TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Markkus Olaf Millend 179888IVSB

SECURE DIGITIZATION OF DOCUMENT TRANSFER PROCESS WITHIN MARITIME SHIPPING INDUSTRY

Bachelor's Thesis

Supervisor: Alexander Norta
PhD

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Markkus Olaf Millend 179888IVSB

MEREKAUBANDUSE SAATEDOKUMENTIDE EDASTAMISE PROTSESSI TURVALINE DIGITALISEERIMINE

bakalaureusetöö

Juhendaja: Alexander Norta
PhD

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Markkus Olaf Millend

10.08.2020

Abstract

Maritime shipping is one of the oldest methods of trade but is lagging behind with the adoption of modern technologies. Trade documents and their transfer has been a problematic aspect of shipping for decades, until recent years when the digitization of documents has become one of the main focuses of the industry.

Research delivered to this date has highlighted how digital documents can be integrated into the industry as well as the main issues regarding the process. One of the most common keywords that occurs throughout various research is blockchain technology. Previous research has primarily highlighted blockchain-based technologies due to their transparent and secure nature along with other platforms, such as TradeLens. As of today blockchain technology is perhaps the safest and the most applicable security tool for the shipping industry, due to its capacity to promote trust and transparency through elements such as timestamps and signature. Even though academics have offered solutions to introduce digital documents and their transfer into the industry, there is still room for more research and work. More specifically the gap is found in the finding a solution that is both secure and seamless to integrate into pre-existing workflows and industry processes.

The purpose of this thesis is to offer a solution that tackles the issue of inefficient and outdated documentation processes through a developed document transfer prototype and supporting research. Additionally, the aim is to help the freight forwarders in maritime shipping space to reduce costs, increase their productivity and avoid time-consuming traditional methods of document transfer by digitising the traditional work processes.

Annotatsioon

Merekaubanduse saatedokumentide edastamise protsessi turvaline digitaliseerimine

Merekaubandus on üks vanimaid kaubanduse ja transpordi vorme. Samas jääb see uute ja kaasaegsete tehnoloogiate kasutusele võtmisel maha teistest transpordi valdkondadest. Kauba saatedokumendid ja nende edastamine on olnud laevanduses murekohaks juba aastakümneid. Viimastel aastatel toimuva digitaliseerimise kontekstis on siiski ka merekaubanduse tegevusharus tõusnud üha enam rambivalgusesse kauba saatedokumentide digitaliseerimine.

Tänaseks on tehtud mitmed uuringuid ja analüüse, mis pakuvad välja, kuidas digitaalseid saatedokumente saaks merekaubanduses edukalt ja lihtsalt olemasolevatesse protsessidesse integreerida. Üks peamiseid märksõnu, mis neist erinevatest uuringutest esile kerkib, on plokiahela tehnoloogia. Varasemad uurimistööd ongi peamiselt esile tõstnud plokiahela tehnoloogia kasutamise võimalusi selleks ja teisi platvorme nagu TradeLens. Kuigi akadeemilises kirjanduses on pakutud mõningaid lahendusi, kuidas merekaubanduses dokumentide digitaliseerimist teostada, on sujuv ja turvaline lahendus üldiselt ikkagi puudulik või praktiliselt ei olegi seda olemas.

Käesoleva töö eesmärgiks ongi pakkuda võimalikke lahendusi praeguse ebatõhusa ja vanamoodsa kauba saatedokumentide edastamise protsessi turvaliseks digitaliseerimiseks merekaubanduses. See aitaks vähendada valdkonna ettevõtete kulusid, tõsta nende tootlikkust ja edastada dokumente kiirelt, kaasaegselt ning usaldusväärselt.

List of abbreviations and terms

TUT	Tallinn University of Technology
EU	European Union
DLT	Distributed Ledger Technology
UNCITRAL	United Nations Committee On Trade Law
EVM	Ethereum Virtual Machine
PKI	Public Key Interface
ORM	Object Relational Mapper
AES	Advanced Encryption Standard
OCSP	Online Certificate Status Protocol
PKI	Public Key Interface
CRM	Customer Relations Management
BPMN	Business Process Modelling Notation

Table of contents

List of figures

1 Introduction

International trade has played a significant role in the exchange of good since early time of civilisation, however during the 20th century it has seen incredible growth. Developments in technology has propelled the industry of shipping forward. While the information technology as we know it today did not exist in the mid-20th century, advancements in the actual form of good transportation was a crucial element in driving the innovation. Containerisation was standardised in 1965 and has since then accelerated the volume of goods shipped globally [1]. As an example, the worth of international trade in 1960s was $0.45 trillion, however by 1990 it jumped to $3.4 [1]. Since then industry leaders have relied on the innovation coming from the information technologies sector to respond effectively to the constantly changing needs of the customer, and remain competitive with competitors [2] [3]. Among many technologies now implemented, some stand out as good examples - Radio Frequency Identification, Electronic Data Interchange and Internet-based technologies to name a few [4]. Information technology is now considered as the most important factor in the supply chain improvement [5], and companies such as Walmart have been successful in integrating complex technologies to work together to enable the company to remain responsive to consumer demand and keep their supply chain lean and effective [4]. Nonetheless, maritime shipping specifically is heavily involved in cooperation between various players within the supply chain and must function with an extremely large amount of transport and trade documents [6]. Thus, heavy bureaucracy can slow down the process of goods transportation significantly. This also encourages the companies in the industry to look for more efficient, faster and cost-effective strategies and technologies to reduce the burden of bureaucratic system [7]. Blockchain technology has been slowly introduced to multiple segments of maritime shipping to enhance the efficiency through improving the transparency of the supply chain processes, reducing the time necessary to clear customs, keep track of documentation and reduce other various costs as well as risks [8]. Blockchain is a decentralised and safely encrypted data repository [9], which is immune to exploitation of the databases themselves [10]. The technology has enabled companies to conduct audits between multiple parties and optimise in real-time, thus promoting trust among members of supply chain [8] [6]. Furthermore, the use of blockchain technology will benefit most members of the supply chain, such as the freight forwarding companies, ports, and other businesses involved in the maritime transportation process due to providing tools previously somewhat inaccessible that can bring benefits to the competitiveness potential of respective companies. Despite the fact that the technology has seen incredible development in the last decade, companies are struggling to adapt these changes themselves, and are failing to convince their partners to also subscribe to the upgrades in technological tools available [4]. Moreover, even among companies that have integrated technologies like blockchain into their workflow processes, not all of them are satisfied with their internal performance, which points to the fact that barriers are still present that prevent successful adaptation of technologies by shipping organisations.

1.1 Problem statement

The aim of this research is to explore how document exchange between members of the maritime trade can be digitized securely and as seamlessly as possible, and through this exploration contribute to the academic knowledge on this specific topic.

The research question which this thesis investigates is: **"How can maritime shipping industry documentation transfer be securely digitized as seamlessly as possible, without disrupting pre-existing processes?"**

1.2 Research process

To find solutions to the aforementioned main research question, it is necessary to analyse academic knowledge delivered to this date and find answers to the following research questions:

- **What are the current inefficiencies in the process of documentation transfer?**

This element of shipping is vital to the entire functionality of the supply chain, as parts of the process like custom clearance, cargo release and ownership transfer all depend on this element specifically.

- **What are the core security risks of standard documentation transfer processes?**

This is important because the traditional method, which is explained in Section 2, has multiple security dangers present as of today.

- **What are the benefits of digitising the documentation transfer processes?**

To find solutions to the inefficiency and security issues, it should be analysed whether digitising the processes would bring any effects.

In order to map the existing processes in the industry, Business Process Modelling Notation (BPMN) is used. BPMN gives a clear overview of business processes in a graphical notation and enables companies to easily implement the procedures.

The Information System Security Risk Management (ISSRM) model is used, to map out the exact security risks within the inefficiencies detected. It is a framework that provides a methodology to identify and evaluate security risks. The model is further explained in the background section of this thesis.

1.3 Thesis outline

The thesis is structured as follows. Section 1 provides an introduction to the industry focusing on the history of the maritime shipping space, the main developments in the industry and the importance of informational technology in shipping today. In addition, an overview of research process is presented. Section 2 concentrates on bringing attention to the main points of maritime shipping to give a better understanding of context for the reader as well as academic knowledge delivered to date on this topic. Industry's history and critical issues it faces in the modern world. It is then followed by the analysis of existing body of knowledge. The section focuses on the most relevant research written regarding the topic. The following section 3 highlights the inefficiencies in the current document transfer processes, such as the reliance on the physical shipment of the documents, which is an outdated process given that today's technology enables secure transfer digitally. In section 4 the research paper focuses on the dangers of the current traditional method of document transfer and how the digitisation of processes could enhance the overall security of the transfer mechanism. Section 5 offers a potential solution that would tackle the inefficiencies and security issues. Coming next, section 6 presents an analysis of the findings with a practical example. Finally, the last section 7 concludes this thesis.

2 Running case and related work

In this part of the thesis, maritime shipping industry's shortcomings regarding the digitisation of documentation processes are highlighted in Section 2.1. Section 2.2 follows with analysis of previous academic knowledge delivered to this date and the ways in which the research has tackled the inefficiencies so far.

2.1 Background

In this section of thesis, background information is given regarding the maritime shipping industry. Additionally, an overview of blockchain technology is given to better understand the following sections of this thesis.

2.1.1 Maritime shipping industry

Today, the maritime shipping industry plays extremely important role in the global trade of goods. In 2018 the volumes of cargo shipped globally reached close to 11 billion tonnes (figure 1), and an expected rise of 3.5% annually will take place until 2024 [11]. Shipping itself is divided into multiple types of cargo with their own types of documents, various containers and methods of cargo storage, which complicates the matter of transportation even further. As already established, the bureaucracy in the maritime shipping space is very strongly integrated into the systematic functionality of the industry.

Because maritime transportation was present before the inception of air travel, multiple documents have been created centuries ago and have remained relatively similar up to this day. The bill of lading, which is essentially the passport of the cargo transported was present before the 16th century, however, became legally binding during the 16th century [12]. To make things even more complex, there are multiple versions of the bill of lading document. House bill of lading is an iteration created by the freight forwarding agency, master bill of lading on the other hand is created by the carrier and so on. In addition to the bill of lading, the package of documents includes an extended list of other documents and invoices necessary to process the shipment of goods. Documents such as the certificate of origin, letter of credit, gross mass declaration and others are needed to confirm the weight, description and the destination of goods, as well as whether the cargo has been paid for and if it is possible to buy the cargo during the transit period.

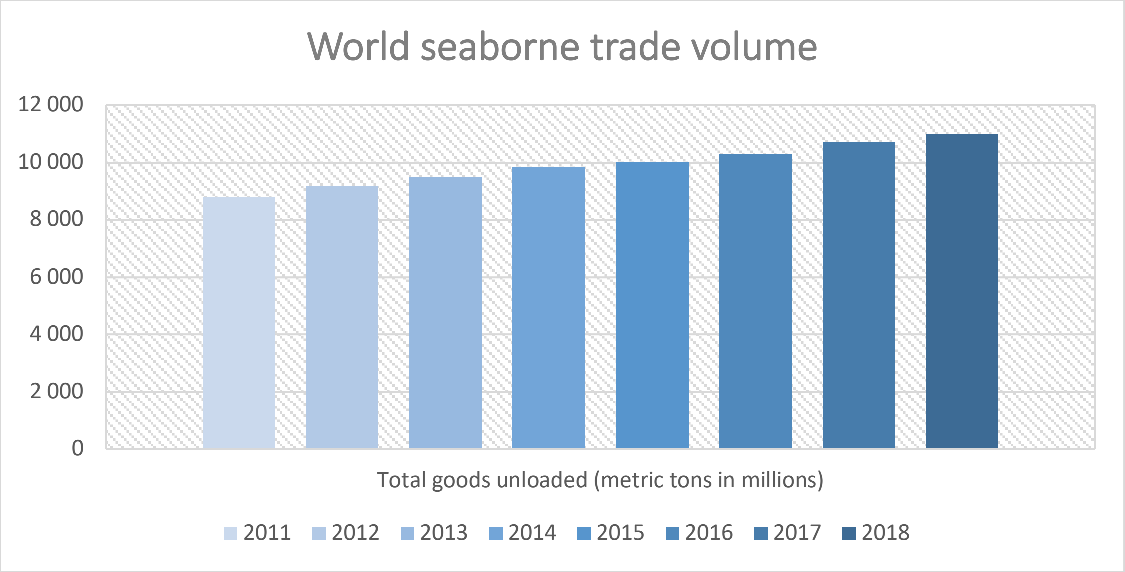


Figure 1. World seaborne trade volume (data source: UNCTAD Stat)

2.1.2 Information system security risk management domain model

As already mentioned, ISSRM domain model is a framework that helps to identify, evaluate and quantify security risks in information systems and their development [13] [14]. It is a set of concepts, that are either asset-related, risk-related or treatment-related. These concepts are briefly introduced.

Assets-related concepts describe an organisation's assets and their security criteria. An asset in this context is anything that is valuable and plays an important role for an organisation to accomplish its objectives. Assets can be **business assets** or **IS assets**. A **security criterion** is a constraint on business asset that describes an asset's security needs [15].

Risk-related concepts define the risks. A risk consists of a threat with one or more vulnerabilities that together lead to negative impacts on the organisations' assets. A threat is a potential attack initiated by a threat agent using an attack method to target IS assets [16].

Risk-treatment related concepts describe the specific concepts to treat a risk. It covers decisions, security requirements and controls. Decisions satisfy security needs and can lead to the mitigation of security risks. Security requirements refine the risk treatment and define conditions that need to be implemented to successfully mitigate security risks. Controls are the means to improve the security by implementing the security requirements [15].

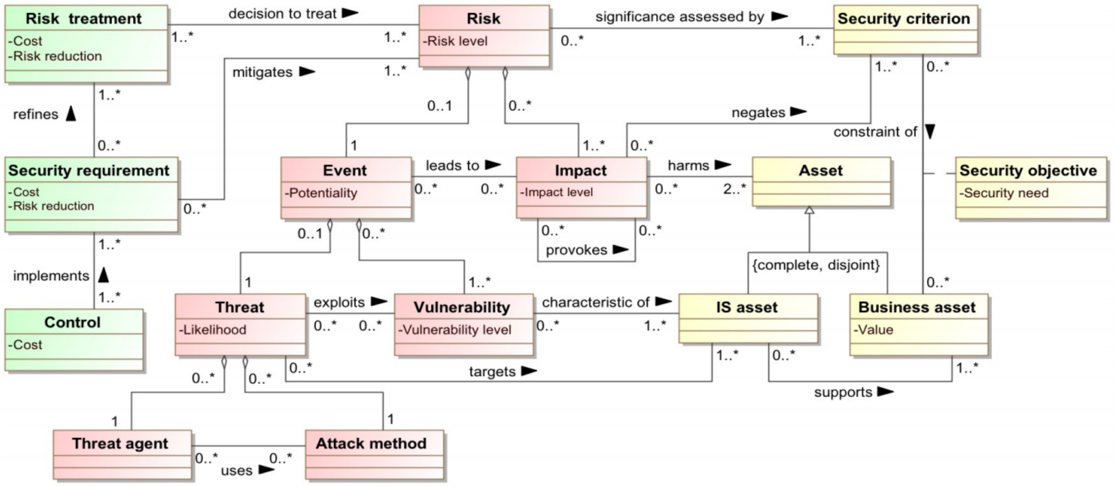


Figure 2 – ISSRM model [13] [14]

In order to apply the ISSRM, the following steps have to be followed [15].

1. Assets that need to be secured have to be defined.
2. Security objectives have to be determined based on the level of protection required for the assets previously defined.
3. Risk analysis and assessment should be conducted to find out potential risks and their impacts.
4. Based on risk analysis, a risk treatment decision should be taken. This results in security requirements definition.
5. Security requirements are implemented into security controls.

2.1.3 Blockchain technology

Blockchain is a relatively new term in the field of information technology. The origins of the concept date back to 2008, when a scientist called Satoshi Nakamoto unveiled a research regarding the technology [17]. Along with the research, the first cryptocurrency Bitcoin was introduced in 2009. Nowadays, blockchain technology has been implemented into other fields, such as public service, Internet of Things (IoT) and smart contracts [18]. Blockchain in its core is a data structure that consist of back-linked list of blocks, which hold a complete list of transaction records. It is stored and managed using distributed ledger technology (DLT). The advantage of this method is that records are not stored in a centralised manner but are decentralised between multiple parties (e.g. nodes) of the blockchain network.

Falsifying records with unilateral changes is not possible, due to the nature of the technology. Once confirmed by the network, it's impossible to alter data afterwards. New transactions are usually confirmed with a mathematical consensus algorithm that varies based on the blockchain network. Each confirmed transaction is stored into the chain permanently and can be later looked up and verified.

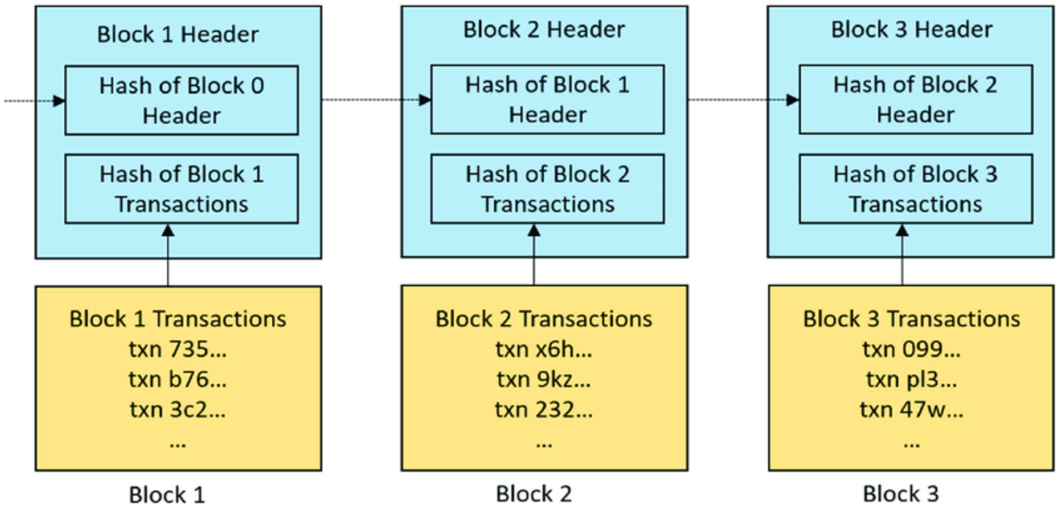


Figure 3 – The structure of blockchain [19].

There are two main types of blockchain networks on the market – public networks and permissioned networks. In the latter, parties of the chain are governed by a set of permissions that allow them to read data or make new transactions. In such networks, all parties are clearly identified.

In practice, blockchain and DLT technology enables different parties of a network to exchange "virtual tokens", such as cryptocurrency or other information. Each blockchain token has a specific owner, who can be identified and verified using public key infrastructure (PKI). In certain types of blockchain networks, such as Ethereum, it is possible to associate smart contracts with tokens. Smart contract is essentially a piece of software that runs on the blockchain network, and thus it is possible to automate various processes if certain conditions are met.

2.2 Running case

The process of documentation in maritime shipping is time-consuming and requires multiple screenings of the client, as well as careful approach to filling out the forms needed. First, an inquiry is received from the buyer. A due diligence process will have to be started to make sure that the client is legitimate and that the risk of fraud is minimal. This process also includes making sure that the country of final destination is open to goods transportation or are there any barriers, such as political or economic sanctions established against the state. After the due diligence process has been passed successfully, the freight forwarding company releases the Proforma Invoice and the sale is finalised. Final step is to prepare the goods and the rest of shipping documentation [20]. The documents are then released and shipped out using a private courier to deliver the documents to the parties of interest, such as banks, carriers etc.

The previously established processes of documentation are done manually by most companies in the industry. As of 2020, there have been multiple companies, who are trying to digitise and optimise these processes from different angles. For example, companies such as Forto are trying to simplify the process of booking a shipment and processing it [21]. On the other hand, Tradelens took a similar approach but decided to implement blockchain into the process as well to increase the security and transparency of the process. The approach of this specific company is analysed in the following Section 3.2 on the state-of-the-art literature.

In conclusion, the maritime shipping space is a well-established industry that has remained relatively stagnant in terms of technological advancements with the major breakthroughs being the containerisation in the second half of the 20th century and the application of the information technologies in the late 20th century and up to this day [1]. While many companies have offered various solutions to the issues of inefficiency in the industry, the implementation of these solutions has still left some of the workflow processes ineffective in the 21st century. This research paper focuses on exploring the inefficiencies of the traditional method of documentation and documentation transfer, as well as some of the difficulties of implementation. The next section looks at the academic research on the topic and analyse the state-of-the-art papers to better explain the issues that the industry is facing.

2.3 Related work

In this section, research delivered to this date is analysed. The main focus will be on current trends in the industry, already developed platforms and pinpointing the weaknesses of already existing solutions.

2.3.1 Document digitization and current barriers

F. Yuan has produced a thorough analysis on the current barriers to digitizing the maritime shipping documents and optimizing the transfer process. In the research, it is proposed that shipping industry's aging documentation transfer process and the issue of countries' different laws and requirements for electronic documents can be tackled by the use of private regulatory systems that are operated by the private sector [22]. These systems would connect parties who are all bound by the system's laws and rules. Users of the system would be various parties of maritime trade – exporters, freight forwarders and other parties of the supply chain. As an example, such systems can be developed using blockchain technology.

Since the industry itself has already created a movement towards the implementation of blockchain technology, it is wise to review the current major barriers that may prevent the adoption of the technology. A study conducted by C. Bavassano, C. Ferrari and A. Tei that focused on published literature, media reports, research (including web-based research) and expert opinions, reveals that local regulators are still unsure of different blockchain initiatives, since there is still no clear understanding of the potential effects of blockchain on the industry [23]. This is largely due to the fact that previously conducted research has focused mainly on the technical aspects of the technology. Furthermore, as stated in F. Yuan's research, different regions and countries around the world have their own standards and regulations. The European Union, for example has its own rules in place for digitising paper-based documents [22]. If smaller regulators in the industry start coming up with their own standards, it will become nearly impossible to develop an internationally recognised standard.

2.3.2 Using blockchain for standardisation and digitisation

C.-S. Yang has conducted a study using Technology Acceptance Model (TAM) among members of the maritime shipping industry in Taiwan. The goal of the study was to examine what are private sector companies' standpoints on using blockchain technology, including how they could most benefit from it. The main topics that were covered in the study were applications, future improvements and intentions to use a blockchain bundling model [8]. The study revealed companies largely support the idea of using blockchain technology since it potentially lays a foundation for standardisation, document digitization and eases overall paperwork.

T. Jensen, J. Hedman and S. Henningsson have published a research on an IBM-Maersk led software called Tradelens, which is a blockchain-based solution that allows companies in the container shipping industry to exchange information, documents and track cargo. The software is perhaps one of the best examples of how shipping documents can be digitised and transferred between parties. In 2019, some major countries in the industry, such as Saudi Arabia, Canada and Russia announced that they had already signed up with Tradelens. However, the research reveals that the there is still a slow adoption rate with other players in the industry. The key factors that contribute to this issue are concerns about the technology, lack of internationally recognized standards for digital documents and reluctance to trust digital documents [24]. Afterall, TradeLens is operating on a permissioned blockchain that is owned by IBM.

A start-up called CargoX is also focusing on the digitalisation of documents and their transfer. More specifically, the main focus is the transfer of the Bill of Lading, which is essentially the most important document of a shipment. The solution may be more appealing for SMEs, since CargoX' platform is not directly affiliated with any shipping company when compared to TradeLens, which is partly owned by Maersk. Additionally, CargoX relies on a public blockchain, rather than a permissioned one [25]. A study conducted by M. Jović, M. Filipović, E. Tijan and M. Jardas analyses different blockchain based solutions (including TradeLens and CargoX) that attempt to digitize documentation in the industry. It reveals that one of the main disadvantages to using blockchain based solutions is the absence of underlying standards, which also points back to previously analysed research. Furthermore, the transition to paperless documentation may not be that seamless since new practices are difficult to be mastered and even simplest forms of implementation require technical expertise [26].

To conclude this related work section, it can be said that there are currently multiple concerns to digitising and transferring documents. Taking into account the aforementioned solutions, it all boils down to difficult implementation methods, distrust for digital solutions or missing standards regarding digital documents which prevent widespread adoption. There is still a need for a solution that complies with the yet-to-be established standards that also features advanced security measures, while still being relatively easy to use. This thesis aims to fill in the gap by suggesting a solution.

3 Inefficiencies in documentation transfer processes

This part of the thesis will explain the traditional processes of documentation creation and their transfer that have been present on the market, and the inefficiencies of them. By pinpointing the exact weaknesses, the section attempts to answer the research question “What are the current inefficiencies in the process of documentation transfer?”.

3.1 Aging error prone documentation creation processes

Before documentation creation and their transfer is analysed, it is necessary to get a clear overview of the existing processes regarding the topic. The processes are mapped using BPMN in Signavio software. The following figure depicts the usual business process regarding the creation of documents and their transfer. The process usually involves three parties – shipper, freight forwarder and logistic(s) partners. The transfer of documents is later analysed as a separate process that spans across multiple parties.

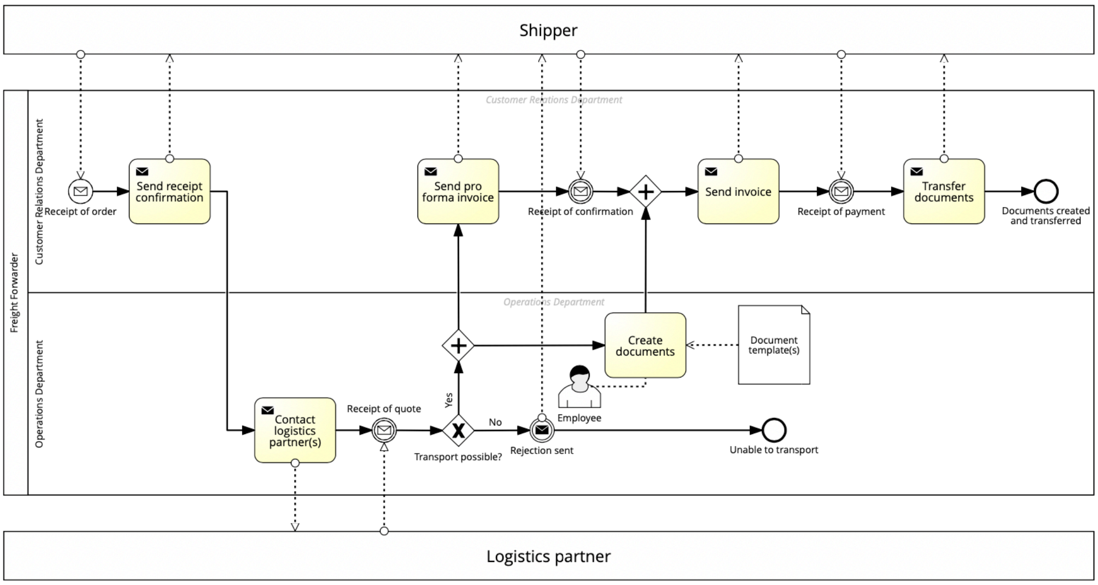


Figure 4 – Documentation creation process (contributed by author)

In the figure, documentation is processed by the freight forwarding company that in most cases handles the logistical chain setup and the creation of necessary documents. The company takes into account the information provided by the shipper or the exporter and then inputs the data onto the documents. The information provided consists of details of the cargo itself, destination of cargo and the dates, as well as parties involved. This information is usually provided either through a phone call, by email or by sending the invoices and the already existing proof of order to the freight forwarder. The freight forwarding company in general has two teams that are responsible for processing orders. The first contact with the freight forwarding company by the client is usually done through the customer support or service department, that records the information given and then passes the details to the internal operations team. The operations department then gets in touch with the logistics companies (trucking firms, shipping lines etc.) to create the logistics chain and after that begins the process of filling out the documents. Some of the more established freight forwarding companies might have an internally developed or outsourced CRM (customer relationship management) software that helps the operations department in the creation of documents, however smaller companies mostly lack access to such toolkits and are forced to create the documents by using templates that were previously created [27]. This process is tedious and lacks the streamlined fashion of specifically designed digital toolkit. The main problem is that the creation of documents takes up too much time and is prone to human error, due to the people filling out the documents one by one.

3.2 Inefficiencies during documentation transfer

To understand why and how the current documentation transfer systems are inefficient, BMPN is once again used to get an exact overview and pinpoint the shortcomings. In addition to buyer, freight forwarder and shipper, banks are also included in the following model. Banks play a vital role in the transfer of documents and issuing of the letter of credit.

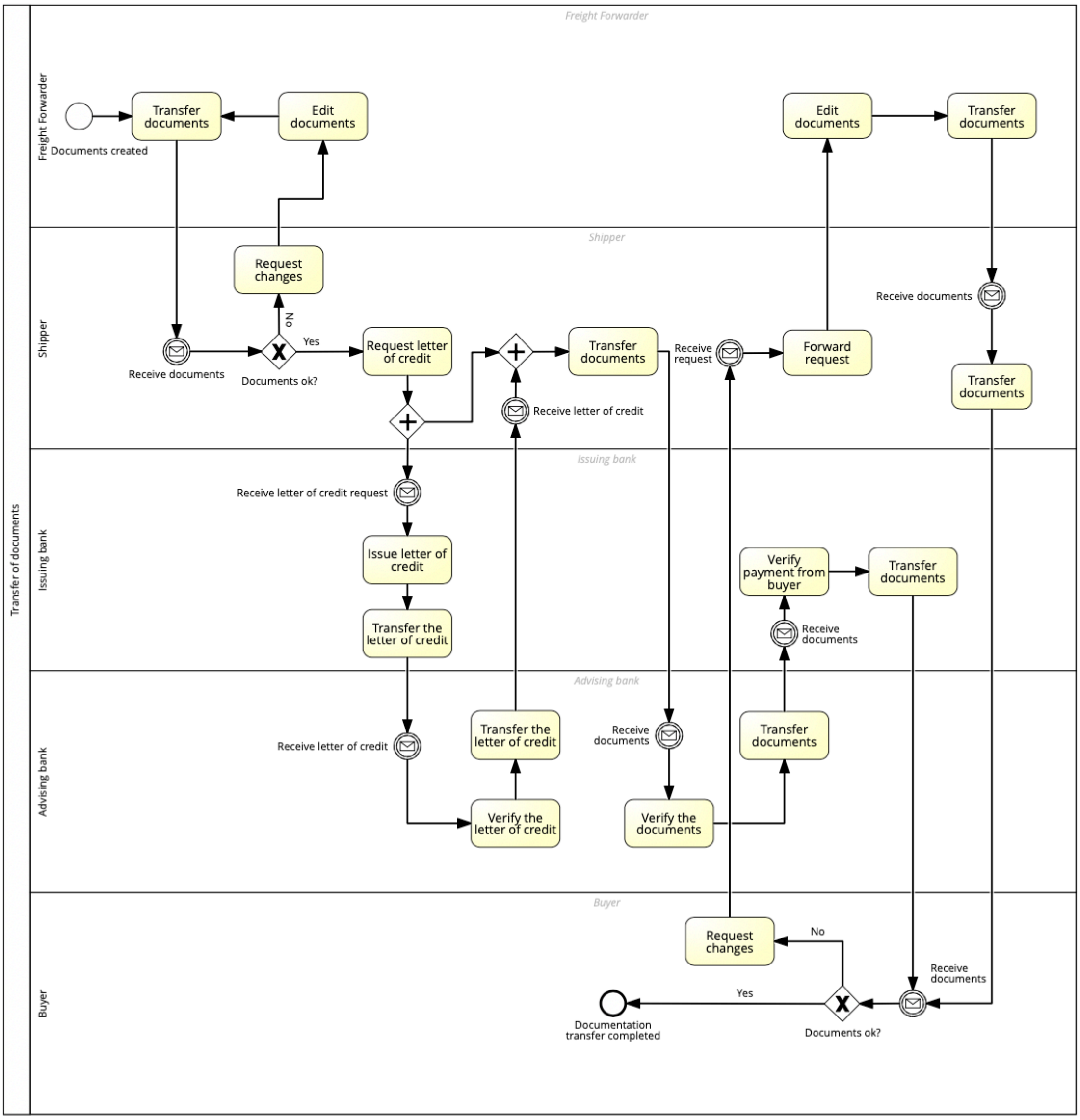


Figure 5 – Transfer of shipping documents (contributed by author)

Once the documents are created the original copies of the bill of lading, certificate of origin and the copies of invoices and other documents are then printed, signed and transfer process is set in motion. Despite the progress made in technology and the availability of document transfer systems on the market, many companies still prefer the traditional method of document transfer. There are, nonetheless, multiple dangers and inefficiencies associated with such method of document transfer. Firstly, the way the documents are filled in currently is a very slow and costly process for companies that do not have access to software tools that can automate the process of document creation. In addition, as already mentioned this process is also prone to human error as many of the documents created can look somewhat similar and the person filling them out one by one might miss the necessary piece of document or insert wrong information by accident. Secondly, printing these documents can be taxing on the environment. Combined with the packaging for the documents, the amount of paper used can be high. Furthermore, archiving and storing these documents in the physical format is sometimes required by the companies, and thus is also inefficient as it might be relatively difficult to find the needed documents quickly. Thirdly, the physical copies of the documents have to be sent by a courier. This adds extensively to the expenses for the freight forwarding company [27]. In addition to the expenses, there is also the danger of documents arriving late. In the case of the document package arriving late the entire supply chain might come to a halt, because without the documents it is not possible to release and process the cargo correctly. This in itself can also add costs due to the ships not being able to unload the cargo or the ports storing the cargo for longer than they ideally should. Fourthly and finally, combining the first issue and the last one together - the danger of the documents being filled out wrong and still shipped is also possible. In this case the documents have to be sent back to the freight forwarder for them to re-issue the document package again with correct information. This is dangerous because it also adds costs for both the private courier services as well as slowing down the efficiency of the supply chain.

3.3 Analysis of inefficiencies

Signavio software that was used to develop the model on figure 4 allows its users to simulate all developed models. For determining the efficiency of current processes, certain variables were defined. Since the documentation transfer relies on courier services, an average cost of 15 euros was set and the duration was set to an average of 24 hours due, assuming that express shipping is used. Upon simulating the model, the results show that the traditional method of documentation transfer is extremely inefficient and slow. The results show that reliance on courier services extends the whole documentation transfer process by 9 days. That also includes two document update requests, which increases the total time even more. In total, 127 euros are spent on courier services.

In conclusion, while the traditional method has been functional for decades, it has now become clear that with the advancements of the technology far better options for document transfer can be achieved. Digitising the documentation process could not only reduce the expenses for the parties involved, but also, drive down costs and increase the efficiency of freight forwarders and other businesses tied to each other within the supply chain.

4 Security risks in the standard documentation transfer processes

This section highlights the main security concerns regarding the current traditional methods of documentation transfer from a freight forwarder’s point of view. In the process, business assets are defined and along with their security risks. In the risk identification process, ISSRM domain model is used as a reference, but not applied. This is due to the fact that the documentation transfer process currently does not rely on any IS processes. Through the analysis, the section attempts to answer the research question “What are the core security risks of standard documentation transfer processes?”

4.1 Assets in the process of documentation transfer

The documentation transfer involves all of the documents that are issued by the freight forwarder. As previously pointed out in the thesis, the documents can be bill of lading, certificate of origin, various invoices etc. In this section of asset determination, we consider all of the documents that need to be transferred a business asset. Usually the documents are transferred simultaneously in packages.

Business asset(s)	Shipping documents
Business process	Documentation transfer process
Process description	Documents are transferred between associated parties using courier services
Security criteria	Confidentiality of shipping documents

The security criterion for the business asset defined above is confidentiality. An unauthorised party should never be able to access the contents of the documents as this could potentially put the whole shipment into jeopardy.

4.2 Analysis of risks to the documentation transfer processes

In the following table, we present a possible attack method on the shipping documents business asset. The attack method is used by two threat agents with different motivations.

	Risk 1	Risk 2
Threat agent	Thief **Motivation:** wants to steal cargo. **Resources:** money to bribe personnel **Expertise:** knowledge of the documentation transfer process	Forger **Motivation:** wants to tamper the documents. **Resources:** money to bribe personnel **Expertise:** knowledge of the documentation transfer process
Attack method	1. Bribes courier service 2. Impersonates a courier	1. Bribes courier service 2. Impersonates a courier
Threat	Unauthorised party gets access to shipping documents.	Unauthorised party gets access to shipping documents.
Vulnerability	Reliance on courier service.	Reliance on courier service.
Event	Thief gets access to shipping documents, since it is impossible to detect an imposter.	Thief gets access to shipping documents, since it is impossible to detect an imposter.
Impact	Shipping documents are compromised, cargo can be stolen at port of discharge.	Shipping documents are compromised and tampered.
Risk	A thief impersonates himself as a courier service employee, through which the thief gets access to original shipping documents and is able to steal the cargo at port of discharge.	A forger impersonates himself as a courier service employee, through which the forger gets access to original shipping documents and is able to tamper the documents.

The analysis in the previous table shows how two threat agents with different motivations are able take advantage of the weaknesses of existing documentation transfer processes. This is possible due to the reliance on traditional courier services, where the courier service employee picks up the package of documents and delivers them to the following party. During the process, the documents are entirely trusted to a 3rd party, who can view the documents at any time. Furthermore, the documents are not protected with any form of tamper-proof methods, since all of the existing processes are built on trust.

To sum up, the current process of traditional document transfer poses significant risks to the freight forwarder. The transfer that is reliant on paper-based format is prone to dangers of the documents arriving late or the information being leaked to outside parties that would lead to the falsification of documents or the cargo being released to the wrong party. Digitising these elements would improve the trust between parties, as they would see exactly when the documents have been created and to whom they have been transferred and would allow the freight forwarding company to avoid risks of not being able to track the documents or track the responsibility properly. When the documents are transferred in a secure digital manner, the dangers of information exploitation decreases. In conclusion, the digitisation of the process would be helpful to the parties involved in the logistical supply chain.

5 Digitising existing documentation transfer processes

This section focuses on introducing technology and security elements to the transfer process, which is currently both inefficient and insecure. Through the development of a process which digitises current method of document transfer, the section attempts to answer the question “What are the benefits of digitising the documentation transfer processes?”

5.1 Requirements for digitisation

As analysed in the previous section on the example of two risks, the current vulnerability in the existing process is the reliance on courier services. Members of the supply chain have to trust a party to handle the transfer who is not associated with the shipment. An obvious alternative would be to transfer documents via e-mail, but since original physical signatures are important in the industry, it is done in the traditional way.

If the reliance on courier services is ruled out, it could be replaced by a potential solution that allows users to transfer documents digitally. However, the solution should satisfy some prerequisites.

The prerequisites for digitising the existing documentation transfer processes are:

- The digitised process should keep the documents secure in order to mitigate previously identified security risks.
- The digitised process should facilitate the creation of signatures.
- The digitised process should be unobtrusive and could be easily integrated into the pre-existing processes.

5.2 Keeping files secure during the transfer

As pointed out in the security threat analysis, the main threat regarding confidentiality of the files is the fact that files are not encrypted or protected while they are in transit. Thus, document confidentiality is a critical part of the solution. In order to tackle this, file encryption can be introduced. In the proposed solution, every initiated transfer revolves around a document that is inputted by the user. Once the file is uploaded, a SHA256 checksum of the file is made and stored for auditing. The checksum acts as one of the safety guarantees for the user. If the file checksum changes while it is in digital transit, the user will know that the file has been tampered and no longer has to trust the file. Once the checksum is made, the file can be encrypted using AES-256-CBC encryption cipher. AES (Asymmetric Encryption System) uses a key to encrypt and decrypt the contents. As a result of file encryption, the file contents are stored as cipher text.

5.3 Creating digital signatures using blockchain technology

To solve the issue of signatures, blockchain technology could be used. A blockchain account consists of cryptographic private key and an account address that can be used to derive the public key. The private key can be used to sign messages which can then later be verified. The potential solution would take advantage of this technology and force the users to confirm their intent to transfer a file or a document by creating a signature. In our case, the message that is being signed, is the document SHA256 hash. As a result, the created signature is stored both on the smart contract and off-chain in the platform database. Parallels can be drawn between the Estonian ID card system, where each person uses their personal private keys that are stored on the ID card to give signatures. However, Estonia has an OCSP (Online Certificate Status Protocol) validation service and other services for validating and confirming digital signatures [28]. Whereas with the proposed solution, it is not wise to assume that every user shall have and ID card and thus storing cryptographic signatures on the blockchain network can be considered as a reliable alternative, due to its decentralised nature.

5.3.1 Smart Contract

Once the transfer is initiated on the platform, an Ethereum smart contract is created and deployed, along with the signature of the user who initiated the transfer. A smart contract is a piece of software that can run on the decentralised EVM (Ethereum Virtual Machine).

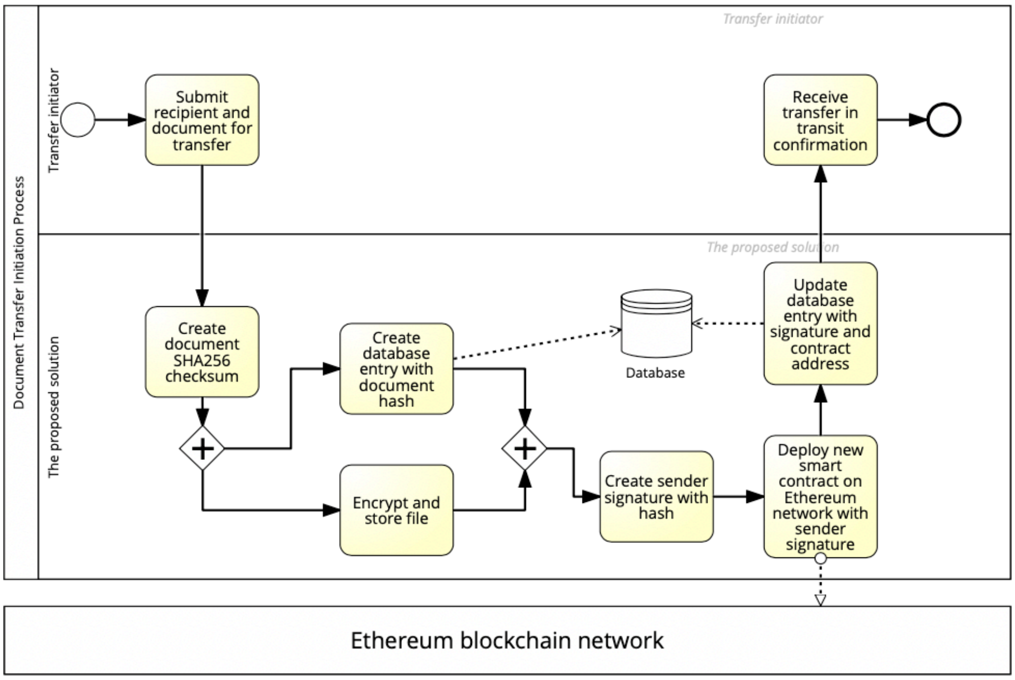
Each smart contract deployment requires the platform operator to spend Ethereum cryptocurrency, which is consumed by the network to confirm the transaction. Each transfer's smart contract contains the following data:

1. The signature of the user who initiated the transfer.
2. The SHA256 checksum of the document that is being transferred.
3. The signature of the user who receives the transfer.
4. The Ethereum account address of the platform operator.

Throughout the whole process, platform operator will remain the technical owner of the smart contract. This is to make sure that not authorised accounts cannot update the smart contract's contents (i.e. the signatures).

5.4 Digital processes to facilitate digital document transfer

Following the requirements for digitising the documentation transfer process, the thesis presents a process which keeps documents encrypted during the entire transfer process, allows signature creation in the form of digital signature and keeps an auditable access log. The proposed processes can be integrated into the pre-existing documentation transfer processes as an entirely new subprocess, thus making the solution unobtrusive.



Document Transfer Initiation Process
Transfer initiator
Transfer initiator
Submit recipient and document for transfer
Receive transfer in transit confirmation
The proposed solution
The proposed solution
Create document SHA256 checksum
Create database entry with document hash
Database
Update database entry with signature and contract address
Encrypt and store file
Create sender signature with hash
Deploy new smart contract on Ethereum network with sender signature
Ethereum blockchain network

Figure 6 – Digital document transfer initiation process (contributed by author)

When the digital document transfer process is initiated, the flow will be:

1. User submits the document and sender ID through a form.
2. The platform creates a SHA256 checksum of the document.
3. The document file is encrypted using AES-256-CBC encryption cipher and stored as a cipher text. A corresponding database entry is created containing details about the transfer and stored file location.
4. The document hash will be signed with sender's private key to create a signature.
5. An Ethereum smart contract is deployed by the platform, along with the sender signature and transaction hash.
6. The database entry is updated with the deployed contract address and sender signature.

To receive documents through the proposed process, the document receiving process is proposed.

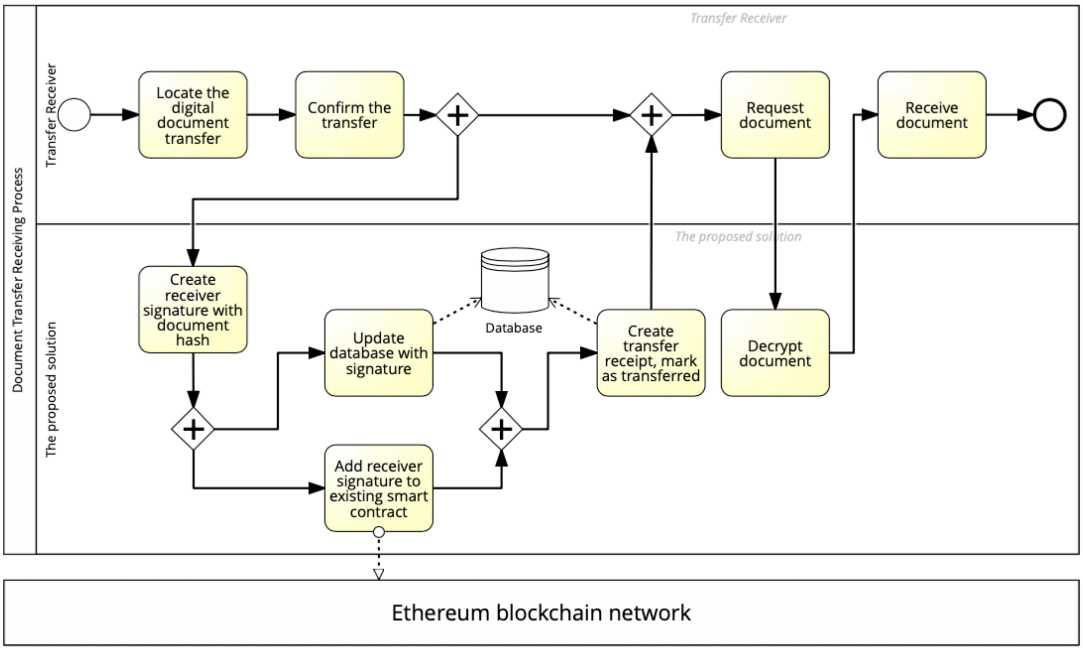

Document Transfer Receiving Process
Transfer Receiver
Transfer Receiver
Locate the digital document transfer
Confirm the transfer
Request document
Receive document
The proposed solution
The proposed solution
Create receiver signature with document hash
Update database with signature
Database
Create transfer receipt, mark as transferred
Decrypt document
Add receiver signature to existing smart contract
Ethereum blockchain network

Figure 7 – Digital document transfer receiving process (contributed by author)

In case of an ongoing transfer and the recipient wants to receive the file, the flow will be:

1. Recipient locates the ongoing transfer.

2. Recipient confirms the transfer. In the process, the document hash is signed with the recipient private key.
3. The created signature is added to the smart contract and database.
4. The transfer can be regarded as completed.

During file download request, the file’s cipher text is decrypted and file is presented.

Once the transfer has been finished the two parties will have a public digital contract (in the form of a smart contract) that confirms information about who were the parties involved and when did the transfer take place. Additionally, if needed, users can exchange document hashes prior to the transfer and then later compare them, to verify the integrity of the file after the transfer has been completed.

To conclude, there are many benefits to the digitisation of the transfer process. Firstly, through the digitisation, documents can be stored securely. Only designated parties can accept and view the files on certain conditions. Secondly, a clear and auditable record is kept regarding the access of the file. Thirdly, the solution has potential to drive down the ridiculous amount of time usually spent for the transfer of documents, including its costs.

6 **Evaluation**

In this section, the proposed solution for secure and digitised documentation transfer is analysed. Specifically, how this subprocess makes the overall process of documentation transfer more efficient and secure.

Namely, to make sure that the designed processes bring positive effects, we compare the initial time and cost results of documentation transfer processes to the proposed one.

The proposed solution is implemented into the main process of documentation transfer (figure 5) as a subprocess. Then, using the Signavio software we run the processes again and get the results. The measurements also include two extra requests for document changes, which make the overall process longer. For the traditional method of transfer, it assumed that each transfer timespan is 24 hours. For the digital transfer, it is assumed that each transfer timespan is 4 hours. Waiting time for human interaction is also taken into account. Due to the nature of the proposed solution, Ethereum had to be used to take measurements for the money spent in the process.

Method	Traditional	Digital
Total time documents spend in transit	216 hours (9 days)	40 hours
Money spent for documents to reach buyer	127 euros	0.01319 Ethereum (approx. 4.5 euros)

Based on the measurement results, it can be said that the designed process can bring positive results into the process of documentation transfer. To additionally prove that the process can be technically implemented, a prototype is constructed.

6.1 The Prototype

As a proof-of-concept, the proposed solution is used as a reference to build a simple document transfer platform that allows users to exchange documents in a secure manner. In this subsection, an overview is given about the technologies used to create this example. The full example is available in GitHub (https://github.com/mllnd/doc-exchange).

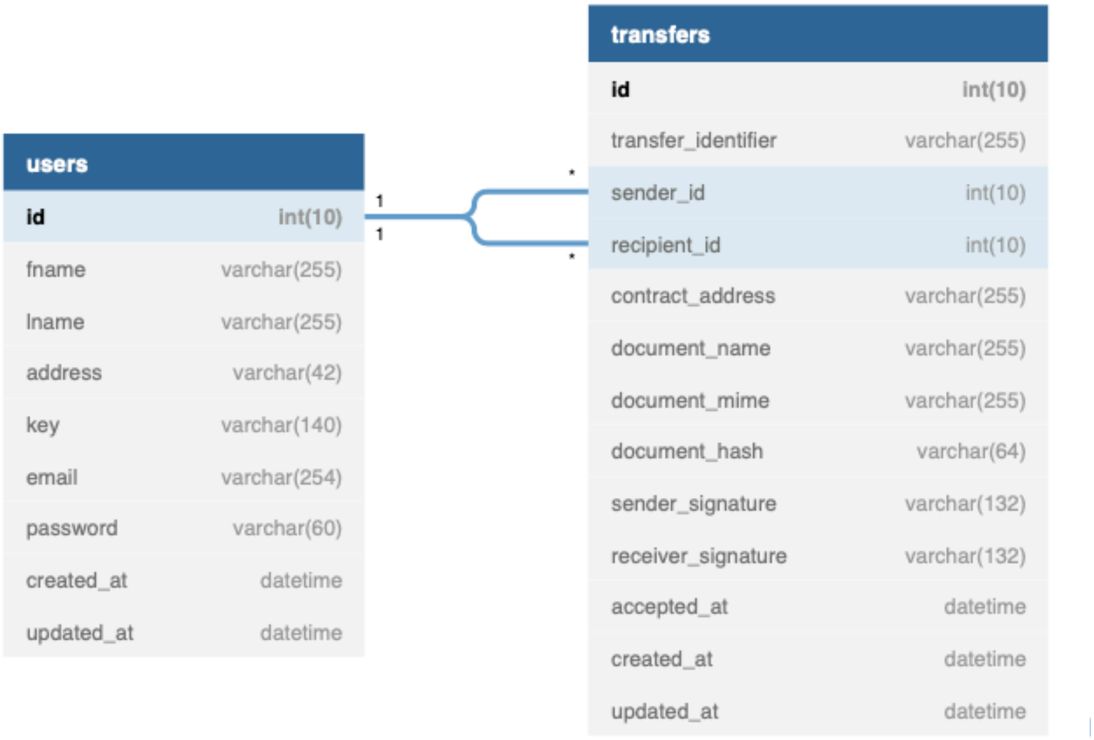
The following technology stack is used:

- Node.js (v12.18.3 LTS)
- AdonisJS (v4.1)
- MariaDB (v10.4.13)

6.1.1 Core Application

A Node.js-based open-source MVC framework AdonisJS (v4.1) powers the core of the application. It provides a very good starting point for a new application, since it has all of the necessary tools, such as a templating engine, database ORM (object relational mapper) and routing layer. Additionally, the framework handles database migrations, authentication and encryption-decryption of data. Another reason why a Node.js based framework works best in this particular scenario is the fact that libraries that enable applications to interact with Ethereum network are mainly written in JavaScript. In this implementation, Web3.js is used to connect to the Ethereum network and deploy smart contracts and interact with them.

Lucid ORM which we use to interact with the database comes pre-installed with AdonisJS. The ORM works well with relational databases, such as MySQL/MariaDB or PostgreSQL. In this implementation, MariaDB (v10.4.13) is used as the database. A simple schema consisting of two tables is sufficient for this implementation (figure below).



users	
id	int(10)
fname	varchar(255)
lname	varchar(255)
address	varchar(42)
key	varchar(140)
email	varchar(254)
password	varchar(60)
created_at	datetime
updated_at	datetime

transfers	
id	int(10)
transfer_identifier	varchar(255)
sender_id	int(10)
recipient_id	int(10)
contract_address	varchar(255)
document_name	varchar(255)
document_mime	varchar(255)
document_hash	varchar(64)
sender_signature	varchar(132)
receiver_signature	varchar(132)
accepted_at	datetime
created_at	datetime
updated_at	datetime

Figure 8. Database schema (contributed by author)

Users table contains various data about the user. The most sensitive data is either hashed or encrypted. User password is hashed using bcrypt before storing it in database. User key in this particular case is the user’s Ethereum account private key, which is also encrypted using AES 256 CBC cipher.

Transfers table contains data regarding all of the ongoing and completed document transfers. It also stores each transfers’ smart contract address and signatures of the parties involved.

6.1.2 Smart Contracts and Platform Operator Ethereum Account

The smart contracts which are deployed during a new transfer are written in Solidity. Solidity is a language specifically designed for writing smart contracts for the EVM. Each contract written in Solidity must be compiled into bytecode before it can be deployed. In this example, we use Solidity compiler version 0.5.16. Unfortunately, each deployment costs a small amount of cryptocurrency, which cannot be charged from the users. As a solution, the platform must have a separate account which can hold small amount of Ethereum to facilitate the transactions on behalf of users. This account is stored as a keystore file, which can only be decrypted on demand with a key. To successfully deploy a smart contract, the flow is:

1. Platform account keystore is decrypted with the private key (Web3.js handles this procedure).
2. Smart contract bytecode is loaded and deployed on the network.
3. Gas estimation is done for the transaction.
4. Smart contract deployment transaction is signed with platform operator account private key.
5. A new signed transaction is sent on the network.

A similar flow is followed when the contract is updated with the signature of the receiver:

1. Platform account keystore is decrypted with the private key (Web3.js handles this procedure).
2. Smart contract is loaded by using the contract address and the bytecode.
3. Smart contract method is called to store the receiver signature.
4. Smart contract method call transaction is signed with platform operator account private key.
5. A new signed transaction is sent on the network.

The smart contract can be seen below on figure 3.

```
pragma solidity >= 0.5.0 < 0.7.0;

contract TransferContract {

  string public senderSignature;
  string public receiverSignature;
  address public ownerAddress;
  string public documentHash;

  constructor(string memory _senderSignature, string memory _hash) public {
    senderSignature = _senderSignature;
    ownerAddress = msg.sender;
    documentHash = _hash;
  }

  function getSenderSignature() public view returns (string memory) {
    return senderSignature;
  }

  function getReceiverSignature() public view returns (string memory) {
    return receiverSignature;
  }

  function getOwnerAddress() public view returns (address) {
    return ownerAddress;
  }

  function setReceiverSignature(string memory signature) public {
    require(msg.sender == ownerAddress);
    receiverSignature = signature;
  }
}
```

Figure 9. Smart contract (contributed by author)

7 Summary

This section concludes this thesis and analyses whether the main problem has been solved with the proposed solution.

Maritime shipping industry is rapidly moving into the 21st century and implementing new technologies to increase the efficiency and transparency of the sector. However, as the industry is still relying on the traditions established over 50 years ago, the transition has not been as seamless as expected. Different laws and regulations have not been able to keep up with the emerging digitalisation and this has started to affect the industry in a negative manner. Existing solutions on the market have tried to come up with their own standards for digital documents (i.e. TradeLens), but the new ways may not be recognised worldwide or may be too obtrusive in terms of existing workflows.

To tackle the issue of missing standards and complex existing solutions, an alternative take is offered to the problem. The proposed solution would still incorporate many of the features of existing solutions, such as transparency and auditability. Furthermore, the solution would incorporate industry-standard encryption methods to protect the contents of users' documents. But most importantly, the implementation would fit seamlessly into pre-existing workflows of companies in the industry.

The developed process enables users to securely exchange documents while having an Ethereum smart contract as a confirmation when exactly the transfer took place. If necessary, 3rd party auditing can be performed using the smart contracts. Furthermore, no sensitive data is shared on the public blockchain, since only addresses and signatures can be obtained from the contract. The real owners of the addresses can only be backtracked using the records on the platform.

7.1 Future Work

A potential aspect that can be improved or potentially worked on is identified for future work.

Application in Other Industries

It is known that other shipping industries, such as rail freight or air freight also rely heavily on traditional paper-based documents. This thesis focused only on the issues of maritime shipping industry and it is unclear what kind of issues are other industries facing (if at all). Should there be a need for a similar solution in different areas, the solution should be fairly easy to implement due to its non-obtrusive nature in terms of existing workflows.

References

[1] D. M. Bernhofen, Z. El-Sahli and R. Kneller, “Estimating the Effects of the Container Revolution on World Trade,” 2012.

[2] V. Grover, “An Empirically Derived Model for the Adoption of Customer-Based Interorganizational Systems,” 1993.

[3] J. Lee and W. Qualls, “A Dynamic Process of Buyer-Seller Technology Adoption,” 2010.

[4] A. K. Asare, T. G. Brashear-Alejandro and J. Kang, “B2B Technology Adoption In Customer Driven Supply Chains,” *Journal of Business & Industrial Marketing,* vol. 31, no. 1, pp. 1-12, 2016.

[5] K. A. Patterson, C. M. Grimm and T. Corsi, “Adopting New Technologies for Supply Chain Management,” *Transportation Research Part E,* vol. 39, no. 2, pp. 95-121, 2003.

[6] A. Lieber, “Trust in Trade: Announcing a new blockchain partner,” 2017. [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/03/trust-trade-announcing-new-blockchain-partner/. [Accessed 15 April 2020].

[7] W. Lehmacher and J. Mcwaters, “How Blockchain Can Restore Trust in Trade,” in *World Economic Forum*, Geneva, Switzerland, 2017.

[8] C.-S. Yang, “Maritime Shipping Digitalization: Blockchain-based Technology Applications, Future Improvements, and Intention to Use,” *Transportation Research Part E,* vol. 131, pp. 108-117, 2019.

[9] N. Petrovsky and S. Apte, “Will blockchain Technology Revolutionize Excipient Supply Chain Management?,” *Journal of Excipients and Food Chemicals,* vol. 7, no. 3, pp. 76-78, 2016.

[10] A. Wright and P. D. Filippi, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia,” 2015.

[11] J. Hoffmann, W. Juan, S. N. Sirimanne, R. Asariotis, M. Assaf, H. Benamara, A. Premti, L. Rodríguez, M. Weller and F. Youssef, “Review of Maritime Transport,” United Nations Publications, New York, USA, 2018.

[12] D. E. Murray, “History and Development of the Bill of Lading,” University of Miami, Miami, USA, 1983.

[13] E. Dubois, P. Heymans, N. Mayer and R. Matulevičius, “A Systematic Approach to Define the Domain of Information System Security Risk Management,” *Intentional Perspectives on Information Systems Engineering,* pp. 289-306, 2010.

[14] N. Mayer, “Model-based Management of Information System Security Risk,” 2009.

[15] O. Altuhhova, R. Matulevičius and N. Ahmed, “Towards Definition of Secure Business Processes,” in *Advanced Information Systems Engineering Workshops: CAiSE 2012 International Workshops*, 2012.

[16] A. Norta, R. Matulevičius and B. Leiding, “Safeguarding a formalized Blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns,” *Computers & Security,* vol. 86, pp. 253-269, 2019.

[17] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[18] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in *2017 IEEE 6th International Congress on Big Data*, 2017.

[19] C. C. Agbo, Q. H. Mahmoud and J. M. Eklund, “Blockchain Technology in Healthcare: A Systematic Review,” 2019.

[20] D. Noah, “Shipping Solutions,” 17 January 2018. [Online]. Available: https://www.shippingsolutions.com/blog/shipping-documentation-process. [Accessed 15 April 2020].

[21] FreighHub GmbH, 2020. [Online]. Available: https://forto.com/en/about-us/. [Accessed 15 April 2020].

[22] F. Yuan, “Digitalization of Maritime Transport Documents,” 2019.

[23] G. Bavassano, C. Ferrari and A. Tei, “Blockchain: How shipping industry is dealing with the ultimate technological leap,” *Research in Transportation Business & Management,* vol. 34, 2020.

[24] T. Jensen, J. Hedman and S. Henningsson, “How TradeLens Delivers Business Value With Blockchain Technology,” *MIS Quarterly Executive,* 2019.

[25] “CargoX,” [Online]. Available: https://cargox.io/solutions/for-transport-and-logistics/#overview. [Accessed 15 June 2020].

[26] M. Jović, M. Filipović, E. Tijan and M. Jardas, “A Review of Blockchain Technology Implementation in Shipping Industry,” *Scientific Journal of Maritime Research,* no. 33, pp. 140-148, 2019.

[27] R. Piers, I. Giannelos, L. de Swart, H. Kramer, S. Mattheis and D. Frisani, “State of play and barriers to the use of electronic transport documents for freight transport,” European Commission, Brussels, 2018.

[28] AS Sertifitseerimiskeskus, “The Estonian ID Card and Digital Signature Concept,” id.ee.

[29] A.P. Moller – Maersk, “A game changer for global trade,” 2020.

[30] K. Jabbar and P. Bjørn, “Infrastructural Grind: Introducing Blockchain Technology in the Shipping Domain,” in *GROUP '18: 2018 ACM Conference on Supporting Groupwork*, 2018.

[31] H. Shi and X. Wang, “Research on the Development Path of Blockchain in Shipping Industry,” in *APCIM & ICTTE 2018: Proceedings of the Asia-Pacific Conference on Intelligent Medical 2018 & International Conference on Transportation and Traffic Engineering 2018*, Beijing, 2018.

[32] M. Levinson, The Box: How the Shipping Container Made the World Smaller and the World Bigger, Princeton University Press, 2016.