F1-score.

Recall is defined as the percentage of correctly identified risky shipment over the total number of risky shipments.

The value of this score range from zero to one, where the best accuracy occurred when the value of this score is one.

6.4.1. Results

The results presented in this section is divided into two parts. In the first part, we evaluate the performance of the first decentralized risk assessment stage. Then, we present the results for the entire proposed method (decentralized and centralized stages).

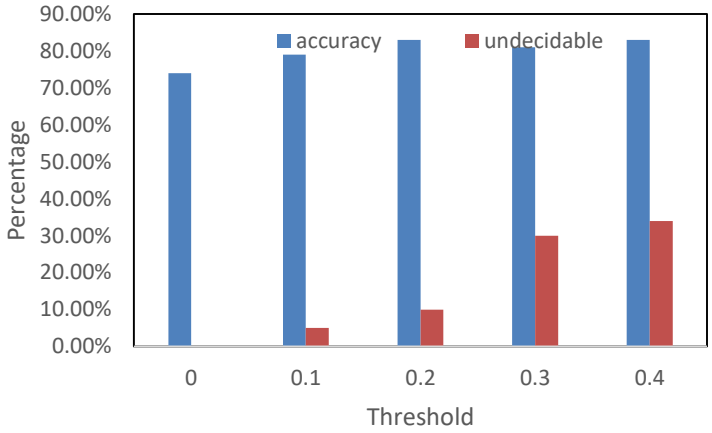

Figure 6-4 Threshold Value Against The Accuracy and the Undecidable Shipments Percentages

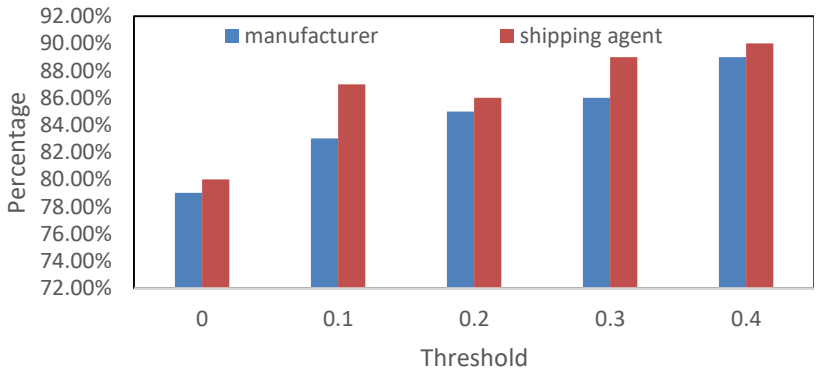

Figure 6-5 Threshold Value Against the Percentage of Risky Shipments Captured by the Manufacturer and the Shipping Agent Assessment Stages

6.4.1.1. Decentralized Risk Assessment Step

To investigate the impact of the threshold value on the accuracy and the percentage of the undecidable shipments, we ran the experiment while varying the value of the threshold. Figure 6-4 shows the results of this experiments. The result show that increasing the threshold value results in increasing the accuracy. This is expected, since increasing the threshold result in increasing the percentage of shipments, which are labeled as undecidable, and this increases the probability of correctly classifying the rest of the shipments. Additionally, increasing the threshold value results in increasing the acceptable gap between the shipments safe and risked outlier factors, and therefore the selected shipments will be expected to have more distinct features that simplify the classification process.

Next, to clarify the percentage of truly risky shipments detected by each risk assessment stage, we ran the experiment while varying the threshold values (Figure 6-5). The results show that the shipping agent risk assessments stage (undeclared goods risk) is always capable of detecting at least the same percentage of risky shipments as the manufacturer stage (value manipulation). This emphasis the relationship between the two risk categories. In the manufacturer risk assessment stage, the objective is to detect the manipulation in the original invoice submitted by the manufacturer (value manipulation risk). In the shipping agent risk assessment stage, the objective is to detect any abnormality in terms of the shipping route. In this direction, shipment declarations that is labelled by the shipping agent risk assessment as risky is more likely to be also labelled as risky by the manufacturer risk assessment.

This is established, since the shipments with undeclared goods risk is expected to use fraudulent manufacturer documents. On other hand, shipments declarations with value

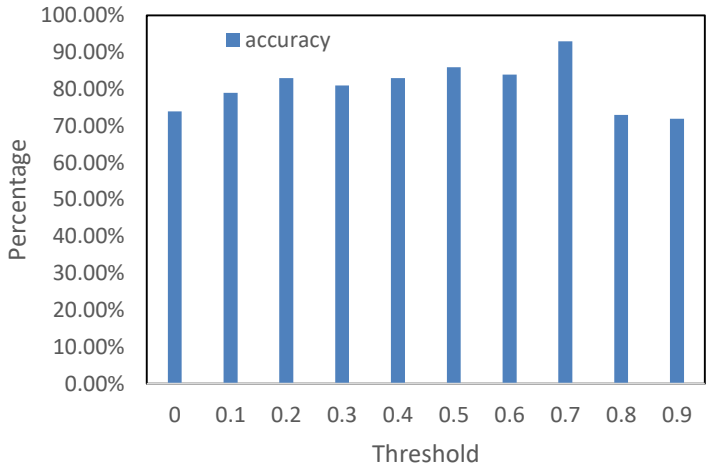

Figure 6-6 Threshold Value Against the Accuracy Percentages

manipulation risk is not necessary expected to have undeclared goods risk, since most cases of this risk type deals with manipulating the information to avoid paying duties.

6.4.1.2. Decentralized and Centralized Risk Assessment Steps

Table 6-1 Performance Measures (Hybrid)

Performance measures

	Precision	recall	F1-score
Risky	89%	96%	92 %
Safe	96%	88%	92 %

Once the decentralized risk assessment stage has been performed. All of the undecidable shipments will be sent to the centralized risk assessment stage for re-classifying. Next, to

investigate the accuracy of the proposed method, we ran the experiment while varying the value of the threshold. Figure 6-6; show the results of this evaluation. From the results we can see that the value of the threshold has a major impact on the accuracy of the proposed method. Increasing the value of this threshold to over 0.1 results in increasing the accuracy of the proposed method. Additionally, as we can see from the figure, increasing the value of the threshold to 0.9 results in reducing the accuracy. To understand this behavior, let us clarify the relationship between the threshold value and performance of the proposed method. Increasing the value of the threshold result in increasing the number of shipments that are classified as undecidable. Having relatively high number of undecidable shipments increases the pressure on the centralized risk assessment stage. Whereas, reducing the threshold value, increase the demand of classification on the decentralized risk assessment stage. These are the main factors behind the seen performance results.

Next, we present the proposed method (the two stages) in term of accuracy factors (precision, recall, and F1-score), we ran the experiments for threshold values equal to 0.5. In these experiments, we calculate the performance factor, for both the risky and safe classification. The results of this experiments are shown in Table 3. From the results, we can see that the precision score for the safe shipment classifications is 96%, where the precision for the risky shipment classification is 89%. The presented result suggests that the proposed method is able to detect safe shipments more efficiently compared to safe shipments. This is expected, since safe shipments is expected to have clearly distinct features. Additionally, from the results we can see that percentage of misclassified risky shipment is higher than the percentage of misclassified safe shipments. This results in increasing the operational time, since these safe shipments that are classified as risky

shipments will be physically inspected. However, this is relatively acceptable compared to the situations where risky shipments are classified as risky.

One of the main advantages of this methods is that news risk assessment stages can be designed and deployed without interrupting the rest of the stages. In addition, since we assume that the method is implemented on-top of blockchain solution for international trade, any risk assessment stage can be modified by simply deploying a new smart contract to replace the current active one. The mechanism of adopting the threshold strategy aim to take advantage of the fact that regardless of the deployed distributed risk assessment method, the centralized risk assessment strategy is also required to be deployed at the custom administration. Beside re-examining risky classified shipments, this centralized risk assessment functionalities are designed to capture the intelligence information provided by external departments (Interpol and police department).

6.5. Conclusion

In this chapter, we proposed hybrid risk assessment method, which consists of distributed and centralized risk assessment steps. The distributed risk assessment step aims to reduce the pressure on customs administration by performing early stage risk assessment. Using this step, points are classified to either safe, risky, and undecidable. The undecidable point (shipments) are re-classified using the centralized risk assessment step. The results show that the proposed method is able to achieve around 90% accuracy.

7. Chapter 7: Discussion

7.1. Introduction

The work in this thesis tackles formalities relative to the trade supply chain and addresses challenges present at different stages and across various parties involved. These challenges result in major economic damages suffered by various nations and businesses.

Illegitimate trade activities occur at a global scale and have a negative impact on the countries affected. This is where nations need to establish reliable risk assessments which encompass the process of analyzing shipment information and tracking shipments in order to identify any suspicious transactions or activities. The ability to validate information and documents provided by supply chain actors is crucial in reducing risks and operational burden.

7.2. Discussion

Taking the current complex situation into consideration, we plan to design algorithmic solutions that automate the process of verifying documents and ensure the legality of transactions. This information sharing mechanism and documentary exchange are a dominant factor in determining the overall efficiency of the end-to-end process in the supply chain. Blockchain technology has emerged as a promising approach for the optimization of the international trade supply chain. By using this technology, the privacy and integrity of the exchanged information are guaranteed. In addition, blockchain technology comprises an information-sharing mechanism that guarantees data immutability and traceability. This, in turn, can establish a trusted communication model

between the supply chain participants and guarantee that the customs authority will receive the required information on time.

Another factor impacting customs authorities and the trade supply chain is monitoring the flow of goods entering the country to detect counterfeit products and smuggling activities. This is where a solid risk assessment methods and techniques should be deployed to identify any deviations from normal activities. Outlier detection is a density-based algorithm (also known as anomaly detection) used to capture exceptional cases that deviate substantially from the majority of patterns. It is the process of finding data objects with behaviors that are very different from expectation. Such objects are called outliers or anomalies. This algorithm will support the blockchain solution by establishing must needed measures of security and compliance.

7.3. Answers to Research Questions

7.3.1. RQ1: Can Blockchain Address Customs Challenges Relative to Import and Export Information Exchange to Mitigate Authenticity Issues?

We conducted a PoC for a novel blockchain-based solution in chapter 3 to optimize the operating model at Dubai Customs for various importation and exportation scenarios. The solution seeks to simplify the processes entailed in both kinds of scenarios and to establish direct, tamper-proof, information-sharing mechanisms for actors in international trade supply chains. To those ends, the proposed model consists of several components that chiefly target the processes of shipment clearance, auditing, and risk assessment.

Several proposals utilized the inherited features of the blockchain technology to address various challenges and optimize several application domains such as health (Jiang, et al.,

2018), agriculture (Hua, et al., 2018), and trade (Casado-Vara, et al., 2018) among others. These proposals have touched the surface on some of these challenges and did not cover the full end-to-end formalities of trade and sets the foundations for the future trade supply chain. The proposed blockchain-based solution tackled the majority of the issues and challenges faced by the trade supply chain parties at the origin and destination that creates a holistic single source of truth for all partners working together to support the common goal of stopping fraudulent activities.

Fraudulent activities will continue to worsen the situation so long as information being exchanged is easily breached and manipulated to evade authorities and make illicit financial gains. These conditions highlight the importance of ensuring data integrity while reducing integration burden. Though there are many approaches to achieve these objectives, none is able to produce a high level of assurance equivalent to the proposed blockchain-based solution with risk management and its core. The scenario that we addressed in this framework tackles a prevalent number of vulnerabilities associated with the cross-border trade supply chain.

The distributed nature and immutability features available in blockchain made it feasible for organizations and businesses to deliver services end-to-end in collaborative fashion. The PoC conducted indicates how we can shift from negative economic and administrative dip to a 100% positive outcome for all participating parties.

The proposed PoC resulted in substantial decrease in number of reported cases in cross-border luxury cars theft in the city of Dubai by 88.65% in 2018 according to the statistics

provided by Dubai Customs. This amounted to time saving of 99% and cost saving of 69% by shifting to the proposed solution and adopting the features that come with it.

This problem will continue to be aggravate the situation the more sophisticated criminal networks become. Thus, the inherited features of blockchain technology will eliminate technical problems associated with sharing of data and integrity of it and it ensure that we stay ahead of criminal networks.

7.3.2. RQ2: Can we Develop Methods that Result in the Reduction of Smuggling Activities and Raise Risk Assessment Accuracy as Part of a Blockchain-based Global Trade Formalities?

We proposed two different methods to address risk related analysis and employed well-known outlier detection and random forest learning algorithms to detect and predict whether the import shipments are considered risky (outlier) or safe. Outlier detection is used to capture exceptional cases that deviate substantially from the majority of patterns. It is the process of finding data objects with behaviors that are very different from expectation. Such objects are called outliers or anomalies. Outlier detection algorithms has advanced the detection of abnormal activities in many application domains such as network traffic intrusion (Huang, et al., 2013; Huang, et al., 2015), money laundering (Gao, 2009; Chen, et al., 2007) and fraud detection (Sharmila, et al., 2019; Malini & Pushpa, 2017; Badriyah, et al., 2018), fake news and misinformation, healthcare analysis, security and surveillance and more.

We addressed the risk related problems in chapters 5 and 6, in the proposed model we propose a lightweight algorithm method that reduces the complexity of the risk assessment

by highlighting factors in the classification of shipments as risky. In chapter 5, we propose a secondary distributed risk assessment method that provides customs administration with online risk assessment capabilities. The proposed method complements the risk assessments performed at customs administration by providing feedback from the early stage of risk analysis. The results show that the proposed method can provide classification that is 83% accurate on average.

With the distributed risk assessment method proposed in chapter 5, the assessment handled general purpose shared risks. This raised some limitations relative to party specific risks handling. To improve the performance of the proposed method in chapter 5 and to provide an early stage of risk analysis, an extension in chapter 6 of the work done in chapter 5 included adding the centralized risk assessment step, and restructuring the decentralized risk assessment step. In this extension, we extend the work conducted in chapter 5 and propose a hybrid risk assessment method that consists of distributed and centralized risk assessment processes. The distributed process provides the customs administration with online risk assessment capabilities about the shipment in several stages during the trade supply chain. This distributed process complements the centralized risk process triggered at the customs administration by providing an early stage of risk analysis information. The results show that the proposed method achieved around 90% accuracy. The reported performance achieved significant results compared to similar approaches in other proposals (Huang, et al., 2013; Huang, et al., 2015; Gao, 2009; Chen, et al., 2017; Sharmila, et al., 2019; Malini & Pushpa, 2017; Badriyah, et al., 2018).

With the best attempts of experts and reliance on traditional tools, there were still outcomes that were not highly reliable. This has led to a large number of false positives and some

true negatives. This situation called for an advanced scientific method to detect where true abnormal activities really lie. This is where the outlier detection algorithms were needed to provide the required insights into protecting border security and fraudulent activities.

By taking birds eye view for all obstacles and challenges facing the trade supply chain whether it is a document or activity related risk, we proved from the experiments with the utmost certainty that by employing leading edge advance technology along with scientific fraud detection algorithms, we are transforming the trade supply chain and supporting economic sustainability.

7.4. Conclusion

This chapter provide discussion on the key findings of the overall aims and objectives. Risk assessment is critical for identifying suspicious activities. Raising the level of true-positives reduces the operational burden and drives competitive advantage. This can be observed in the results achieved in the proposed solution.

8. Chapter 8: Conclusion and Future Works

8.1. Conclusion

Nations around the globe are focused on trade facilitation to compete in the trade supply chain. Trade is a key determinant of a country's economic viability, eliminating unnecessary cost and procedural challenges will ensure delivery of effective trade services. The formalities applying to the trade supply chain are often complex, time consuming and inefficient. Barriers can result from inefficient procedures, regulations and infrastructure services, among many others. The speed and ease with which cross-border business transactions are conducted dictates having a high degree of quality to achieve efficiency in trade procedures. The reduction of barriers is highly critical in ensuring the legitimacy of trade. This involves elimination of fraudulent activities, resource waste and reducing costs on trading firms, consumers and society.

The current COVID-19 pandemic hit the world hard in many ways and forced a near total shutdown of global trade supply chain. Economies faced the risk of collapse in turn governments resorted to pushing for return of business to normal while they have not weathered the risk of further loss of life. This is where the proposed blockchain platform accentuates the need for organizations and governments to improve the integrity, trust, transparency and provenance of various supplies especially pharmaceutical products and medical supplies, in addition to food, goods and industrial and consumer products. To develop future pandemic preparedness and accelerate economic rally, resilience in supply chains can be improved through the responsible deployment of blockchain technologies as proven in the proposed methodology.

Today, counterfeit goods and products is a growing problem in the international trade domain. Counterfeits and pirated goods have a major impact on world market. It is estimated the imports of counterfeits are worth half a trillion dollars a year amounting to 2.5% of global imports. On the other hand, reports indicate that the counterfeit market today including online piracy generates returns of up to $600 billion annually. This amounts to $600 billion losses for businesses from across the world. This has major adverse influence on the sales and profits of firms as well as on revenue, security, economy, health, safety and environment. This is a major concern for governments, businesses and consumers. Fake goods reaching consumers and markets are a global problem. Counterfeiting produces copies that endanger lives: faulty products or parts, medicines that make people sick, harmful toys, zero nourishment baby formula and instruments delivering false readings. Parties have to make sure authentic goods are sold and delivered to the consumers and can identify authentic products and avail to consumers where they can obtain them. Improving traceability of physical goods by creating an auditable and tamper-proof record of the journey behind all products across the supply chain. By preventing the selling of fake goods and counterfeits many benefits will be realized by businesses, society and the environment.

These barriers arise due to the fact that the global trade supply chain operating model is paper-based resulting in difficulties, costs, discrepancies and counterfeit products. The risk of documentary fraud demands proper mitigation that leads to the reduction of reconciliation transaction cost between and within the participating parties. The economic impact is felt by many countries and action is required to ensure the current barriers do not impact their GDP. Authorities and businesses must immediately collaborate on effective

ways and mechanisms to eliminate supply chain barriers and encourage participation of small and medium-sized enterprises. This can come as a system of trade in which trust, transparency, authenticity and traceability can be guaranteed. Furthermore, government and in particular customs authorities have a major responsibility to mitigate these problems and ensure the legitimacy of trade activities.

From a customs authority perspective, having detailed information about a shipment/consignment is crucial to assist in determining the risk factors associated with that particular shipment or consignment. Without accurate information that helps the authority in trusting the data at hand operational activities will create a number of issues and delays for both the authority and the trader. The costly alternative would mean physically inspecting 100% of shipments crossing the border which would defeat the facilitation aspect. This method is not feasible for countries trying to compete in the highly competitive trade domain.

Furthermore, Procedures, formalities and mechanisms that help simplify and standardize information flows related to the import and export of goods can help reduce or eliminate un-necessary steps and improve transparency. Reducing operating costs remains the most frequently pursued goal. Consequently, countries that do not pursue certain reforms will incur additional costs due to barriers and may discover a reduction in their volume of trade.

In this work, we explored the benefit of designing a customs-based blockchain solutions to ensure the legitimacy of trade and simplify the trade formalities.

Blockchain is considered to offer large potential for improving processes and enhancing business models in the trade, transport, logistics and supply chain management. Connecting

all members of the supply chain to a decentralized network and allowing them to exchange data and documents in a secure and trusted manner is what blockchain promises to provide.

Blockchain technology is said to guarantee trade integrity, secure global supply chains and protect revenues. Additionally, it provides critical factors to all parties involved:

- Real-time visibility and control
- Strengthens law enforcement capacity
- Helps in meeting regulatory requirements
- Cost effectiveness, security and privacy

Blockchain technology, is a distributed ledger where each participating party has his own identical copy of the entire transaction history. The ledger is stored as a group of connected blocks each having a set of transactions. Blocks are connected together through hashing mechanism. A block hash value is obtained through the use of a hash function, which receives the entire block as input and returns a fixed length that has a value. Each block stores the hash values of itself and the previous block. Therefore, at any time, changing the data of one block will result in changing the hash value of the block, and therefore it will no longer match the hash value stored in the next block. Through the use of hashing, we can ensure the integrity of the data (ledger), since it simplifies the process of detecting any manipulation in the data. This mechanism is highly important in ensuring authenticity of the trade information being exchanged which eliminates intentional manipulation of data and reduces illegitimate trade activities. Through the use of a consensus method the integrity of the data can be ensured. It is no surprise that the trade supply chain is investigating the potential of this technology, particularly in the context of exchanging the

paper-based documents required at every step of the trade journey. The ability to connect all carriers, banks, forwarders, traders and other parties of the international trading supply chain to ensure compliance and gain control is the desire of the trade industry. Managing provenance and ownership of documents on the blockchain eliminating disputes, forgeries and unnecessary risks are what is anticipated with the blockchain technology (Allen, et al., 2019).

Therefore, this thesis presents blockchain solutions that can be used to address the following barriers: (1) Counterfeit goods, (2) forged trade documents, and (3) time and cost of goods clearance from a customs perspective. Accordingly, in this work the contribution is two-fold (1) Develop a blockchain-based approach to address the importation and exportation and ensure information authenticity from customs perspective. (2) Develop a lightweight algorithmic method to be used by the blockchain-based approach for the detection of smuggling activities.

The presented blockchain-based approach aims to automate the process of exportation and validating the exporting document. Due to the current demand at Dubai Customs we have used the car exportation process as a use-case to test and validate the proposed approach. In this use-case, we are dealing with several parties consisting of the Road and Transport Authority, Dubai Police, Rental Companies and Banks connected together with Dubai Customs using a blockchain based solution. In this direction, once a trader requests the clearance to export a car the blockchain solution will verify the information provided by the trader with all parties connected to the blockchain solution. This helps, in eliminating the problem in exporting luxury cars using fake documents.

The proposed risk assessment method consists of two phases; (1) Behavioral Assessment and (2) Features Assessment. In the behavioral assessment we look at shipments from a density perspective to determine the risk factor which can either be risk-free, risky or un-decidable. In other words, we determine whether a shipment is common or not. The main idea of the first phase is to perform risk assessments for shipments at two stages of the international trade supply chain—at the manufacturer and at the shipping agent—both of which can allow the capture of value manipulation risks and undeclared goods risks. Risks related to value manipulation can be assessed by analyzing the manufacturer's information (e.g. invoice and country of origin), while undeclared goods risks can be assessed using information related to the shipment's path and type. For each type of risk assessment, the proposed method represents the shipment's information as points in multi-dimensional space consisting of two kinds of subspace: safe and risky. Risky subspace encompasses shipments whose risks have been identified and confirmed, whereas safe subspace encompasses ones without any identified risks. The dimensions of each space represent the parameters used to analyze the type of risk. For instance, for value manipulation risk, assume that the parameters, also used during the risk analysis, are the invoice value ($), goods type, and country of origin, each of which can be represented as a dimension in the value manipulation space. The first phase classifies shipments to risky, safe, and un-decidable. The Un-decidable shipments will become the input for the second phase. And these shipments do not have density information to be accurately labeled by the first phase. In the second phase, the un-decidable shipments are classified using predictive machine learning model which uses the entire shipments features to establish the classification labels. By the entire features we refer to the attributes used in the value manipulation and

undeclared goods risk assessment stages. The results show that the method can provide classifications that are 93% accurate on average. These results are unprecedented when it comes to risk assessment and paves the way for a major transformation in the shipment clearance space. This will aid customs authorities to achieve their objectives relative to ensuring compliance while facilitating cross-border trade. This will enable authorities to secure borders and protect their local societies in a seamless risk-free fashion. With this method in place, a number of barriers associated with trade activities will be something of the past. Thus, we belief that we are on the verge of revolutionizing the role of customs authorities and the global trade supply chain altogether.

Despite the promise that blockchain will revolutionize the way we handle business transactions and the supply chain operating model, adopters face a number of challenges. One of these challenges is the fact that different industry players are working as separate alliances, consortiums or networks on implementing blockchain using different Hyperledger fabrics. Currently, a number of these initiatives are in place, the TradeLens program spearheaded by IBM and Maersk, the Global Shipping Business Network, and the Blockchain in Transport Alliance. Although, they lack interoperability due to their own unique data protocols, rules and processing approach; the language they speak is unique to their specific initiative. With major industry players joining differing blockchain camps they are unable to integrate across the global supply chain. This leads to re-establishing industry or supply chain silos. However, for this challenge to be rectified an international body must be established to cooperate and coordinate between the various private and public stakeholders to work on establishing a common standard. Otherwise, the scalability of interoperability will not deliver the desired value for the supply chain parties. Recently,

a group of digital leaders from Maersk, CMA CGM, Hapag-Lloyd, MSC and ONE initiated discussions on the creation of common information technology standards. Without a common information standard to address the integration between the different fabric needs, cross-network communication is impossible. Therefore, it's highly critical for the various network participants to work together on establishing a standard mapping layer to enable cross-network data exchange. It is therefore in the national interest of policymakers to inspire further cooperation, initiate discussions, and even encourage experimentation in this domain.

8.2. Implications

The carried out work in this thesis has allowed proper, secure information sharing and risk assessment mechanisms. Documents verification to prevent fraud and counterfeiting is an exceptionally costly and time-consuming activity. Because actors in international trade supply chains do not communicate with each other directly, customs authorities may ask customers to provide additional documentation that can verify documents already submitted. Additionally, because customs regulations vary from country to country, whether certain goods are permitted or prohibited by customs authorities also varies, while some goods may be allowed to enter countries provided that they have a special permit from government authorities. In the current operating model, although customers are expected to promptly provide all required permits for processing, delays in submitting the required documents are common and invariably prolong processing and raise shipment costs.

The lack of communication among actors in international trade supply chains reduces the efficiency of the current trade model. In particular, the semi-isolation of actors can result

in the failure of customs authorities to identify fraudulent documents, which allows unhealthy products to enter communities and potentially cause harm to society. Such failure can also result in the trade of counterfeit products, which can significantly affect local economies, as well as reduce customs revenue, because documents may have been altered to lessen duties. At the same time, the lack of communication also lengthens processing times and increases shipment costs, which intensifies pressure placed upon traders and, as a result, can reduce the volume of trade.

In this work, we propose a novel blockchain-based solution to optimize the operating model at Dubai Customs for various importation and exportation scenarios. The solution seeks to simplify the processes entailed in both kinds of scenarios and to establish direct, tamper-proof, information-sharing mechanisms for actors in international trade supply chains. To those ends, the proposed model consists of several computational components that chiefly target the processes of shipment clearance, auditing, and risk assessment.

The proposed computational model is designed to optimize the processing components used in international trade supply chains as a whole. That objective is driven by the need to fully automate customs authority-related processes in order to help customs authorities to facilitate trade while protecting society. The architecture of the model should ensure the simplicity of adding and modifying functionalities, which is possible by virtually dividing the presented model into layers such that each layer contains functionalities corresponding to the specific objective. In that way, any component will be able to be rewritten without significantly affecting the overall architecture.

The functionalities of risk assessment encompass the process of analyzing shipment information and tracking shipments in order to identify any suspicious transactions or activities. Risk assessment is typically performed by customs authorities in a centralized fashion. In that process, whenever information concerning a new shipment becomes available, it is entered into the risk assessment engine to examine the shipment, which involves comparing the shipment's features (i.e. attributes) with available historical data as part of following a learning-based model. Consequently, the accuracy of the assessment depends upon the historical data provided and the number of attributes—up to 120—that can be used to describe each shipment and transaction. In that sense, the model is complex in terms of computational requirements, and any irregularity in shipping activity heightens the pressure on customs authorities to provide and perform reliable services in a timely manner. Moreover, once a shipment is declared to be risky, then several time-consuming manual processes are required to clearly identify the source of the risk.

To address this problem, in the proposed model we propose a lightweight algorithm solution that reduces the complexity of the risk assessment by highlighting factors in the classification of shipments as risky. As an online algorithm, the solution involves performing risk assessment at different stages of supply chain when any actor submits shipment information to the blockchain. For instance, once a manufacture uploads an invoice to the blockchain, then risk assessment can be performed on the information in the invoice (e.g. amount and type of good). Such assessment will return an outlier factor that can be directly submitted to customs authorities via the proposed model to inform their identification of suspicious shipment. In particular, high outlier factors (e.g. 10) increase suspicion about the shipment more than low ones (e.g. 3).

The principal idea of the proposed solution is to divide the space for historical data into safe and risky compartments for each supply chain actor (e.g. manufacturers and shipping agents). Once new shipment information is received by one of those actors, the algorithmic approach will identify the space with the most similar behavior among past shipments. The outlier factor for the shipment will be calculated to determine whether it should be treated as risky. A major advantage of the approach is that customs authorities will analyses the outlier factors of shipments at early stages of the shipment's life, which will afford authorities more time to perform detailed analyses.

Though blockchain technology will transform trade it is still in its infancy. Wider public and private sector adaptability, cross-fabric interoperability, and a policy environment is essential for realizing the potential benefits and value of blockchain. We hope that this work spurs further empirical research in this area.

8.3. Future Works

In this work, we proposed hybrid risk assessment method, which consists of distributed and centralized risk assessment steps. The distributed risk assessment step aims to reduce the pressure on trade supply chain parties by performing early stage risk assessment. The results show that the proposed method is able to achieve around 90% accuracy.

Additionally, we are planning to investigate the possibility of improving the accuracy by adopting other ensemble learning method in the centralized risk assessment step. Furthermore, advances in technology can have major potential to further increase the efficiency and effectiveness across the supply chain. This will be a staged out approach in which we can complement the blockchain solution with an AI-based risk assessment methodology that can predict risks and allow supply chain parties to act in pro-active mode instead of re-active.

References

Ahrenholz, J., Claudiu, D., Thomas, H. & Jae, K., 2008. *CORE: A real-time network emulator*. s.l., In MILCOM 2008-2008 IEEE Military Communications Conference.

Aitzhan, N. Z. & Svetinovic, D., 2018. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Transactions on Dependable and Secure Computing,* 15(5), pp. 840-852.

Allen, D. W. et al., 2019. International Policy Coordination For Blockchain Supply Chains. *Asia & the Pacific Policy Studies,* 6(3), pp. 367-380.

Alzahrani, N. & Bulusu, N., 2018. *Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain.* Munich, 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock'18.

Androulaki, E. et al., 2018. *Hyperledger Fabric Hyperledger Fabric: A Distributed Operating System For Permissioned Blockchains.* Porto, Thirteenth EuroSys Conference.

Badriyah, T., Rahmaniah, L. & Syarif, I., 2018. *Nearest Neighbour and Statistics Method based for Detecting Fraud in Auto Insurance.* Batam, International Conference on Applied Engineering (ICAE).

Baralla, G. et al., 2018. *A Blockchain Based System to Ensure Transparency and Reliability in Food Supply Chain.* Turin, Euro-Par 2018: Parallel Processing Workshops, pp. 379-391.

Bauder, R., Da Rosa, R. & Khoshgoftaar, T., 2018. *Identifying Medicare Provider Fraud With Unsupervised Machine Learning.* Salt Lake City, UT, IEEE International Conference on Information Reuse and Integration (IRI).

Belu, M. G., 2019. Application of Blockchain in International Trade: An Overview. *The Romanian Economic Journal,* XXII(71), pp. 2-16.

Blackstone, E., Fuhr, J. P. & Pociask, S., 2014. The Health and Economic Effects of Counterfeit Drugs. *American Health & Drug Benefits,* 7(4), pp. 216-244.

Blockchain Training Alliance (BTA), 2018. *Developing on Hyperledger Fabric,* s.l.: Blockchain Training Alliance (BTA).

Blocksplain, 2018. *Blockchain Speeds & The Scalability Debate.* [Online].

Bocek, T., Rodrigues, B. B., Strasser, T. & Stiller, B., 2017. *Blockchains Everywhere - A Use-Case Of Blockchains In The Pharma Supply-Chain.* Lisbon, IFIP/IEEE Symposium on Integrated Network and Service Management (IM).

Breunig, M. M., Kriegel, H.-P., Ng, R. T. & Sander, J., 2000. *LOF: Identifying Density-Based Local Outliers.* Dalles, TX, ACM SIGMOD 2000 International Conference On Management Of Data.

C. Technologies, 2018. *Blockchain (E-Book),* s.l.: s.n.

Cachin, C., 2016. *Architecture of the Hyperledger Blockchain Fabric.* Chicago, Distributed Cryptocurrencies and Consensus Ledgers "DDCL 2016".

Casado-Vara, R., Prieto, J., De la Prieta, F. & Corchado, J. M., 2018. How Blockchain Improves The Supply Chain: Case Study Alimentary Supply Chain. *Procedia Computer Science,* Volume 134, pp. 393-398.

Chang, Y., Iakovou, E. & Shi, W., 2019. 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*, pp. 1-18.

Chen, M.-C., Wang, R.-J. & Chen, A.-P., 2007. *An Empirical Study For The Detection Of Corporate Financial Anomaly Using Outlier Mining Techniques.* Gyeongju, International Conference on Convergence Information Technology (ICCIT 2007).

Chen, S. et al., 2017. *A Blockchain-Based Supply Chain Quality Management Framework.* Shanghai, IEEE 14th International Conference on e-Business Engineering (ICEBE).

Chen, T. & Guestrin, C., 2016. *XGBoost: A Scalable Tree Boosting System.* San Francisco, 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.

Cui, Y. & Idota, H., 2018. *Improving Supply Chain Resilience with Establishing A Decentralized Information Sharing Mechanism.* Saint-Etienne, 5th Multidisciplinary International Social Networks Conference.

Engelenburg, S. V., Janssen, M. & Klievink, B., 2017. 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*, Volume 52, pp. 595-618.

Etherscan, 2019. *Etherscan.* [Online] Available at: https://etherscan.io/

Gan, Z. & Zhou, X., 2018. *Abnormal Network Traffic Detection Based on Improved LOF Algorithm.* Hangzhou, 10th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC).

Gao, Z., 2009. *Application of Cluster-Based Local Outlier Factor.* Wuhan, International Conference on Management and Service Science.

Guo, Y. & Liang, C., 2016. Blockchain Application And Outlook In The Banking Industry. *Financial Innovation,* 2(24).

Gupta, A., 2014. E-Commerce: Role of E-Commerce In Today's Business. *International Journal of Computing and Corporate Research,* 4(1).

Hepp, T., Wortner, P. & Schönhals, A., 2018. *Securing Physical Assets on the Blockchain Linking a novel Object Identification Concept with Distributed Ledgers.* Munich, 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock'18.

Ho, T. K., 1995. *Random Decision Forests.* Montreal, 3rd International Conference on Document Analysis and Recognition.

Hua, J. et al., 2018. *Blockchain Based Provenance for Agricultural Products: A Distributed Platform with Duplicated and Shared Bookkeeping.* Changshu, IEEE Intelligent Vehicles Symposium (IV).

Huang, S.-Y., Yu, F., Tsaih, R.-H. & Huang, Y., 2015. *Network-Traffic Anomaly Detection With Incremental Majority Learning.* Killarney, International Joint Conference on Neural Networks (IJCNN).

Huang, T. et al., 2013. *An LOF-Based Adaptive Anomaly Detection Scheme For Cloud Computing*. Japan, IEEE 37th Annual Computer Software and Applications Conference Workshops.

Hung, P., Li, H. & Jeng, J.-J., 2004. *WS-Negotiation: An Overview Of Research Issues.* Big Island, 37th Annual Hawaii International Conference on System Sciences.

Imeri, A. & Khadraoui, D., 2018. *The Security and Traceability of Shared Information in the Process of Transportation of Dangerous Goods.* Paris, 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS).

Innes, J. & Falconer, M., 1995. A survey of activity-based costing in the UK's largest companies. *Management accounting research,* 6(2), pp. 137-153.

Jiang, S. et al., 2018. *BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange.* Taormina, Sicily, IEEE International Conference on Smart Computing (SMARTCOMP).

Juma, H., Shaalan, K. & Kamel, I., 2019a. A survey on using blockchain in trade supply chain solutions. *IEEE Access*, Issue 7, pp. 184115-184132.

Juma, H., Shaalan, K. & Kamel, I., 2019b. Customs-based Blockchain Solution for Exportation Protection. *In International Symposium on Parallel Architectures, Algorithms and Programming (pp. 405-416). Springer, Singapore*..

Juma, H., Shaalan, K. & Kamel, I., 2019c. Customs-Based Distributed Risk Assessment Method. *In International Symposium on Parallel Architectures, Algorithms and Programming (pp. 417-429). Springer, Singapore*..

Kamath, R., 2018. Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. *The JBBA,* 1(1), pp. 47-53.

Kang, E. S., Pee, S. J., Song, J. G. & Jang, J. W., 2018. *A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid.* Nagoya, 3rd International Conference on Computer and Communication Systems (ICCCS).

Kumar, M. V. & Iyengar, N. C. S. N., 2017. A Framework for Blockchain Technology in Rice Supply Chain Management Plantation. *Advanced Science and Technology Letters,* Volume 146, pp. 125-130.

Kumar, N. & Jha, A., 2016. Pharmaceutical " Good Transportation Practices (GTP) " -An Innovative Concept In " GXP " Acronym. *American Journal of Pharmacy & Health Research,* 4(1), pp. 1-10.

Larik, A. S. & Haider, S., 2011. Clustering Based Anomalous Transaction Reporting. *Procedia Computer Science,* Volume 3, pp. 606-610.

Laszka, A. et al., 2018. *TRANSAX : A Blockchain-based Decentralized Forward-Trading Energy Exchange for Transactive Microgrids.* Singapore, IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS).

Lehmacher, W., 2017. *Why blockchain should be global trade's next port of call.* [Online] Available at: https://www.weforum.org/agenda/2017/05/blockchain-ports-global-trades/ [Accessed 10 November 2017].

Lehmacher, W. & Mcwaters, J., 2017. *How blockchain can restore trust in trade.* [Online] Available at: https://www.weforum.org/agenda/2017/02/blockchain-trade-trust-

transparency

[Accessed 18 November 2017].

Leng, K. et al., 2018. Research On Agricultural Supply Chain System With Double Chain Architecture Based On Blockchain Technology. *Future Generation Computer Systems*, Volume 86, pp. 641-649.

Li, B. & Wang, Y., 2018. *RZKPB: A Privacy-Preserving Blockchain-Based Fair Transaction Method for Sharing Economy.* New York, 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).

Liu, C. et al., 2018. Adaptive Blockchain-Based Electric Vehicle Participation Scheme in Smart Grid Platform. *IEEE Access*, Volume 6, pp. 25657-25665.

Li, Z. et al., 2017. Consortium Blockchain For Secure Energy Trading In Industrial Internet Of Things. *IEEE Transactions on Industrial Informatics*, 14(8), pp. 3690-3700.

Loklindt, C., Moeller, M.-P. & Kinra, A., 2018. *How Blockchain Could Be Adopted For Exchanging Documentation In The Shipping Industry*, Copenhagen: Copenhagen Business School.

Lu, Q. & Xu, X., 2017. Adaptable Blockchain-Based Systems: A Case Study for Product Traceability. *IEEE Software*, 34(6), pp. 21-27.

Macedo, L., 2018. Blockchain for Trade Facilitation: Ethereum, eWTP, COs and Regulatory Issues. *World Customs Journal*, 12(2), pp. 87-94.

Malik, S., Kanhere, S. S. & Jurdak, R., 2018. *ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains.* Cambridge, MA, IEEE 17th International Symposium on Network Computing and Applications (NCA).

Malini, N. & Pushpa, M., 2017. *Analysis On Credit Card Fraud Identification Techniques Based On Knn And Outlier Detection.* Chennai, Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB).

Mao, D., Hao, Z., Wang, F. & Li, H., 2019. Novel Automatic Food Trading System Using Consortium Blockchain. *Arabian Journal for Science and Engineering*, 44(3439–3455).

McDaniel, C. & Norberg, H. C., 2019. *Can Blockchain Technology Facilitate International Trade?,* Arlington: Mercatus Center.

Mengelkamp, E. et al., 2017. A Blockchain-based Smart Grid: Towards Sustainable Local Energy Markets. *Computer Science - Research and Development,* 33(1-2), pp. 207-214.

Meng, M. H. & Qian, Y., 2018. *A Blockchain Aided Metric for Predictive Delivery Performance in Supply Chain Management.* Singapore, IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI).

Min, X., Li, Q., Liu, L. & Cui, L., 2016. *A Permissioned Blockchain Framework For Supporting Instant Transaction And Dynamic Block Size.* Tianjin, IEEE Trustcom/BigDataSE/ISPA.

Mori, A. T., Meena, E. & Kaale, E. A., 2018. Economic Cost Of Substandard And Falsified Human Medicines And Cosmetics With Banned Ingredients In Tanzania From 2005 To

2015: A Retrospective Review Of Data From The Regulatory Authority. *BJM Open*, 8(6), pp. 1-7.

Muzammal, M., Qu, Q. & Nasrulin, B., 2019. Renovating Blockchain With Distributed Databases: An Open Source System. *Future Generation Computer Systems,* Volume 90, pp. 105-117.

OECD/EUIPO, 2016. *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact.* Paris: OECD Publishing.

Pawczuk, L., Massey, R. & Holdowsky, J., 2019. *Global Blockchain Survey- Blockchain Gets Down To Business,* s.l.: Deloitte Insights.

Perboli, G., Musso, S. & Rosano, M., 2018. Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases. *IEEE Access,* Volume 6, pp. 62018-62028.

Pittl, B., Mach, W. & Schikuta, E., 2016. *An Implementation of the WS-Agreement Negotiation Standard in CloudSim.* Vienna, IEEE 20th International Enterprise Distributed Object Computing Workshop (EDOCW).

Pittl, B., Mach, W. & Schikuta, E., 2018. *Bazaar-Blockchain: A Blockchain For Bazaar-Based Cloud Markets.* San Francisco, IEEE International Conference on Services Computing (SCC).

Pour, F. S. A., Tatar, U. & Gheorghe, A., 2018. *Agent-Based Model of Sand Supply Governance Employing Blockchain Technology.* Baltimore, Annual Simulation Symposium - ANSS '18.

Rauchs, M., Blandin, A., Bear, K. & McKeon, S., 2019. *2nd Global Enterprise blockchain benchmarking Study*, Cambridge: Cambridge Centre for Alternative Finance.

Roberts, J. J., 2017. *The Diamond Industry Is Obsessed With The Blockchain.* [Online] Available at: https://fortune.com/2017/09/12/diamond-blockchain-everledger/

Seal, 2018. *Seal Network To Build Blockchain Anti-Counterfeiting Network With The European Commission.* [Online] Available at: https://seal.network/press-releases/seal-network-to-build-blockchain-anti-counterfeiting-network-with-the-european-commission.html

Sharmila, V. C. et al., 2019. *Credit Card Fraud Detection Using Anomaly Techniques.* Chennai, 1st International Conference on Innovations in Information and Communication Technology (ICIICT).

Smartz, 2018. *How Blockchain and Smart Contracts Can Improve Customs Control.* [Online] Available at: https://medium.com/smartz-blog/how-blockchain-and-smart-contracts-can-improve-customs-control-1501ca00068f

Su, Z. et al., 2019. A Secure Charging Scheme for Electric Vehicles with Smart Communities in Energy Blockchain. *IEEE Internet of Things Journal*, 6(3), pp. 4601-4613.

Thiruchelvam, V., Mughisha, A. S., Shahpasand, M. & Bamiah, M., 2018. Blockchain-Based Technology In The Coffee Supply Chain Trade: Case Of Burundi Coffee. *Journal of Telecommunication, Electronic and Computer Engineering*, 10(3-2), pp. 121-125.

Tian, F., 2017. *A Supply Chain Traceability System For Food Safety Based On HACCP, Blockchain & Internet Of Things*. Dalian, International Conference on Service Systems and Service Management.

Toyoda, K., Mathiopoulos, P. T., Sasase, I. & Ohtsuki, T., 2017. A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain. *IEEE Access,* Volume 5, pp. 17465-17477.

Tracr, 2019. *Tracr*. [Online] Available at: https://www.tracr.com/ [Accessed 26 March 2019].

Tranfield, D., Denyer, D. & Smart, P., 2003. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management,* Volume 14, pp. 207-222.

Trust Chain, 2019. *The TrustChain Initiative.* [Online] Available at: https://www.trustchainjewelry.com/ [Accessed 26 March 2019].

Tseng, J.-H., Liao, Y.-C., Chong, B. & Liao, S.-w., 2018. Governance On The Drug Supply Chain Via Gcoin Blockchain. *International Journal of Environmental Research and Public Health,* 15(6), pp. 1-8.

UCOT, 2018. *Ucot'S Supply Chain Management.* [Online] Available at: https://www.ucot.world/

UNECE, 2013. *Trade Facilitation Implementation Guide.* [Online] Available at: https://www.unece.org/ [Accessed 13 11 2017].

UNODC, U. N. O. o. D. a. C., 2018. *Crime and criminal justice statistics.* [Online] Available at: http://www.unodc.org/unodc/en/data-and-analysis/statistics/crime.html [Accessed 12 January 2020].

Vos, D. et al., 2018. DEFenD: A Secure and Privacy-Preserving Decentralized System for Freight Declaration. *European Society for Socially Embedded Technologies (EUSSET),* 2(11).

Westerkamp, M., Victor, F. & Küpper, A., 2018. *Blockchain-based Supply Chain Traceability: Token Recipes Model Manufacturing Processes.* Halifax, IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).

Wood, G., 2018. *Ethereum: A Secure Decentralised Generalised Transaction Ledger,* s.l.: s.n.

World Customs Organization, 2018. *WCO SAFE Framework of Standards.* s.l.:World Customs Organization.

Wu, H. et al., 2017. A Distributed Ledger For Supply Chain Physical Distribution Visibility. *Information,* 8(4), p. 137.

Xiao, E., 2017. *Alibaba, Jd Tackle China's Fake Goods Problem With Blockchain.* [Online]

Available at: https://www.techinasia.com/alibaba-jd-ecommerce-giants-fight-fake-goods-blockchain

Xie, W. et al., 2018. *ETTF: A Trusted Trading Framework Using Blockchain in E-commerce.* Nanjing, IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)).

Xu, C. et al., 2018. *Making Big Data Open in Collaborative Edges: A Blockchain-Based Framework with Reduced Resource Requirements.* Kansas City, 2018 IEEE International Conference on Communications (ICC2018).

Xu, X. et al., 2019. Designing Blockchain-Based Applications A Case Study For Imported Product Traceability. *Future Generation Computer Systems,* Volume 92, pp. 399-406.

Zheng, Z. et al., 2018. Blockchain Challenges And Opportunities: A Survey. *Int. J. Web and Grid Services,* 14(4), p. 352.