A Tracking and Tracing System for a Supply Chain

Miguel Ângelo Afonso Duarte Palma

Thesis to obtain the Master of Science Degree in

Segurança de Informação e Direito no Ciberespaço

Supervisor: Professor Miguel Nuno Dias Alves Pupo Correia

Supervisor: Doctor Leandro Cruz

Examination Committee

Chairperson: Professor Paulo Carreira Mateus

Supervisor: Doctor Leandro Cruz

Members of Committee: Professor Sérgio Guerreiro

December 2020

Acknowledgements

I express my thanks to all those who have somehow contributed to making this thesis possible.

First, I would like to thank Dr Leandro Cruz for the guidance of this dissertation. I am grateful that you believed in me, in my abilities and that you never gave up supporting me. I have no words to express all the commitment, availability, patience and dedication provided during this journey.

I thank, Prof Dr Miguel Pupo Correia, for having accepted me as your supervisor, for his presence, readiness and help in this dissertation's development. Additionally, I want to repay you for the friendship you put on this path, making it more fertile.

To Dr Alberto Lopez, I am grateful for the suggestions and exchange of ideas. Questions were raised, which, in a way, made the content of this dissertation richer.

I am grateful to the Imprensa Nacional-Casa da Moeda (INCM), particularly to Dr Sílvia Garcia, for the opportunity granted, for the attention and availability.

To my family and friends, I thank you for the affection and strength that you have always given me.

To my friend Alexandre Manso, I thank you for your patience, friendship and sharing good times.

It is with gratitude that I want to acknowledge the unconditional support of two wonderful people. Elvira and Rodrigo, thank you for your availability and friendship.

My special and loving thanks go to my parents, for the education they provided me, for the efforts they made, the patience, the presence and the encouragement. I embrace you in thanks for always walking beside me.

Finally, I want to thank my great love, Catarina Fortunato Martins, for having always believed in me, for always being by my side in good and bad times. Thank you for your kindness, love and tireless presence along this path.

Agradecimentos

Expresso os meus agradecimentos a todos aqueles que de alguma forma contribuíram para que esta tese se tornasse possível.

Em primeiro lugar, gostaria de agradecer ao Dr. Leandro Cruz pela orientação desta dissertação. Agradeço o facto de ter acreditado em mim, nas minhas capacidades e de nunca ter desistido de me apoiar. Não tenho palavras para expressar todo o empenho, disponibilidade, paciência e dedicação prestados durante este percurso.

Agradeço ao Prof. Dr. Miguel Pupo Correia por me ter aceite enquanto orientando, pela sua presença, prontidão e ajuda no desenvolvimento desta dissertação. Adicionalmente, quero retribuir-lhe a amizade que colocou neste caminho, tornando-o mais fértil.

Ao Dr. Alberto Lopez, agradeço as sugestões e troca de ideias. Foram levantadas questões, que de certa forma tornaram o conteúdo desta dissertação mais rico.

Agradeço à Imprensa Nacional-Casa da Moeda (INCM), em particular à Dra. Sílvia Garcia, pela oportunidade concedida, pela atenção e disponibilidade prestadas.

À minha família e aos meus amigos, agradeço o carinho e a força que sempre me deram.

Ao meu amigo Alexandre Manso, agradeço a paciência, amizade e partilha de bons momentos.

É com gratidão que quero reconhecer o apoio incondicional de duas pessoas maravilhosas. Elvira e Rodrigo, obrigado pela vossa disponibilidade e amizade.

O meu agradecimento especial e carinhoso, vai para os meus pais, pela educação que me facultaram, pelos esforços que fizeram, pela paciência, pela presença e pelo incentivo. Abraço-vos em agradecimento por caminharem sempre ao meu lado.

Finalmente, quero agradecer ao meu grande amor, Catarina Fortunato Martins, por ter sempre acreditado em mim, por ter estado sempre ao meu lado nos bons e nos maus momentos. Obrigado pelo teu carinho, amor e presença incansável ao longo deste caminho.

Abstract

Traceability systems can improve the overall operations efficiency and logistics, improve brand reputation, and are resilient against counterfeiting products. However, most traceability systems do not cover the entire supply chain or have systems that only cover the product information. Sometimes this can lead to trust issues between the stakeholders and the consumers.

On this work, we classify these systems into three levels according to the type of tracked information. Furthermore, we propose a general architecture for tracking and tracing (T&T) systems for a supply chain that contains several applications related to different stakeholders. We will analyse this architecture under the perspectives of security, privacy, transparency, performance, among others.

We focused on the decentralised case, more precisely, using blockchain. Blockchain is the right candidate for different applications and areas because of its features such as immutability, data integrity, and many others. Blockchain brings to supply chain a solution with useful features such as security, auditability, transparency and privacy.

To the best of our knowledge, there is no level three T&T system for a supply chain that covers a wide range of products. All known experiences are strict with a specific type of product. We believe that the absence of a system like this is because of the implementation costs and a lack of confidence of the participants. Besides those obstacles, we think that the big obstacle is to convince all entities to participate in the proposed architecture. Future research suggests a practical implementation and analysis of the proposed architecture.

Keywords: Traceability; Supply Chain; Blockchain; Architecture Analysis;

Resumo

Os sistemas de rastreabilidade podem melhorar a eficácia geral das operações e logística, melhorar a reputação da marca e são resilientes contra a falsificação de produtos. Contudo, a maioria dos sistemas de rastreabilidade não cobrem toda a *supply chain* ou monitorizam apenas uma parte das informações do produto. Por sua vez, isto pode levar a problemas de confiança entre as partes interessadas e os consumidores.

Neste trabalho, classificamos estes sistemas em três níveis e propomos uma arquitetura geral para uma *supply chain* que contém vários aplicativos relacionados com diferentes participantes. Analisámos esta arquitetura sob as perspetivas de segurança, privacidade, transparência, desempenho, entre outros.

Focamos no caso descentralizado, mais precisamente na blockchain. A blockchain é uma boa candidata para diferentes aplicações e áreas devido às suas propriedades como a imutabilidade, integridade de dados, entre outros. A blockchain traz para a *supply chain* uma solução com algumas propriedades úteis como a segurança, auditoria, transparência e privacidade.

Tanto quanto é do nosso conhecimento, não existe um sistema de rastreabilidade de nível três para uma supply chain capaz de cobrir uma vasta gama de produtos. Acreditamos que a ausência de um sistema como este se deve aos custos de implementação aliado à falta de confiança dos participantes. Para além desses obstáculos, pensamos que o grande obstáculo é convencer todas as entidades a participarem na arquitetura proposta. Sugerimos para o futuro pesquisas relacionadas com a implementação prática e análise da arquitetura proposta.

Palavras-chave: Rastreabilidade; *Supply Chain*; Blockchain; Análise de Arquitetura;

Contents

List of Tables

List of Figures

1. Introduction

Most businesses, if not all, have a supply chain. A *supply chain* involves all the processes and activities from which the material flows, ranging from raw materials to the end-consumer [1]. *Traceability systems* are an essential component in any supply chain, and they are characterised by "the ability to trace the history, application, or location of an object" [2]. These systems identify units of products with the ability to register information about when and where these units were moved or transformed. Those systems can also link all data and transfer the relevant information about the product to the next stage of the supply chain [3].

Traceability systems bring a set of benefits to the supply chain, such as **(i)** improvements in logistics and overall operations efficiency, **(ii)** brand reputation, and **(iii)** resilience against counterfeiting, tax evasion and unsafe food. They also meet stakeholder's increasing demands ensuring product authenticity [4].

Nowadays, it is possible to observe a proliferation of these systems with logistic traceability solutions for specific contexts. For example, when someone sends a package using the courier, both the sender and the receiver are able to know the package's location at any given point in time. When a company buys raw materials or distributes a manufactured product, it may want to know who is involved in the transportation and where this product is. This process gives the company more control over the supply chain, improving production and storage planning, which, in turn, improves efficiency and reduces costs.

Moreover, the increased efficiency and cost reduction allows for an improvement in production and price reduction. Additionally, transparency of information is essential to build trust and strengthen the relationship between a consumer and the product. Both aspects collaborate to improve brand reputation.

Finally, one major problem that affects supply chains is product counterfeiting, whose proliferation could be significantly reduced by improved means of traceability. *Counterfeiting* is an illicit business in which items try to imitate a legit product. These fake products can be dangerous and even pose risks to the consumer's health. The illegitimate selling of counterfeit products has wide-ranging impacts in society, e.g. by affecting revenues of legitimate businesses, hence impacting their ability to continue their activity and secure people's jobs [5]. Pharmaceutical counterfeiting is one of the areas in which illicit trade can not only affect people's income but put at risk their lives. The World Health Organization (WHO) estimates that 1 in 10 medical products are substandard or falsified in developing countries [6]. Aside from pharmaceutical counterfeiting, there is also a problem related to food supply chains,

particularly unsafe food. According to the Center for Disease Control and Prevention (CDCP), during 2017, reports have shown that a total of 841 foodborne diseases resulted in 14.481 illnesses, 827 hospitalisations, and 20 deaths [7].

In this work, we consider three levels for traceability systems. The higher the level, the more complete the traceability system will be. On the first level, there is traceability only for product identification. This product identification is widely used from factories to retail, but it is not broad enough to cover the entire supply chain. The second level adds product identification and geographical position along with the transportation and production flow (the stakeholder in possession of the product at a specific time). This traceability system covers most of the entire supply chain, although there is a lack of information about the supply chain's product conditions and properties. The third level adds to the previous one, the product properties along the entire supply chain. This level gives more transparency and control over the traceability system.

GS1 [8] is an international not-for-profit organisation that has focused on improving traceability in supply chains. GS1 has a global solution that enhances the supply chain's visibility with improved traceability and transparency. It has an international identification standard that helps in identifying and authenticating a product in real-time.

There are several initiatives for implementing traceability systems for supply chains of levels two and three. Nevertheless, all of them address specific solutions: a supply chain for a specific product, or even only part of the chain for a specific product. Some of these solutions use *auto-ID technologies* and other *IoT* tools to measure different properties of the tracked product [9]. Auto-ID technologies provide all the available solutions for tracking and tracing the logistics network [10].

These initiatives and the traceability system levels bring us to the research question: Why there is not any solution for a level three traceability system that can be applied to any supply chain? In this research, we are showing that the technology is mature enough to have such a solution (both for the centralised and for the decentralised case). The centralised case is widely studied and known. We look to better evaluate the decentralised case to see if it is also mature by focusing on blockchain technology. Therefore, we propose a *tracking and tracing* (T&T) system architecture for a supply chain that goes beyond the GS1 solution. The proposed architecture is a justification that we have the needed technology to create a global solution that includes a level three traceability system.

1.1. Objectives

This master's thesis's main objective is to propose a tracking and tracing (T&T) system architecture for supply chains. The proposed T&T architecture is presented as a solution for either a centralised and decentralised supply chain model.

The present dissertation contains the following specific objectives:

- A proposal of the T&T architecture model for the supply chain. The proposal demonstrates the different components of the architecture and how they interact with each other.
- A proposal of three different levels for traceability solutions, where the proposed T&T architecture was designed to include all three levels.
- A proposal of a blockchain supply chain, which is the implementation of blockchain in the proposed T&T architecture.
- A comparison and analysis of different properties from centralised supply chain and blockchain supply chain architectures.
- A demonstration of how blockchain and T&T technologies interact with the proposed architecture.
- An alternative solution to blockchain supply chain, where it uses centralised and blockchain systems.
- A review and comparative analysis of the different T&T technologies used in supply chain systems.
- A theoretical analysis of the different properties of the blockchain supply chain architecture.

1.2. Dissertation Structure

The thesis is organised as follows. In the first chapter, we lay out our motivation, objectives, and contributions to existing literature. The second chapter presents a literature review focused mainly on scientific papers and books about the tracking and tracing systems. The third chapter is the core of the thesis and covers the dissertation's primary objective: the proposed architecture for a tracking and tracing system. The fourth chapter follows the same idea of the second chapter, where it introduces blockchain. The fifth chapter discusses how blockchain can be implemented in the proposed architecture. It also demonstrates how T&T technologies can be implemented in the proposed T&T architecture and how they interact with the different architectural components. The sixth chapter introduces security as a fundamental component for the T&T systems for supply chains. The seventh chapter introduces a theoretical analysis of the proposed architecture properties. This chapter also discusses the benefits of accreditation and certification in the proposed architecture and trust as a subjective property in the proposed architecture. The eighth and last chapter discusses and summarises our work to clarify and respond to the objectives and motivations described in the introduction. Additionally, some of the present work's limitations are put forward, suggesting topics for further research.

2. Tracking and Tracing Systems

GS1 is the only organisation, non-profit and originally founded in 1974, with the trusted role of Issuing Agency for unique object identifiers [8]. GS1, in 2007, introduced a Global Traceability Standard (GTS) to assist organisations and industries in the design and implementation of traceability systems [2].

The GS1 Global Traceability Standard (GTS) [2], defines *traceability* as "the ability to trace the history, application, or location of an object. When considering a product or service, traceability can relate to the origin of materials and parts, the processing history, and the distribution and location of the product or service after delivery". Traceability can be divided into two processes: *tracking* and *tracing*.

Tracking and Tracing (T&T) are two terms with different meanings but both important in a supply chain system. *Tracking* is the process where the product details of each production stage are recorded (Figure 1). *Tracing* is the inverse process of tracking. The history and responsibilities at different stages of the cycle (from the client to the origin of the product) are followed (Figure 1). In a traceability management system, there is an internal and external traceability activity. Internal traceability is where the product's origin, the process operations, and the final destination of the product are traced. The external activity is supply chain traceability, where a specific product unit is followed along the production chain [11].

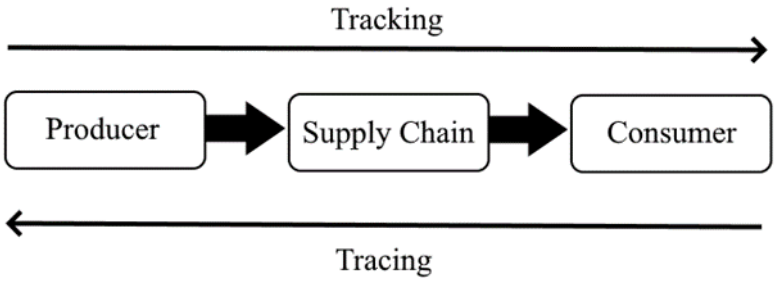

Figure 1 - Tracking and Tracing system [11]

On this work, traceability systems are classified into three different levels (Figure 2). The higher the level, the more complete the traceability system is.

At the first level, the traceability system is only able to identify the product. Product identification is an essential feature, widely used, from factories to retail, but it is not broad enough to cover the entire supply chain [12]. An example of this type of system is the barcode containing the product's identification, where this identification is unique per product batch. It could also be achieved using RFID, simplifying the product identification process. Another example of level one would be identifying the product in different stages of the supply chain

only by reading the barcode attached in the product. Many distributor companies do this type of traceability.

The second level is more complex than the first one and includes the identification of the nodes (geographical position or entity that holds the product at that time) from where the product flows. This additional feature could be achieved, for example, by technology like GPS, plugged in the product. Another option is to add an RFID in the product, which is automatically scanned by a geographically referenced system, for example, if this system runs in a transportation truck [12]. This second level has a better T&T system than the first one because it has a broad application in the supply chain. It is possible to trace each node from where the product flows, which leads to better security against counterfeit products in the supply chain.

The third level can trace all the properties of raw materials or products along the supply chain. This level extends the control and transparency of the traceability system, which can be very beneficial, for example, in an agri-food and health systems. IoT technologies can be a handy tool on this level. For example, smart IoT sensors or other smart devices can gather information about the products in real-time [13].

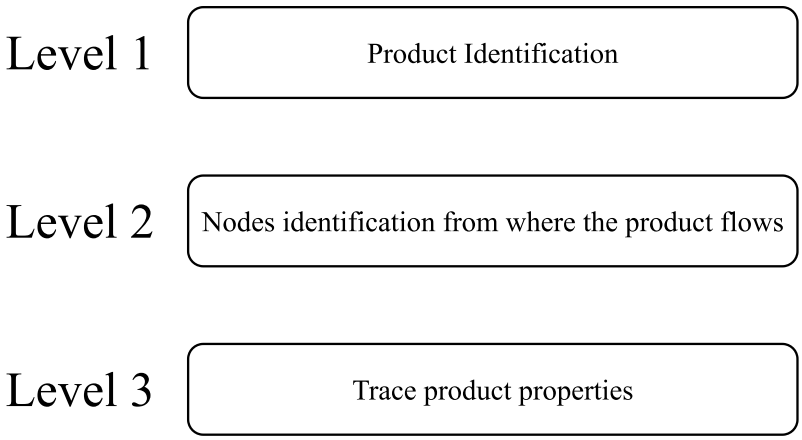

Figure 2 - Classification of traceability systems in three different levels

Nowadays, it is considered necessary for global manufacturing companies to monitor and manage logistics in supply chain networks. The monitoring is related to the tracking and tracing in supply chain logistics and delivery network, which is one of the driving factors to build trust among suppliers, manufactures and customer satisfaction [10]. In this way, level three of T&T systems will probably become more common in supply chains. It will increase the trust between all entities in a supply chain (Section 2.1) and will use all types of emerging auto-ID technologies (Section 2.3).

2.1. The Trust Chain

The relation between trust and traceability is tight. Traceability increases trust for several reasons. For example, it is possible to achieve transparency and effective communication with traceability, which leads to increased trust. Trust can enhance the overall performance, improve flexibility, responsiveness and cost reduction of a supply chain [14]. Trust is one of the most critical factors in a committed and collaborative relationship between supply chains partners. It can be performed over a B2B (*business to business*), B2C (*business to consumer*), or a B2B2C (*business to business to consumer*) flow.

In the B2C case, the business sells products or services directly to the end-consumer without an intermediary. In this case, the business will be able to monitor how its product reaches the consumers. A B2B flow is when the consumer is also a business, for example, an outsourcing service, or a material supplier. This work focuses more on the second case. For example, a producer (second B) buys a product from its supplier (first B). In this case, the consumer wants to know the production per distribution stage to improve its planning.

These concepts can be combined into a B2B2C flow. For example, a producer (first B) hire a distributor (second B) to deliver its product to the final consumer (C). Both consumer and producer can obtain several advantages of proper traceability of the product along this chain, which will improve the trust between all these parts.

There are several examples of T&T for the supply chain in the three levels. However, there is no universal system that contains wide traceability of the products, more precisely, the third level of traceability. Why? The chain of trust with different types of stakeholders shows that in addition to technological challenges, the management challenge of the parties involved can be quite complex. An in-depth analysis of this aspect is outside the scope of this thesis. Still, it is essential to mention that this aspect has been the main obstacle for level three T&T systems for supply chains. This assumption is based on the fact that the technological part is increasingly well developed with regard to the necessary elements of this system.

From a technological perspective, there are many issues related to the implementation of a robust system capable of being used by different types of users (different usability requirements), in different places (data transmission), and able to manage the high volume of data (databases). All of this demands a good trust relationship between the participants and high security in the traceability system. Besides the technological challenges, the management challenges are still the most significant limitation for a traceability system. Nowadays, technology implementation is more viable due to advances in networks, cryptography, auto-ID

technologies, and many others (particularly the recent ascension of blockchain technology). It indicates that the lack of a third level T&T system for the supply chain is not only a technological matter but also a management/political issue.

Regarding management, it is essential to integrate all stakeholders in the complex chain, each with different business interests, and often in places with different jurisdictions. It builds a non-trivial management challenge for a massive T&T solution. There are already initiatives related to the management process of traceability systems. For example, GS1 introduced the barcode in 1974 and convinced governments and industries worldwide to adopt it [15]. Also, traceability systems for products such as tobacco and alcoholic beverages need to pay specific taxes, where these products are widely managed and controlled to fight against tax evasion. For example, in Europe, there is a system called Id Issuer that controls the tax stamps for tobacco [16].

2.2. Traceability Flow in Supply Chain

Figure 3 shows an example of a product flow in a T&T system, where a manufacturer or accredited authority initially codes a product. Afterwards, the product flows through *n* distribution entities, where each distribution entity updates the information until it reaches the end-customer [17].

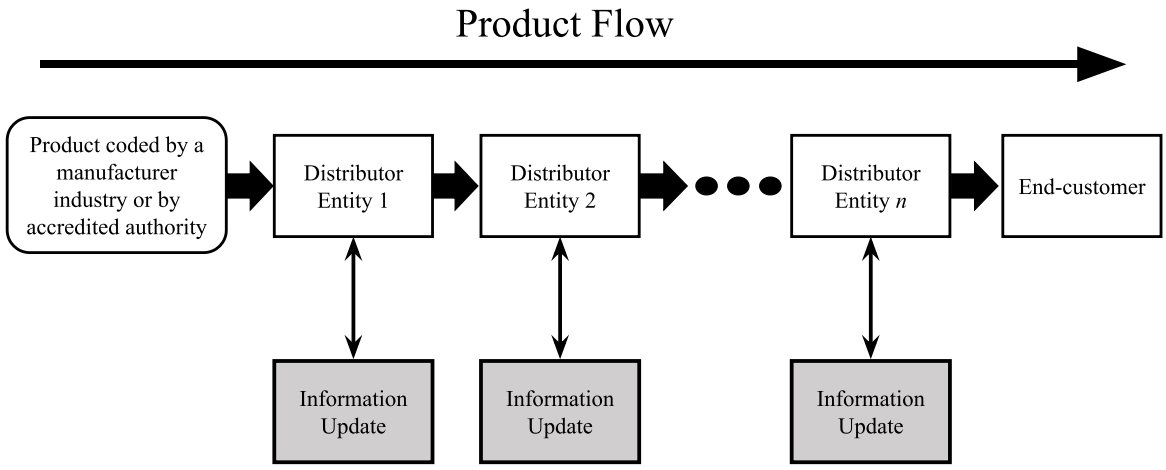

Figure 3 – Product flow in a supply chain [17]

This product flow can be aggregated into multiple product flows, where each product flow represents an interaction between two entities (Figure 4).

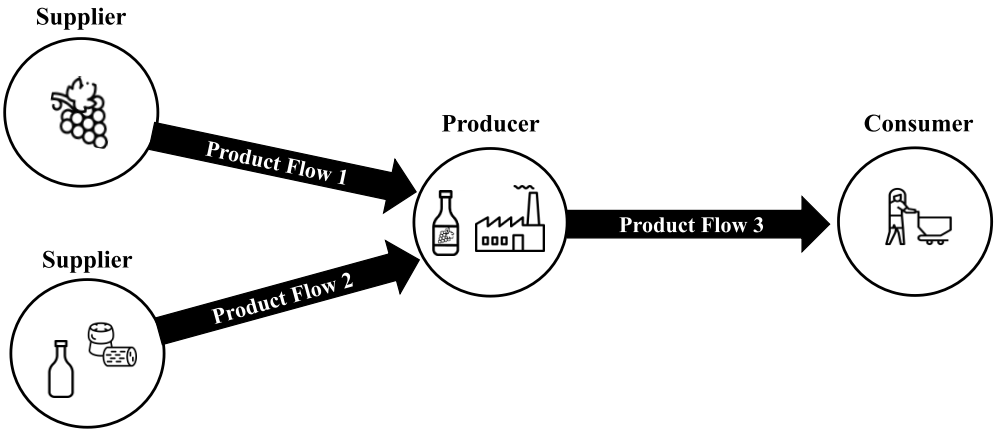

Figure 4 - Multiple products flow across the supply chain

As shown in Figure 4, a product flow could start from a supplier and end in the producer, where the producer is the end-customer because it receives the raw materials to manufacture the product. Each supplier has its own product flow with the producer. Another product flow would start from the producer and end in the consumer, where retail stores would act as an intermediary of the product flow.

On multiple product flows, the traceability information goes from the supplier to the consumer. Currently, in terms of applicability, according to the IMR (Instituto de Marketing Research) [18], traceability systems trace all phases of the supply chain (product flow) from raw materials to the supermarket.

Aside from this product flow, it is essential to distinguish both traceability and supply chain since both terms are part of this flow. A supply chain "encompasses all the processes and activities that lead from the initial raw materials to the final finished product, as well as all the functions and services within and outside a company" [1], and as mentioned above, traceability is defined as "the ability to trace the history, application, or location of an object" [2].

It is essential to mention that there is an absence of a broad traceability system like the one presented. However, as mentioned earlier, there are already partial solutions capable of reaching some extent [12], [13]. It may be desirable the proposal of a broad solution capable of being integrated into these partial solutions.

2.3. Auto-ID Technologies

A tracking and tracing system can be widely enhanced by using automatic identification (auto-ID) technologies. Auto-ID technologies are technologies that provide all the available solutions for tracking and tracing the logistics network. This type of technology enhances the management and control of products, making life easier for logistic services. It is crucial to keep in mind that there are various auto-ID technologies. Each one of them has a distinctive feature, which, at times, makes it challenging to select the best technology [10].

Over time, retail and manufacturing companies have grown an interest in auto-ID technologies. As for auto-ID technologies in tracking and tracing, there is the *Bar Code*, *Quick Response Code* (QR Code), *Radio Frequency Identification* (RFID), *Radio Frequency Data Capture* (RFDC), *Real-Time Location Systems* (RTLS), and *Global Positioning System* (GPS) [10]. The most common and widespread technology for encoding data is the *bar code* [11]. GS1 standard frameworks support other data carriers for traceability in supply chains such as QR Code and RFID. These technologies can store product information across five dimensions: what, who, where, when, and why, giving the ability to track and trace a product at any stage of the supply [2].

The *barcode* is categorised as a one-dimensional information entity, where the representation of data is in the form of parallel lines and spaces between them. The barcode contains essential information about the product and is read by barcode readers [10].

There are different types of barcodes, where one of the most common ones for supply chains, particularly in Europe, is the EAN (International Article Number). Initially, the EAN was also known as European Article Number. However, it was later renamed as International Article Number because not only it could be used as a product identifier in Europe, but also it could be used in other points of the world. There are two types of EAN: EAN-8 with eight digits, and EAN-13 with thirteen digits. The EAN-8 is a shortened version of the EAN-13 barcode, and it is mainly used for smaller sized packages, such as candies or cigarettes. In the EAN-8, the eight digits are divided into two sets of four (Figure 5), with two country digits, five data digits that identify the product and a final check number [19].

Figure 5 - EAN-8 bar code example

EAN-13 is the most recognised barcode in Europe used in different types of supply chains. This code is used for large-sized packages when EAN-8 cannot be used. From the thirteen digits (Figure 6), the first two are a GS1 Prefix that identifies the product country of origin. The next five digits identify the company, the following five digits identify the product, and the last digit is a check number [20].

Figure 6 - EAN-13 bar code example

The QR Code is also known as a two-dimensional bar code and is readable by dedicated QR Code readers and mobile phones with a camera (Figure 7) [10].

Figure 7 - QR Code example with a text inside it

The QR Code is a second-generation barcode and is called a two-dimensional bar code because the information is read both horizontally and vertically [21]. It contains much more information than one-dimensional barcodes, and they can be quickly read. For this reason, the QR Code is widely used for several purposes, including traceability.

As a curiosity, Leandro Cruz et al. [22] developed a new Machine Readable Code (MRC) called Graphic Code. This MRC has two significant advantages: aesthetics and larger coding capacity, opening the possibility to be used for identification and tracking. Later on, the Imprensa Nacional - Casa da Moeda (INCM) along with the University of Coimbra developed an MRC called UniQode. The UniQode offers a unique identifier that can be validated through a smartphone, making this a versatile tool to fight against counterfeit products, promoting trust in the market [23].

Based on radio frequencies, the RFID system is composed of a reader and a tag, that reacts in the presence of an electromagnetic field emitted by the reader. The reader is responsible for reading the tag contents and for writing in the tag. The tag contains a limited amount (about 2KB) of user-addressed data stored in a chip [10].

The RFDC technology uses an auto-ID technology to read or identify any object and data capture that collects the read data by the auto-ID technology and sends it to a computer system [10].

Another auto-ID technology is the RTLS, a system that continuously monitors an object or product's location in real-time. Real-time tracking is achieved by tags and readers, where the tags are attached to the objects, and the readers receive wireless signals from the tags to determine their location [10].

At last, the GPS provides the capability to monitor assets from any location in the world remotely. This system can operate entirely on battery, giving an almost precise location of the monitored asset or other related information [10].

Each auto-ID technology has its features, and in Table 1, we compare all the technologies mentioned above against the following a set of features.

- *Line of sight* relates to how technology can read or scan a product;
- *Reading work* indicates whether the reading or scanning is performed manually by the user, or whether it is automatic, without the user's intervention;
- *Ambient lighting arrangement* evaluates the need for light in the area to read or scan;
- *Durability* describes how resistant to adversary conditions or harsh environments the technology is;
- *Ability to store information* refers to whether it is only possible to read information about the product, or if it is possible to read and write;
- *Cost* of each technology is compared descriptively but without a specific value;
- Each technology's *security* is a vital feature, and it is evaluated by comparison with other technologies;
- The last feature compared in the table is *device support*, which describes which devices support the mentioned technology.

Table 1 - Adapted Table with a comparative analysis of different T&T technologies [24]

Features	Barcode	QR Code	RFID	RFDC	RTLS	GPS
Line of sight	The scanner must physically see to scan the bar	The scanner must physically see to scan the bar [25]	Can only be used within the read range	Can only be used within the read range [10]	Can only be used within the read range [10]	Long read range
Reading work	Manual	Manual [25]	Automatic	Automatic [10]	Automatic [10]	Automatic
Ambient lighting arrangement	Works well in well-lit areas	Works well in well-lit areas [25]	No ambient lighting needed	No ambient lighting needed [10]	No ambient lighting needed [10]	No ambient lighting needed
Durability	Easily scratched and not readable if dirty, greasy, or wet	Damaged tags may work, 30% data recoverable [25]	Better protection and can withstand harsh environments	Depends if used with bar code or with RFID [10]	Adequate protection in general [10]	Can be kept inside a strong container
Ability to store information	Read-only	Read-only [25]	Read and writing tag	Read-only [10]	Read-only [10]	N/A
Cost	Cheaper than RFID	Cheaper than RFID, but higher than Barcode [25], [26]	Cheaper than GPS	Expensive	Inexpensive [10]	Most expensive option
Security	Highly secure	More secure than Bar Code [21]	Possible security risks due to wireless connections	Possible security risks due to wireless connections [10]	Possible security risks due to wireless connections [10]	Secure
Device support	Easy to support bar code in any camera-enabled-mobile	Any application that reads QR Code or the mobile phone camera [25]	Extra hardware needed	Extra hardware needed, such as a computer [10]	Extra hardware needed [10]	Supported by mobile devices

From this table, it is possible to observe that each technology has its advantages and disadvantages. When using these technologies, it is possible to use more than one at a time, but this solution comes with higher costs.

Shamsuzzoha et al. [10] evaluated three T&T technologies' performance in the logistics network: Barcode, QR Code, and RFID. Based on each technology's advantages and disadvantages, the authors concluded that organisations might use RFID tags for T&T logistics. In some circumstances, a barcode can be used. They also mention that it is essential to consider the flexibility and quality of the T&T system. For example, the cost of maintaining an RFID reader and tags is higher than a QR Code or a barcode. However, in terms of readability and durability, the RFID proves to be better. It is crucial to analyse each option before deciding which one is more suitable to use.

Organisations might choose one or more technologies that can be combined for better quality and efficiency of the T&T system. For this purpose, it is essential to know the pros and cons of auto-ID technologies. Furthermore, it is also essential to know some of T&T auto-ID technologies' applications in the real-world context. In the next section, it will be presented some of these applications.

2.4. Applications of T&T auto-ID Technologies

One thing that T&T auto-ID technologies share in common is that all of these technologies are applied to the tracking and tracing of assets in a business environment. However, each one of them may differ in terms of applicability in a real-world context.

Barcodes are applied to postal services, retail stores, and supply networks to track the available products [10]. Barcode technology finds applications in inventory control, production control and monitoring attendance [27]. For example, a study shows the application of barcode technology in warehouse management and logistics, where the Barcode can enhance the management level while bringing economic benefits for logistics enterprises [28]. Barcodes 1D and 2D depend on visual systems to read the code and parse the encoded information. This type of system works well in a controlled environment but can be challenging in wild spaces. However, this technology is still relevant in several contexts, and there are still researches and innovations in Barcode technology. For example, a recent study demonstrated the Barcode usage to track the calories of the product that the end-user wants to consume, recording the user's daily calories and further suggesting the required calories so that the end-user can maintain a healthy lifestyle [29].

The QR Code was created for tracking items and is used in many areas such as retailing, healthcare, transportation, and manufacturing. It has also been applied in other fields such as electronic payment, tampering detection, electronic ticket, coupon, and many others [30].

RFID has been used in biometric technology for security purposes. However, it can be used in clothing, non-metallic materials, and in the human body [10]. Besides the mentioned, RFID is also used for assets management to determine an item's presence. For tracking to determine an item's location, for authenticity verification to verify an item's source, for automated payment to conduct a financial transaction and for matching to ensure that affiliated items are not separated [31].

The RFDC is used in tracking commercial goods [10], although there is a lack of bibliography around this type of technology. RTLS is used in various sectors such as military, healthcare, postal services, retails, navigation, recreation, and many other sectors [10]. An application of RTLS is the use of this technology to monitor material flow, providing a view of weak spots in production processes. For example, it can be used to determine the cause of production delays [32].

Lastly, GPS technology has become more of a consumer product since it has many applications [10]. GPS can be used to evaluate road traffic congestion, for terrorism where it can be possible to determine a terrorist attacker's location, and for tourism where it is possible to gather information and points of interest based on a location instance. It can also be used for disaster relief, where it is possible to predict based on location and timing earthquakes and flood wildfires, and many others. [33].

A recent study about COVID-19 used GPS and other localisation and communication technologies to detect and control the diffusion of COVID-19. This study detected infected individuals and traced their prior contacts using localisation and communication technologies to isolate individuals likely to have been infected [34].

Different technologies can have different applications depending on the scenario. Technologies like QR Code and GPS have more applications besides supply chains than the other mentioned technologies because the other technologies may not have proven useful or efficient in other areas. Their true potential in the other areas still needs to be discovered.

2.5. T&T Use Cases

Before presenting the proposed solution, it is essential to mention two different use cases to compare both use cases with the proposed solution. The first use case includes a supply chain with one central entity responsible for the T&T system, and the second use case is based on multiple entities responsible for the T&T system.

Both use cases can be either a centralised or decentralised system. However, the second use case is more achievable in a decentralised case scenario due to increasing trust in this approach. The supply chain entities can be summarised as a supplier, distributor, producer, retailer, and consumer. The supplier is responsible for providing raw materials to the producer. The producer acquires the raw materials from the supplier, uses the raw materials to produce the product, and sells it to the retailers. The distributor is the middle man of transferring goods between the seller and the buyer. The retailer purchases a batch of products and sells directly to the consumer in the retail. For last, the consumer buys and uses the product.

2.5.1. Use Case 1

Use case one is based on a central entity is responsible for the T&T system. As an example, Figure 8 shows a wine supply chain, where the producer is the central entity responsible for the supply chain system. The producer is a trusted entity in the system, which means that it can make decisions considering all the business entities participating in the supply chain [35]. Therefore, this entity can assure the other network participants that this solution is reliable, whether this solution is centralised or decentralised. This central entity plays a vital role in the management of this network.

There is a possibility of implementing a cloud service on this use case. The producer, which is the central entity in this case, could use a cloud service instead of using their server and storage systems for the supply chain. For the cloud service, it could use infrastructure as a service (IaaS), where a private cloud would assure the server and storage instead of being the central entity. In this case, the cloud service would give more scalability in the supply chain, where the supply chain can grow without worrying about the IT resources [36].

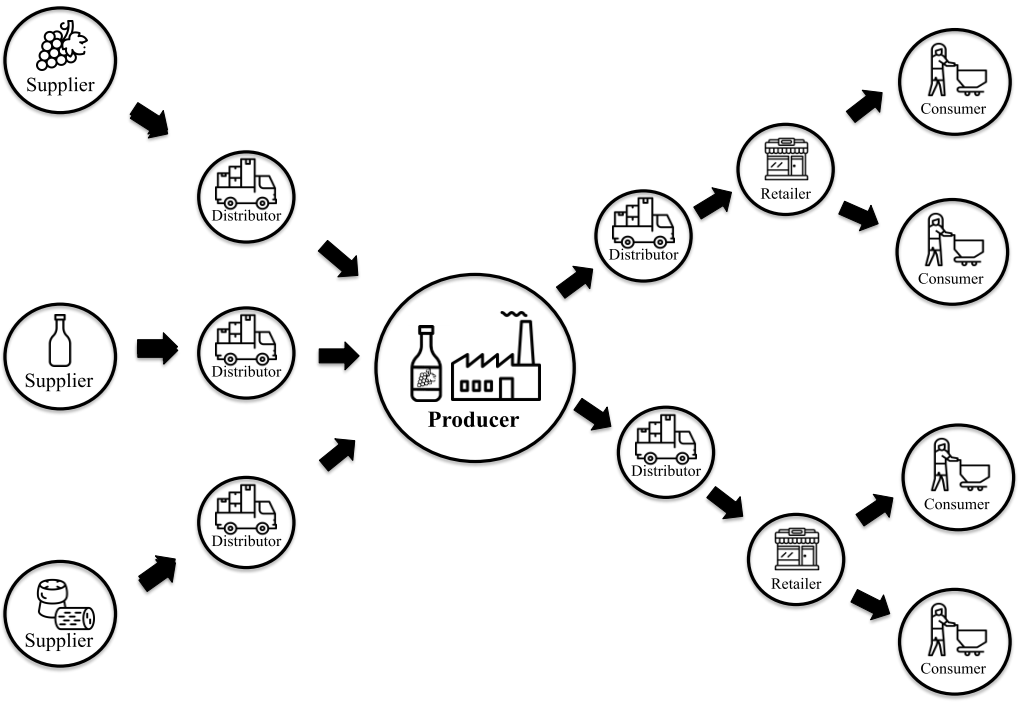

Figure 8 – Central entity supply chain example

When referring to Figure 4, it is possible to observe multiple products flows on this example. There are three product flows from the three different suppliers, and that same flow ends at the producer. Then the producer starts a new product flow with the retailer. It is essential to mention that the producer, distributor, and retailer can split this product flow into more product flows.

2.5.2. Use Case 2

Figure 9 shows a use case of a juice supply chain. There are multiple producers on this supply chain where each producer is treated as a separate business unit. Each producer makes their own decisions focusing on their own business. Each one is working locally and independently, which increases the local control and increase the local appearance [35]. In this way, bringing all network participants to a unified solution is much more complicated. A decentralised and highly reliable system would benefit the managers of each entity to embark on the solution.

This use case could also use the same cloud services from the previous use case. An entity, outside of the supply chain, would be responsible for assuring the cloud servers for the entire supply chain or for different supply chain entities. The benefits would be the same as described in the previous use case [36].

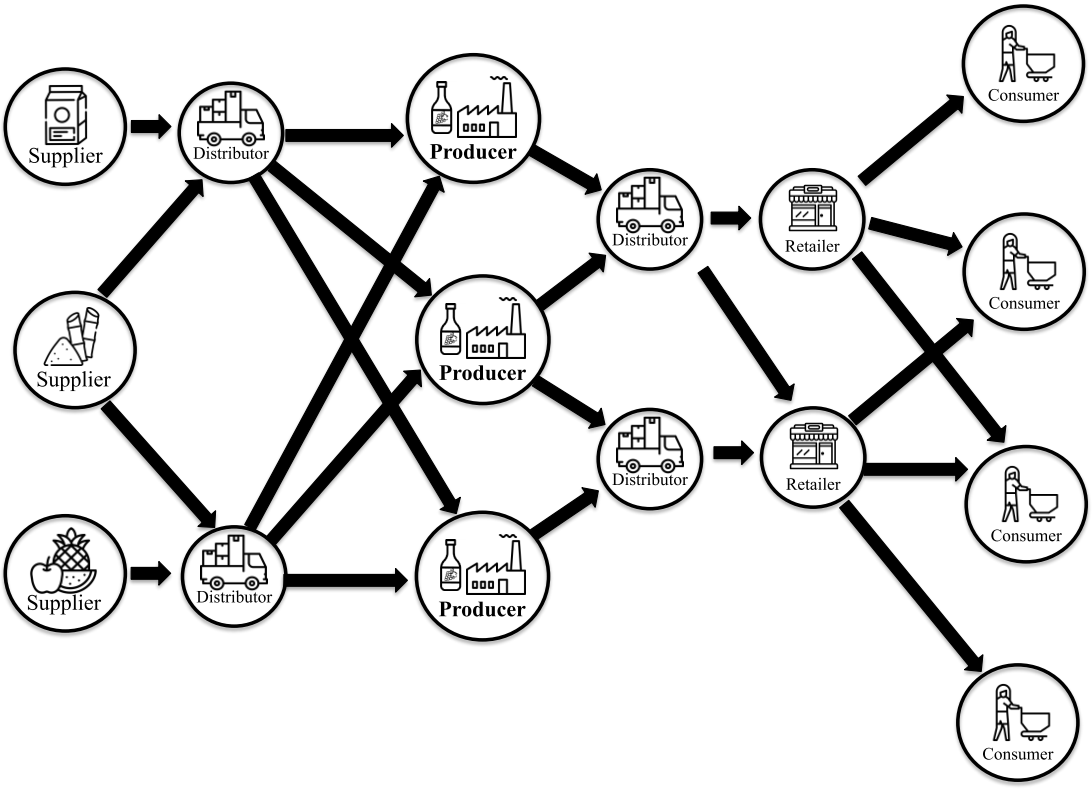

Figure 9 – Multiple entities in the supply chain example

On this example, it is also possible to observe multiple product flows (Figure 4), where it applies the same logic as explained in the use case one. However, instead of one producer, there are three producers, which means that there are even more product flows than the previous use case. Also, the supplier can split the product flow into different distributors for different producers.

In both use cases, it is possible to observe different product flows. A traceability system should cover the whole supply chain, more precisely, it should cover all the product flows of the supply chain.

3. T&T Architecture Proposal

This chapter will introduce a Tracking and Tracing architecture that can be used mostly for a supply chain system on levels two and three (level one can be implemented without connecting parts). The proposed architecture can be implemented both in a centralised and decentralised way. In centralised, there will be a central implementation of the business model's logic and the database. In decentralised, both business model and database are implemented in nodes. We will demonstrate how to implement the architecture in both ways. However, we will focus more on the decentralised case, since the centralised case has been extensively studied over the past few decades. It is also worth mentioning that one of the objectives of this thesis is to demonstrate how to implement the decentralised case using a blockchain. Throughout this chapter, we will be keeping the discussion generic, leaving the specific details for the next chapters.

3.1. Proposed T&T Architecture

The proposed architecture is composed of two main elements: the kernel and the applications. The kernel processes the business rules and stores the system information, and the applications are responsible for acquiring data and displaying information. The data captured by the different applications are sent to the kernel that will process them and eventually return a response. Also, the applications are used as an entry to consult the stored data. It is considered an integral part of the kernel's activities intrinsically related to the traceability of the product and its properties. Secondary tasks such as the inference of properties, specific transactions to stakeholders that do not need to be shared with other nodes, functionalities to improve applications' usability, and many others will be considered integral parts of the applications. This work will not detail these features as they can be quite different from case to case. We will focus on what is seen as a common part of any traceability system for a supply chain.

In the proposed architecture, the application nodes can communicate with the T&T kernel through four primary operations:

- **Node setup**: All the participating entities require the node setup to invoke transactions. This step is only required if the participating entity is not already enrolled in the T&T kernel.
- **Notification**: In notification, the entity gives information about the current state of the product.

- **Registration**: In registration, the raw material or the product is registered on the transaction. It is described details such as the ID of the product/s, temperature where the material was stored, date and time of the product creation, and other details. These details are different depending on the supply chain and depending on the supply chain stage.
- **Consultance**: This is a generic and a customised event, where the nodes can retrieve specific information from the T&T kernel through an API in the node application.

The four mentioned operations were proposed based on the European Commission Business Innovation Observatory case study [37], and also on what we think a T&T system must have to assure a level three traceability system. The number of operations proposed on this work is not limited to these four. There is the possibility to add more operations based on the business needs.

Figure 10 illustrates all the operations between the application node and the T&T kernel in the architecture.

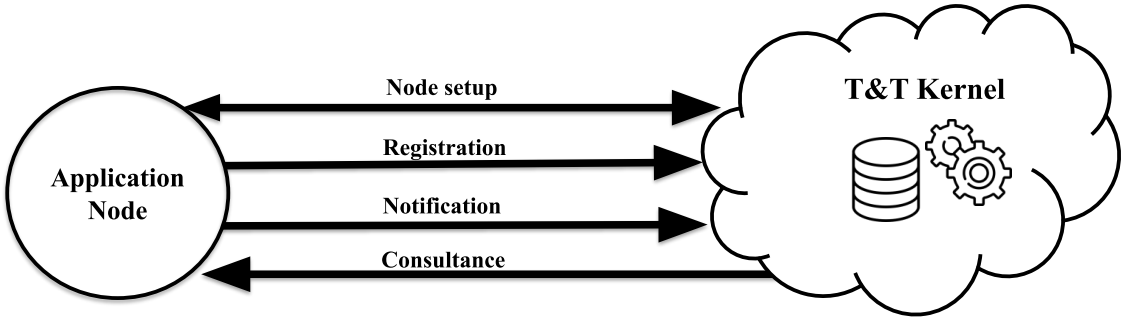

Figure 10 - Operations between the application node and the T&T kernel in the proposed T&T architecture

In section 3.2, we will introduce a use case for this architecture applied to the supply chain. We will describe how to instantiate four types of application nodes for this context.

Besides the operations between the application node and the T&T kernel, the proposed T&T architecture will have four main components (Figure 11). These four components are part of the T&T kernel, and those are business rules model, database, network and user authentication system.

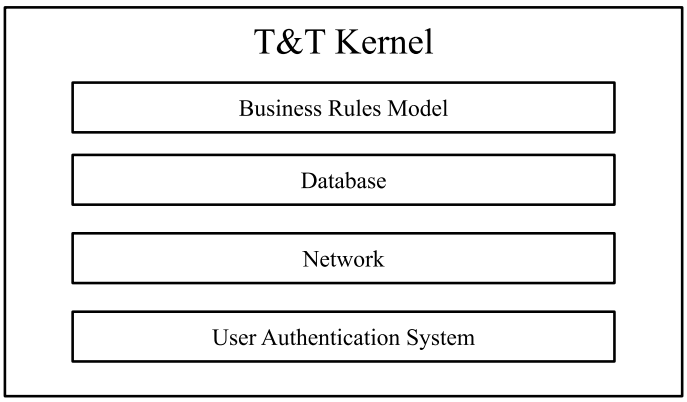

Figure 11 - Components of the T&T kernel

Business Rules Model is one of the essential components of the T&T kernel. The business rules model is responsible for shaping a business's behaviour and guide the behaviour of the business's employees. The business rules explain what is and not allowed, and it explains the consequences of violation. This model is essential because it is possible to achieve training and learning, software requirements, communication, managing compliance, direct execution and knowledge management [38].

Another component of the T&T kernel is the database. A database is an organised collection of information that a user can access through an API in a computer system. On this work, we will only mention the centralised database and decentralised database.

The network is another component in the architecture that allows the communication between the application node and the T&T kernel. The network also contains a gateway, which has a set of policies related to the user's authentication and management in the system.

For last, we have the user authentication system, a verification system responsible for confirming the user's authenticity. Each one of these components will be discussed later in the centralised and decentralised architecture components sub-chapter.

3.2. Application nodes: A use case

After explaining the different operations of node applications with the T&T kernel, it is important to give some examples of each entity operations with the T&T kernel. Figure 12 illustrates an example of the proposed T&T architecture, where it is possible to observe each different node application connected to the T&T kernel.

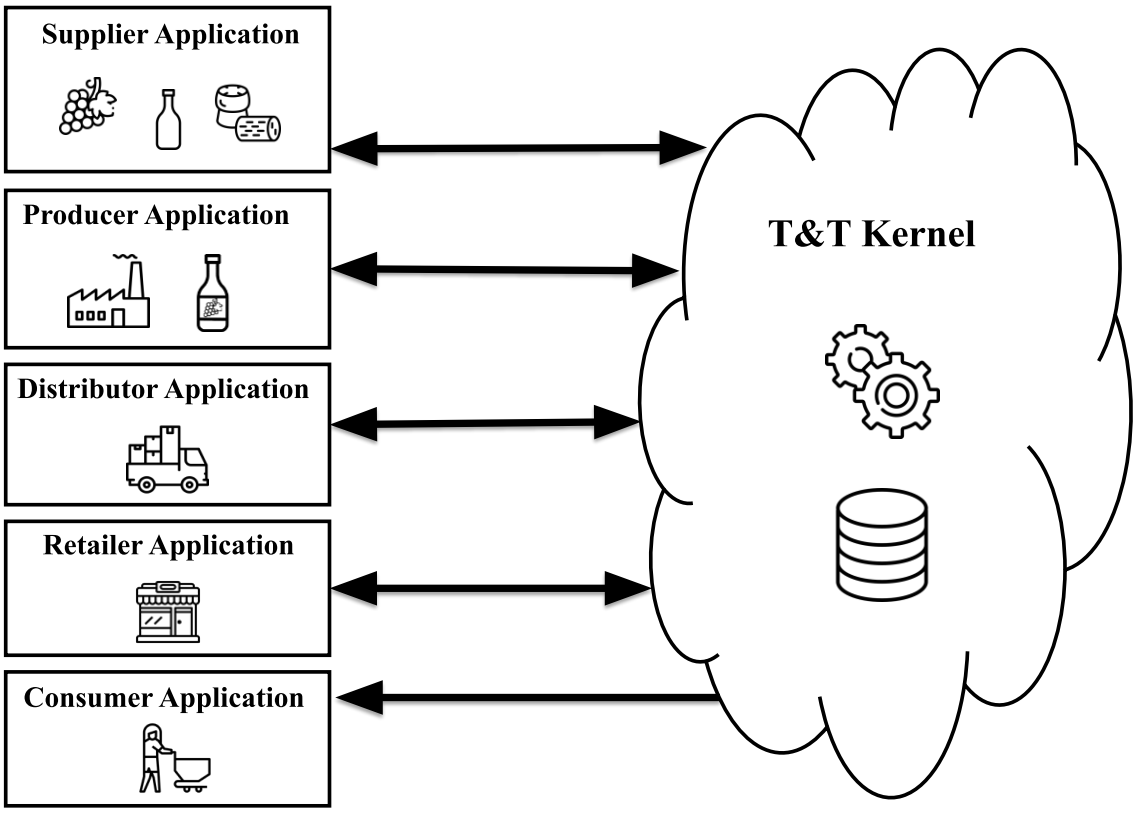

Figure 12 – Example of the proposed T&T system architecture

The supplier application has a node setup, registration, and notification interaction with the T&T kernel (Figure 13). In terms of traceability, the supplier should register the raw material source, where each raw material has a unique code. It should also notify when the raw material departs to the producer, explaining the quantity of raw material dispatched, the distributor responsible for the transportation, and other details. The registration and notification details should be followed according to the business rules model.

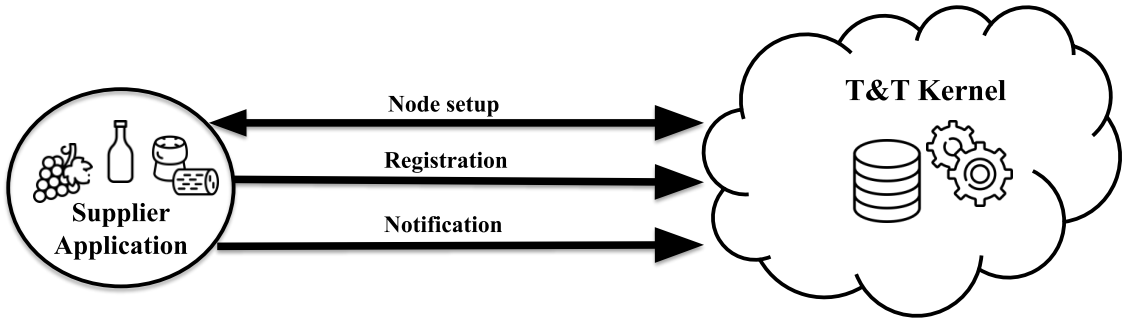

Figure 13 - Supplier Application interactions with the T&T kernel

The distributor application has a node setup and notification interaction with the T&T kernel (Figure 14). The role of the distributor is to inform the path of the product flow continuously.

In notification, the transaction will contain different types of information related to product transportation, such as the location of the product at different dates and times tracked by a GPS, for example, the temperature where the products are stored and other types of information.

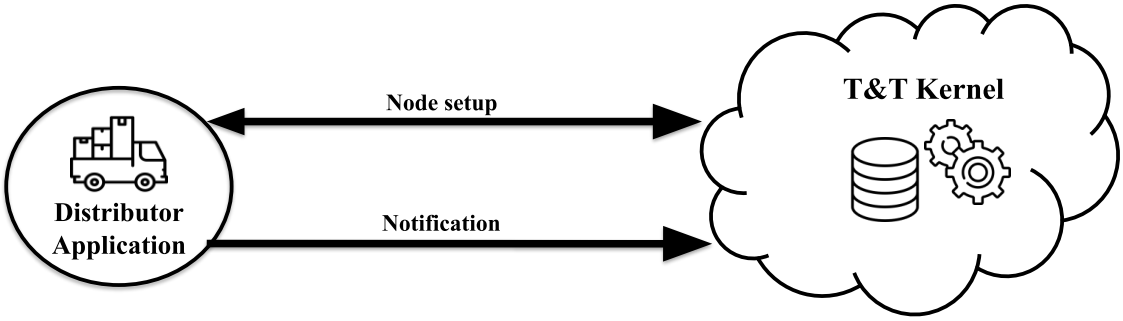

Figure 14 - Distributor Application interactions with the T&T kernel

The producer application has a node setup, notification, registration, and consultance interaction with the T&T kernel (Figure 15). The producer is responsible for registering the product information into the system. Each product should have a unique code according to the chosen international coding standard. The producer can notify when the raw material is received or when the product is dispatched to the retail. Also, the producer can consult any details about the current transaction or from previous transactions.

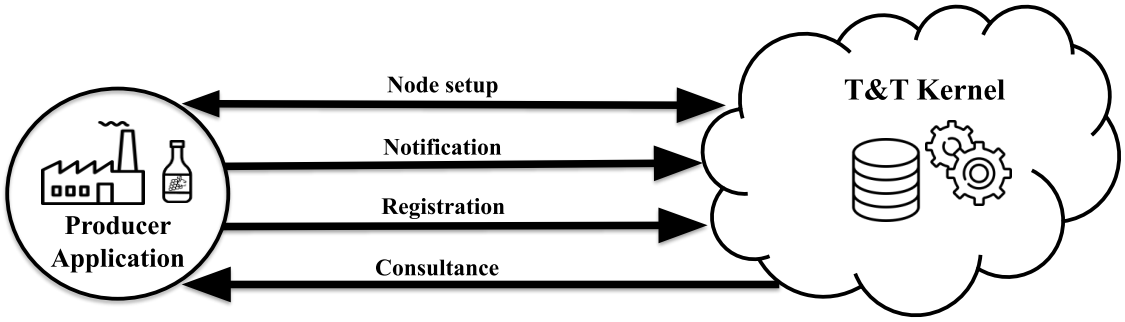

Figure 15 - Producer Application interactions with the T&T kernel

The retailer application has the same interactions as the producer application (Figure 16) but different responsibilities. It is important to refer that the retailer in consultance may have different privileges than the producer. For example, the retailer could only access the details about the transaction made with the producer, which means that the retailer cannot access the details between the producer and the supplier.

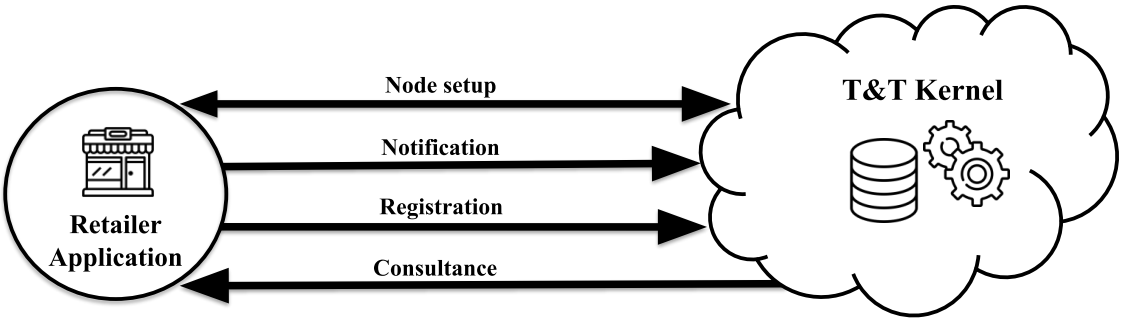

Figure 16 - Retailer Application interactions with the T&T kernel

The consumer application has only one interaction with the T&T kernel, which is consultance (Figure 17). The consumer can choose to participate in the network, which allows the consultance of the bought product, more precisely, the consumer would get details of the product from the supplier to the retail.

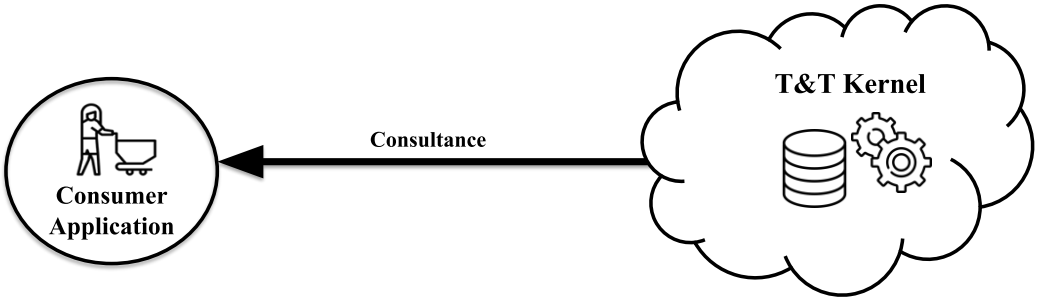

Figure 17 - Consumer Application interaction with the T&T kernel

Besides explaining the operations between the application nodes and the T&T kernel, it is also essential to explain how the different T&T architecture components can be implemented in a centralised and decentralised system.

3.3. Centralised Architecture Components

On a centralised architecture, there is a central entity that obtains and stores all the data in a single location and makes all the decisions individually (Figure 18) [39].

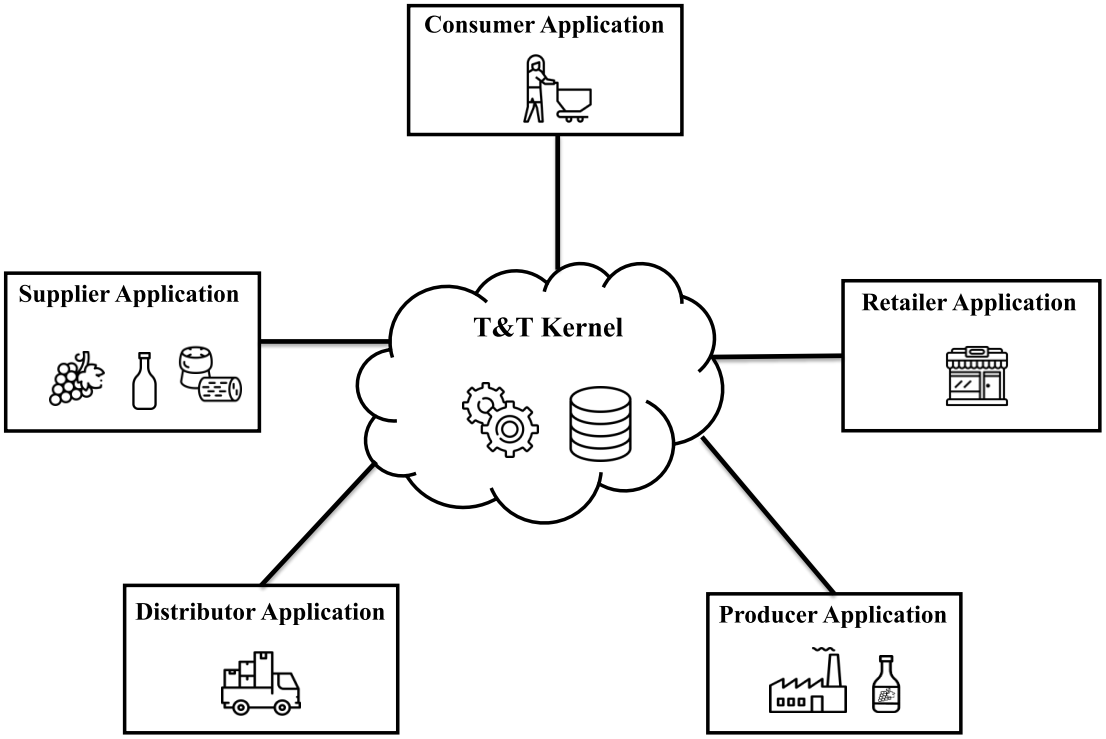

Figure 18 – Centralised T&T architecture

In a centralised architecture, the network is built around a single server that handles all the clients' interactions. This server is maintained by a central authority that retains total control over all aspects of the network. There is a gateway responsible for the application nodes management and authentication to the T&T kernel in the network. Also, the gateway communicates directly with the user authentication system to authenticate the node applications in the T&T kernel.

As for the database, it is used a centralised database. A centralised database is where all the data is located, stored, and maintained in a single location. Usually, it is maintained by a central organisation, and the users have no direct access to the data. Instead, they have access to an API that controls reading and writing (according to the business model rules). The database, gateway and user authentication system should be configured according to the business rules model.

3.4. Decentralised Architecture Components

On a decentralised architecture, there is no central database. Instead, the data is distributed through a set of nodes and stored in a ledger, as shown in Figure 19. Each node is capable of interacting with other nodes through a gateway. Also, the nodes can interact with the kernel (that is distributed over the applications), either by receiving a transaction to store in the ledger or to submit a transaction to the kernel.

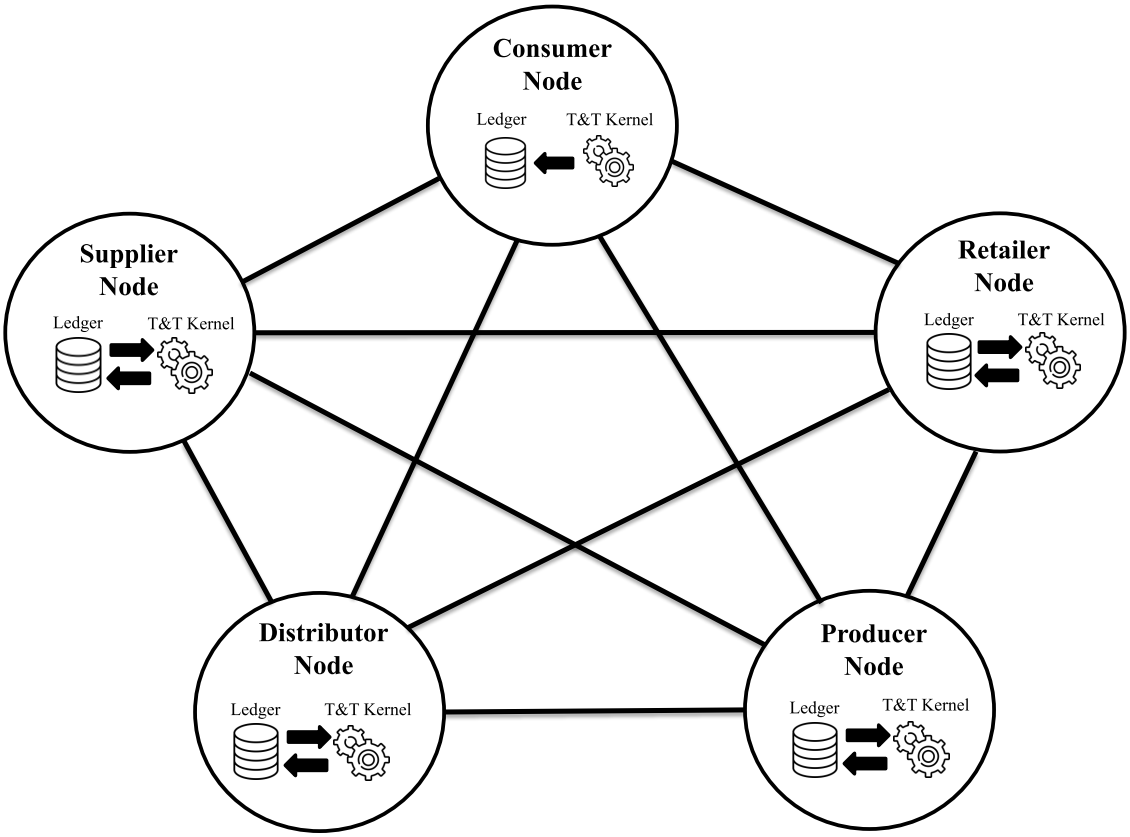

Figure 19 – Decentralised T&T architecture

This architecture is distributed, which means that the system is maintained by more than one computer. There are multiple nodes capable of communicating with each other with the ability to share resources between them. In this network, the gateway and user authentication system will work the same way as mentioned in the centralised architecture components.

Each node will have its own database called ledger located and stored in the node computer. All nodes maintain the ledger contents and each application node have read and write access according to the business model rules.

4. Blockchain Fundamentals

In 1991, Haber and Stornetta [40] proposed a solution to the timestamping problem. This solution proposed that all the data entries were sequentially ordered by timestamps in a record, making it difficult to tamper without leaving a sign. This solution contributed to the creation of the blockchain concept.

Later, in 2008, Nakamoto [41] introduced blockchain technology to create the cryptocurrency *Bitcoin* by maintaining immutable ledgers in thousands of nodes.

In 2014, the Ethereum White Paper introduced blockchain 2.0, expanding blockchain application scope with new features and utilities. Blockchain 2.0 added the *smart contracts* to the blockchain, improved the transparency and privacy to address some problems in the Bitcoin network, and introduced the term *Decentralized Autonomous Organizations*, also known as DAO [42].

Most blockchain systems are decentralised, but there are some cases where a private blockchain is centralised. An administrative authority controls a centralised system, making it easy to maintain, manage, and impose trust. However, it has some drawbacks such as low stability and central point of failure. In the central point of failure if the central core fails, then all the system fails. A decentralised system does not have a centralised control since the nodes may have different privileges to accomplish specific tasks. Decentralised systems overcome the drawbacks of centralised systems because there is no central point of failure. It is essential to mention that a decentralised system can be distributed, which means that two or more nodes work together synchronously to maintain the system. Naturally, decentralised systems are more complex in terms of development (mostly on data access and information synchronisation) and setup. As an example, a peer-to-peer (P2P) system is a distributed system [43].

4.1. Blockchain Concept

Blockchain is a *distributed ledger technology* (DLT). It has a network of peers, where transactions occur directly between peers (P2P) and are maintained and confirmed by their peers. In this technology, data is shared and recorded across multiple data stores called *ledgers* maintained by distributed network computer servers called *nodes* [44].

Figure 20 illustrates how the distributed ledger network works. There are four nodes (A, B, C, D) each from different organisations. All nodes share one thing in common: the ledger. For example, when node A creates a new transaction block with node B, the information is shared across the entire system through an encrypted channel. Once the nodes receive the data, the

network participants confirm the block validity to add the new block to the respective ledger. This broadcast communication of each transaction increases the system latency and affect scalability.

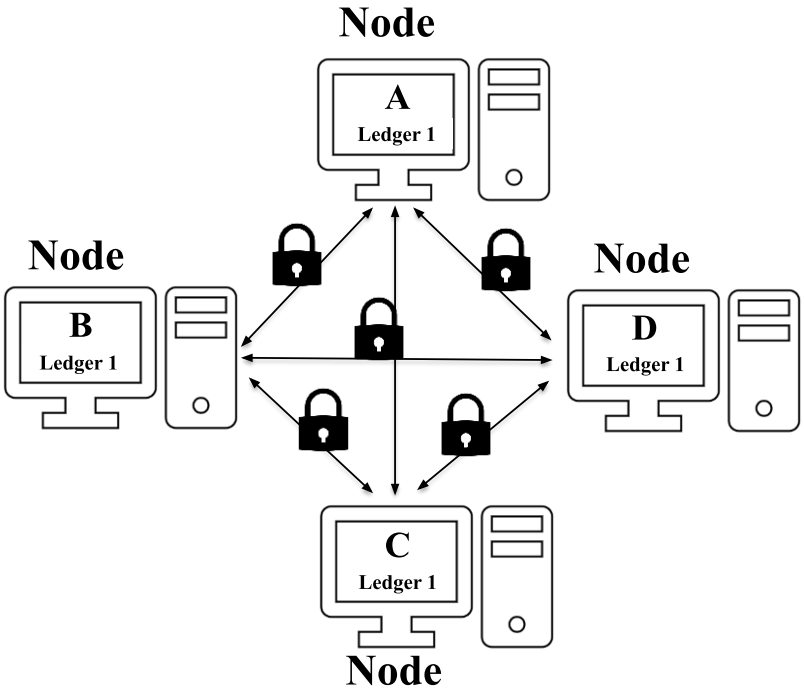

Figure 20 – Distributed ledger network

For blockchain, the P2P network is mostly used for data sharing and communication between peers. It is important to refer that P2P networks have their pros and cons. In terms of advantages, **(1)** it is easy to connect and organise; **(2)** there is no need for a devoted server; **(3)** it is economical to acquire and maintain a node; and **(4)** the consumers can handle their specific assets. As for disadvantages, **(1)** a P2P network is not so secure that viruses, spam, and spyware can disrupt confidentiality on the network; **(2)** backups are challenging to handle; and **(3)** this type of network has high latency and scalability problems [45].

It is also essential to explain why this process is called *blockchain*. It all started in the Nakamoto Bitcoin article, where he introduced a data structure concept called the *chain of blocks* [41]. In this *chain of blocks*, all blocks are connected through a hash from the previous block, which leads to the *blockchain* concept. Each block from the chain contains one or more valid transactions in it and all the nodes have these blocks stored in a ledger.

At first, blockchain was seen as a perfect DLT. However, some research around the topic has shown that blockchain has some issues and challenges that still require a solution today [46]. One of the most concerning challenges is the scalability trilemma problem [47]. In scalability trilemma, it has been observed that blockchains can have at most two of three properties. Those three properties are decentralisation, scalability, and security, as shown in Figure 21. This

problem needs to be considered in blockchain implementation, where the responsible organisation for the implementation should choose the two most suitable properties depending on the needs.

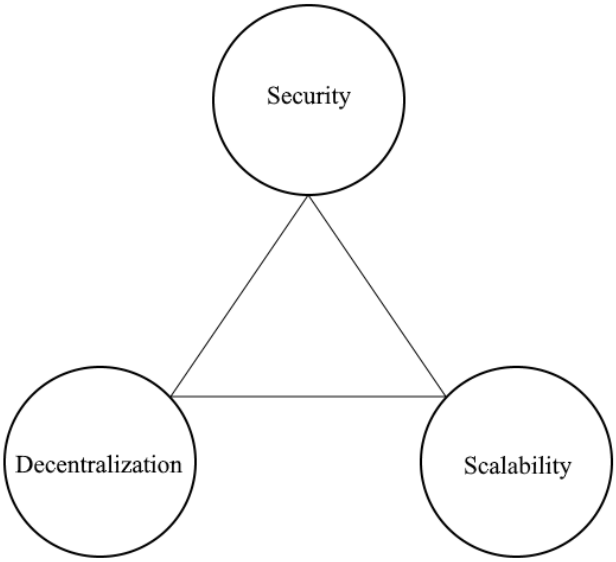

Figure 21 - Scalability Trilemma Model

There is no explanation about this restriction of having two of three properties. However, based on empirical observation, multiple examples prove that this trilemma trade-off exists in different scenarios. For example, **(1)** Bitcoin and Ethereum are secure and decentralised solutions, but in terms of scalability, each transaction can take too long when compared to a Visa payment that takes 65,000 transactions per second; and **(2)** current centralised databases such as SQL have security and scalability, but they do not have decentralisation. Every distributed system should aim to achieve these three properties, where it should be considered which one is less important than the others. A distributed system is scalable if the network is easily expanded without requiring an excessive amount of storage. It is secure if it is consistent and available at all times, and it is decentralised if it has nodes capable of handling the system. In this last case, the nodes must be owned by many individuals or organisations [48].

In terms of applications, blockchain was already used for voting, currency, smart property, intellectual property rights, contracts, finance, health, cloud services, and many more [49]. As stated by Singhal et al. [43], developing blockchain applications is only limited by our imagination, which means that more blockchain applications will be created to serve our daily basis in the future. This thesis follows the same idea by analysing the possibility of implementing blockchain in a supply chain context. For example, Feng Tian [50] applied blockchain technology in an agri-food supply chain traceability system.

In this chapter, it is essential to give an insight into blockchain technology. We will explain the blockchain architecture components, different types of blockchain, consensus protocol, and blockchain properties, and we will review and compare the different blockchain frameworks.

4.2. Blockchain Architecture

Blockchain has incorporated in its architecture, cryptographic primitives, blocks, ledgers, nodes, and transactions [51], [52]. Optionally, it can be used smart contracts in the architecture. These elements will be explained in the following subsections.

4.2.1. Cryptographic primitives

As for cryptographic primitives, blockchain often uses cryptographic hash functions and asymmetric-key cryptography for digital signatures [51], [53]. Hash functions play a significant role in many blockchain components, such as securing the block header and data, creating unique identifiers, and address derivation [51]. Asymmetric-key cryptography is known by the use of a key pair, a public and a private key. The key pair can either be used for encryption or digital signing purposes. For example, blockchain commonly uses the elliptic curve digital signature algorithm (ECDSA) [53].

4.2.2. Transaction

A transaction represents an interaction between parties. For example, with cryptocurrencies, a transaction represents the transfer of cryptocurrency between blockchain network users. Another example could be with the supply chain, where a transaction represents the exchange agreement between two stakeholders.

Blockchain transactions must have at least two types of information: input and output. The input is a digital asset that is being transferred, and the output is the digital asset that is being transferred to another user [51].

4.2.3. Block

A block is a pointer that connects data from previous blocks. A block can be split into a block header (which contains metadata for the block) and a block body (which has data related to the transaction). All blockchains can implement their own data fields for the header and body. For example, Bitcoin and Ethereum for the block header has a version of the block and has the previous block hash called parent block hash. It also has the hash of the current block,

timestamp of the block, block's size, and a nonce value [51], [53]. As for the block body, it contains all the transactions with a transaction counter. The block has a limit for the transactions that can hold, and that limit depends on the block size. On these blocks, the digital signature is responsible for the validation and authentication of transactions. It is also essential to refer the genesis block, which is the blockchain's first block. It is generally hardcoded on blockchain technology, meaning that the data on that block is manually introduced by the blockchain developer [43]. In the blockchain structure, the blocks are chained to each other, making a chain of blocks (Figure 22).

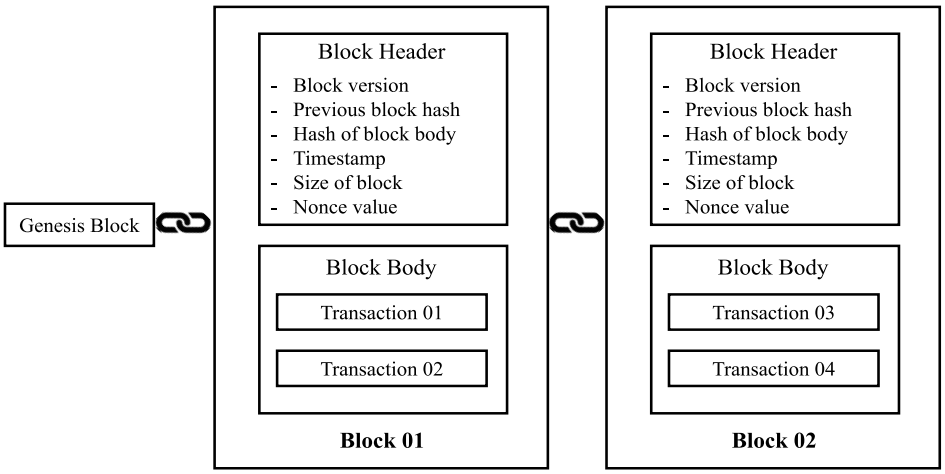

Figure 22 - Illustrative representation of the chain of blocks

Each block contains the previous block hash, which is the hash of the last block header. This implementation is the main reason behind the chain of linked blocks, ensuring the blockchain security and immutability. The block hash depends on the contents inside the block, which means that any modification or forgery would change the block hash. This modification would be easily detected and rejected by the system because the previous block hash from the next block would be different from the modified block. Also, some blocks may contain zero transactions. This aspect is vital to maintain the blockchain network's security by having constant blocks published, preventing attackers from modifying or "catching up" a blockchain.

4.2.4. Ledger

A ledger is defined as "a collection of transactions". In the blockchain, a ledger contains a list of blocks, where each block contains one or more transactions. The blocks data are distributed to all participating nodes in the network, where each participant stores the block information in its own ledger. The transaction data inside the block is signed cryptographically, making it possible to know which entity wrote that data [43], [51].

4.2.5. Nodes

In the blockchain, there is no centralised node. Instead, there is a set of nodes that provide consuming services. The nodes are responsible for maintaining the ledger, which contains a duplicate copy of the occurred transactions, and they are responsible for verifying the node's connection to peers [52]. Optionally, each node may contain or not a smart contract.

4.2.6. Smart Contract

The smart contract is an optional component in the blockchain. It is executed in blockchain nodes, and it automatically triggers a transaction under certain conditions. There are permissionless and permissioned smart contracts, where the last one is more used for collaborative business processes. Smart contracts can bring various advantages such as autonomy in the process, minimise the interactions between parties (avoids middleman services), and reduce administration costs [54].

4.3. The Different Blockchain Types

Blockchain is also called the technology with many "faces" since it can range from a fully open and permissionless type to a private one [55]. Therefore, blockchain can be divided into three different types: permissionless, permissioned, and hybrid, where each type determines the permission rules [53].

A *permissionless blockchain* is also known as a *public blockchain*. This type of blockchain allows anyone to participate, which means that anyone can create and validate blocks. The participants can also store or update data through transactions along with the participant entities, which makes this blockchain transparent and accessible to everyone. Generally, the code behind a *public blockchain* platform is open source. In this approach, any user can read and write in blocks without permission from an authority, making this type of system a target to malicious actors because there is an absence of rules and permissions. So, to prevent it, a decentralised mechanism known as consensus mitigates any malicious attempts to subvert the system [51]. An example of a public blockchain is the famous cryptocurrency Bitcoin, the first blockchain application [41].

A *permissioned blockchain*, also called *private blockchain*, has a restrictive condition compared to a public blockchain. Users must be approved by some authority to take part in the system activities. This type uses the same mechanism as a public blockchain. However, it has the

advantage of not requiring the maintenance of resources since it only allows authorised entities, ensuring chain data privacy [56]. A permissioned blockchain can be *public permissioned*, where everybody can join and use the infrastructure according to the access rules, or it can be *private permissioned*, where only the authorised peers have access to the blockchain according to the access rules. This type of blockchain can be used by organisations when the blockchain requires some control and protection or can be used between organisations that do not fully trust each other [51].

For last, there is the *hybrid blockchain* type, also known as *consortium blockchain*. This type of blockchain is public but only to an authorised group of peers (partly decentralised). The blockchain copies are exclusively distributed among the authorised participants, and all parties agree to the consensus by using privileged servers with a set of rules [57]. Table 2 summarises the properties of each blockchain type.

Table 2 – Comparison of different blockchain types by its properties

	Permissionless Blockchain	**Permissioned Blockchain**	**Hybrid Blockchain**
Participation	Open to anyone	Open to authorised individuals or entities	Open to an authorised group of peers
Write access	Anybody	Only the authorised peers	Only the specified group of peers
Read access	Anybody	Can be open to the public, or it can be closed only to the authorised individuals or entities	Anybody
Decentralisation	Fully decentralised	Partly decentralised	Partly decentralised

Each blockchain, regardless of the type, needs a consensus to validate any transaction, and so, we will explain the consensus protocol role in the blockchain.

4.4. Blockchain Consensus

Most blockchain systems, if not all, use consensus protocol. Such protocol aims to get all the nodes to agree on one consistent state of the ledger. This protocol can either be an incentivised or a non-incentivised consensus. In incentivised consensus, the blockchain rewards the users for keeping the network system alive. This approach is used in cryptocurrency systems such as Bitcoin or Ethereum, both public blockchains [43]. The non-incentivised consensus is deployed in private blockchain systems, for example, in Hyperledger Fabric, where there is no reward mechanism to enforce the consensus mechanism. Another critical aspect of the consensus protocol is its use as an authentication algorithm, where it validates each transaction before its commitment to the chain [58].

The *Proof of Work* is a popular consensus protocol used in the Bitcoin network [41]. This algorithm uses "mining" work, where a specific work must be done for a block to be proposed for the network [43]. The *Proof of Stake* is another popular consensus algorithm. Instead of "mining work", there are validators in the network that stake to participate in the validation process. The higher the stakes, the better the chances to participate [43]. The *Delegated Proof of Stake* is similar to *Proof of Stake*. The stake concept is involved, but the stakeholders can vote to choose some nodes as witnesses and delegates on this algorithm. The witnesses are responsible and rewarded for creating new blocks, and the delegates are responsible for maintaining the network [59]. The *Practical Byzantine Fault Tolerance* uses a voting system where all the nodes should participate in adding a block into the chain [60]. The consensus is reached when more than 2/3 of all nodes agree upon that block, tolerating less than 1/3 of malicious activity. *Ripple* is a consensus protocol that uses PBFT and is similar to Stellar consensus protocol. There are two types of nodes on this network, one type is the server nodes responsible for the consensus protocol to be applied, and the other type is the client nodes responsible for transactions. Another aspect of this protocol is that each miner uses a trusted subset of nodes to reach consensus. To reach consensus, 80% of the nodes must agree over a transaction [61].

4.5. Blockchain Properties

Blockchain has several properties that make it a suitable candidate for different applications and areas. Those properties are discussed below.

Privacy gives control to the user on how much data can be given to third parties. Generally, centralised systems can achieve privacy easily. However, specific blockchain frameworks have protocols that allow achieving a certain level of privacy to assure the safety of sensitive data [52].

Immutability is one of the most desired properties, which says that any data cannot be tampered. This property is assured by cryptography, and the more blocks the blockchain has, the higher is its immutability [43].

A network is **resilient** when responding to different network problems like packet drops and temporary node failures. [43]. The blockchain has a resilient property since it has multiple nodes always available, capable of responding to any network problems.

Auditability is the ability to do "a systematic, independent, and documented process to evaluate and monitor whether the audit criteria are fulfilled" [62]. Blockchain can be used when is needed compliance of business activities. It ensures an audit track by making the transactions data public verifiable [43], [53], [62].

As for **transparency**, blockchain data is updated for all the participating nodes and can be verified by the public. However, in some cases, the amount of information in that data can be restricted only to users with privileges [52].

The ledger is **consistent** when all the nodes agree upon a particular transaction, and this consistency is assured by the correct consensus mechanism [43].

Blockchain technology plays a significant role in data **integrity**, where data integrity refers to the accuracy and consistency of data over its lifecycle. Cryptographic functions in the blockchain, such as digital signatures, ensure transaction integrity [43], [63]. Another example is the public verifiability in blockchain, where the integrity of data can be verified by anyone [52].

In the blockchain, data is stored in the chain and shared in a **distributed manner**, so there is no single point of failure.

Finally, blockchain is a distributed system, whereas long as there are participating nodes in the network, the data will be **persisted** in a distributed way.

4.6. Blockchain Frameworks

In order to implement blockchain, it is crucial to choose a blockchain framework. A blockchain framework can be defined as a "software solution that simplifies the development and deployment of blockchain application with little customisation" [64].

The blockchain frameworks contain tools and libraries that allow developing blockchain solutions, containing features such as transaction details, consensus protocol, and many others. When choosing a framework, the blockchain developer should consider different factors, such as processing power, storage, and scalability. It is also essential to analyse each framework's pros and cons before choosing it [64].

In Appendix 1, Table 4 shows a comparison of different blockchain frameworks. Each framework is compared by its privacy features, accessibility, consensus, speed, scalability, transaction cost, incentive, and smart contract. The privacy features are related to the privacy of the transactions or the user's identity, where the transactions information or user's identity can be either private or accessible to anyone. The accessibility is related to the blockchain type, more precisely, which access permission the blockchain has. The consensus parameter is related to which consensus protocol is used in that blockchain framework. In speed parameter is evaluated the speed of transactions more precisely and, when possible, is described the number of transactions that can occur in a given time. In terms of scalability, it is evaluated if the blockchain has a high or low transaction throughput. For the transaction cost parameter, each transaction's cost is either a high-cost or low-cost transaction. In the incentive parameter, it may be required or not the use of a cryptocurrency to maintain the network. For last, in smart contract parameter is specified if the smart contract is available or not for that framework. When it is available, it is specified the programming language used to write the smart contracts.

This comparison of different blockchain frameworks will help in the next chapter because we will choose a blockchain framework for the blockchain supply chain architecture.

In this chapter, we have covered the essential topics about blockchain to understand how it is implemented the blockchain supply chain, a decentralised approach in the proposed architecture.

5. Blockchain Supply Chain

In this chapter, we will discuss the implementation of blockchain in the proposed T&T architecture. We will explain why the blockchain is suitable for the proposed T&T architecture. We will also compare blockchain with the other distributed ledger technologies to explain why it was chosen instead of any other distributed ledger technology.

This chapter includes the most suitable type of blockchain and blockchain framework for the proposed architecture. We will explain the blockchain architecture components and how the transactions work based on the chosen blockchain framework. Furthermore, we will explain how to integrate the T&T technologies into smart contracts and demonstrate how blockchain, T&T technologies are integrated into the proposed architecture. Posteriorly, we compare some centralised supply chain features with the blockchain supply chain, and additionally, we propose an alternative solution to blockchain supply chain called *off-chain supply chain.* Finally, we give some real use cases examples where the blockchain was implemented in supply chains as an alternative solution to centralised supply chains.

5.1. Is Blockchain suitable for Supply Chain?

Before using blockchain on the proposed architecture, it is essential to study if the blockchain implementation makes sense. There are some cases where blockchain implementation is not suitable or does not make sense. Wüst and Gervais [56] introduced a flow chart that determines whether the blockchain implementation is suitable for this context. Figure 23 shows an adapted flow chart used to decide if the blockchain is an appropriate solution for the current case.

When trying to implement a blockchain, the first question is if it is necessary to store state, and the answer is yes. It is essential to store state because multiple participants are interacting and changing the state of the system. A stored state gives transparency to the transactions made between the participants while maintaining some degree of privacy.

The second question is related to the number of participants, more precisely, if there are multiple writers. The writers, in this case, are entities that have writing access permissions. The answer is yes since a decentralised supply chain will have multiple entities with write permissions.

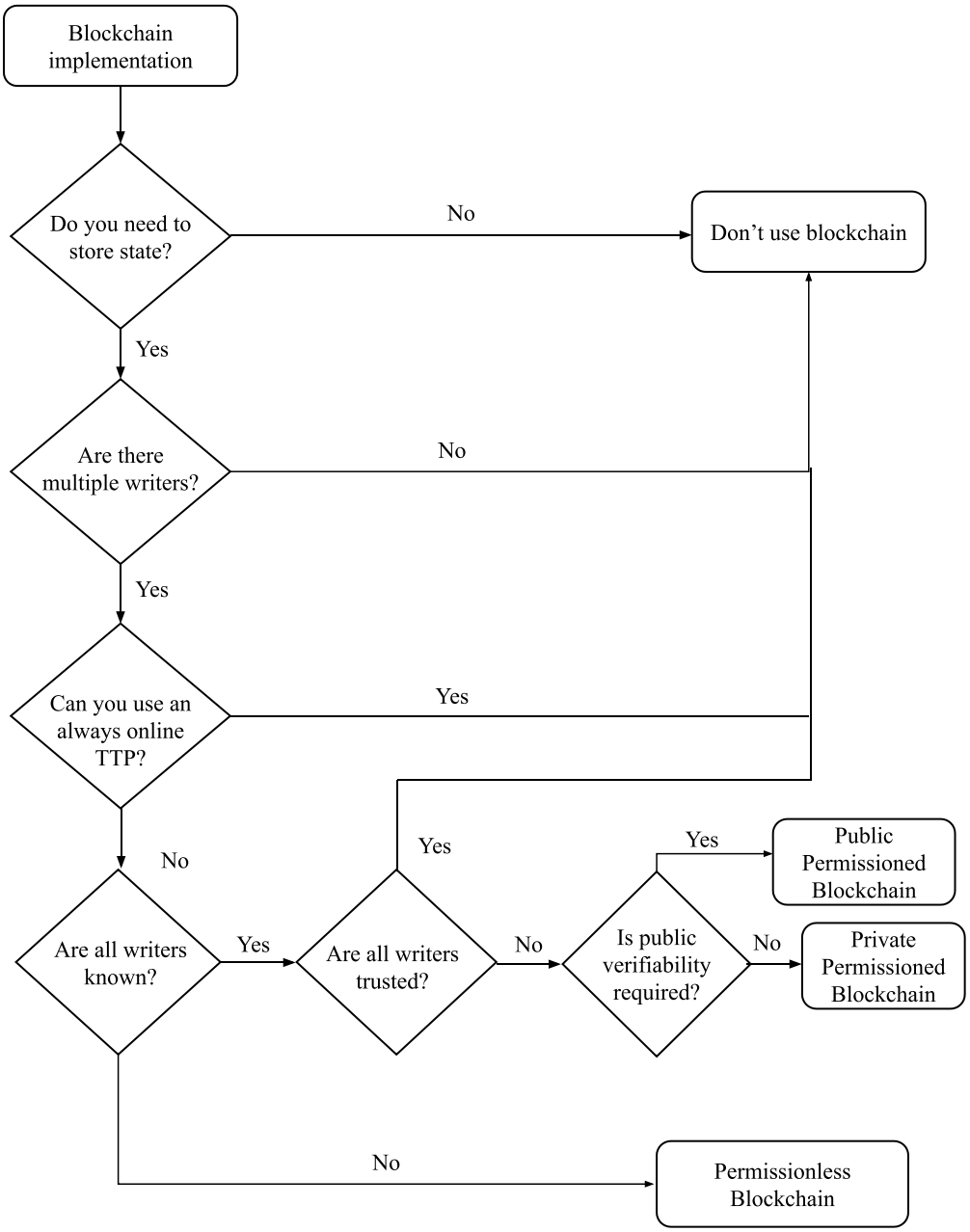

Figure 23 - Adapted flow chart to determine if the blockchain is needed for our case [56]

The third question asks if it is possible to use an online trusted third party (TTP), and the answer to the question is yes and no. A TTP is an entity that mediates the interactions between two parties, whom both trust the third party. The answer is yes if the organisation wants an online TTP capable of mediating the transactions between the participants, answering that blockchain is not suitable. The answer could be no if the organisation does not want a TTP mediating the process. The answer to this question is more a management and bureaucratic question than a technical question. To encourage multiple stakeholders, with different interests, probably the non using of a TTP would be interesting. For example, without a TTP, it is possible to achieve a certain degree of privacy between the stakeholders.

At this point, we know that blockchain is suitable for the proposed architecture. The only thing that still needs an answer is the type of blockchain. The fourth question asks if all participants/writers are known, and the answer is yes. Only enters in the network the entities that will be participating in the supply chain.

The fifth answer asks if all the participants/writers are trusted, and the answer is no. There is no transparency in the current supply chains, which means no one can trust the other entities' information.

The sixth and last question asks if anyone can verify the stored data's validity, and the answer is no. Only the participant entities in the network are allowed to verify the validity of a transaction's content. With all the answers, we determine that the suitable blockchain for this case is a private permissioned blockchain.

5.2. Comparing Blockchain With Other DLTs

In recent years, blockchain has become a trending topic in the supply chain and financial sectors. There are different DLT's such as Blockchain, Hashgraph, Sidechain, Tangle and many more [65], [66]. Each one of the DLT's is somehow unique between themselves. As mentioned in previous chapters, blockchain features are immutability, enhanced security, consensus protocol, and smart contracts. In the blockchain, data is represented in a chain of blocks, where all the blocks follow a specific sequence.

Hashgraph is a platform based on Directed Acyclic Graph (DAG) to shortcome some of the blockchain problems such as scalability and cost. It involves the same concept of blockchain. However, it is built and works differently. The structure is based on columns with many vertices, where each vertex is called an event. An event can be created and submitted by a user and to create an event, a user must randomly pick a member in the network to gossip all the available information. As for the features, hashgraph is fair and fast. It has virtual voting and its highly efficient. It is fair because it ensures that consensus timestamps are assigned to all events, and it has a high throughput of transactions since it uses a gossip-about-gossip protocol. It has a virtual voting feature, where all members maintain the full history of transactions by maintaining DAG of events. It is a highly efficient DLT because no event is discarded, all the events are used for DAG [66].

Sidechain is a DLT that combines two different blockchain architectures to address some of the blockchain problems. The main blockchain is divided into segments, where there are sub-networks that process locally any submitted requests. In other words, on this DLT, instead of

having one blockchain, it has a group of sub-blockchains and the main blockchain. It is possible to move digital assets between sidechains, where it is possible to hide data from other participants. Sidechain has essential features, such as scalability and privacy. It solves the scalability problems of blockchain by creating sub-blockchains. It solves some blockchains' privacy problem by creating a constraint over who can access specific data in the network [66]. Tangle, a platform developed by IOTA, uses DAG, where each vertex is called site. The edges between the sites correspond to a transaction approval. It was proposed to address some blockchain problems. Some features of tangle are scalability, micro-transactions, and quantum-resistant. As for scalability, it has near-infinite scalability, because an increase of participating users on the network leads to faster validation times, and users can validate transactions in parallel. It has the concept of micro-transactions where miner and validator's role is combined into one role, which means that instead of paying an additional fee to the miner for validating a transaction, users use their computing power. Related to quantum-resistant, Tangle uses a Winter One Time Signature scheme described as a quantum-resistant algorithm [65], [66].

Every DLT is different from each other, in particular, each one with their features. All of this DLT's are still developing, and as for blockchain, it still lacks maturity. However, blockchain has been more used in real-world applications than the other DLT's. In those real-world applications, for example, in the supply chain, it was demonstrated that blockchain could add value to them. Those examples will be explained later in this chapter.

We conclude that there is still a long way to say what is the best DLT for supply chains, mainly because there is a lack of maturity in all DLT's. This thesis focuses on blockchain because it is a well studied DLT. It has many practical applications in real-world, and it has many frameworks for different use case scenarios.

5.3. Blockchain Type and Framework for the Proposed Architecture

A blockchain framework is a software solution that contains infrastructure and libraries that simplify and allows the development and deployment of blockchain applications. A blockchain framework has features and capabilities such as consensus protocol, the transaction between the nodes, user identity, and many others [64]. When choosing a blockchain framework, it is crucial to consider the different features that the framework assures. Besides that, it is essential to choose a framework that best suits the proposed architecture purpose.

For the proposed T&T architecture, we have chosen permissioned blockchain since it has the same traceability of digital assets, the same distributed, resilient, and redundant data storage

system as a public blockchain. As mentioned in the blockchain chapter, this type of blockchain is more used in organisations to control and protect the blockchain or when organisations do not fully trust each other. This type of blockchain can also require that all users be authorised and identified to send or receive transactions, making it easier to audit and detect fraudulent activity. This permissioned blockchain will be private permissioned because the objective is only to allow the authorised peers to access the blockchain.

From the blockchain frameworks mentioned in chapter three, it will be used the Hyperledger framework since it can be applied to manufacturing and supply chain industries. Besides that, Hyperledger is open source and has a strong industry backup by many financial institutions since 2015 [64]. Inside the Hyperledger framework, there is a set of frameworks that can be used for different use cases. Appendix 2 presents the Table 5 that summarises all the Hyperledger infrastructure frameworks with the respective description and use cases. Additionally, Hyperledger infrastructure comes with some tools and libraries that can be used in conjunction with the frameworks. Appendix 3 presents Table 6 and Table 7 that summarises all the tools and libraries in Hyperledger infrastructure. As a framework, the Hyperledger Fabric is the most suitable option for the proposed T&T architecture because some functionalities and features are useful for a supply chain scenario. For example, the transactions applied to the architecture should be confidential only between the exchanging parties using a private channel. From the tools and libraries, it can be chosen any tool or library that will benefit and contribute to better blockchain implementation.

Hyperledger Fabric framework initially mentioned Kafka, PBFT and Raft as consensus protocols. Currently, the only available solution is Raft, since Kafka is already deprecated in last versions of Hyperledger Fabric and PBFT is not yet implemented in the framework. Raft consensus protocol is based on a “leader and follower” model. The leader is dynamically elected among the other participant nodes (followers). Raft is a crash fault-tolerant (CFT) consensus protocol since it can tolerate the loss of nodes, including the leader nodes. The only thing that needs to be assured is the majority of participant nodes to work correctly [67].

In Hyperledger Fabric, the consensus process is divided into three phases: endorsement, ordering, and validation. In the endorsement phase, the participants endorse a transaction, where a policy drives this endorsement. For example, for a transaction to be endorsed, it must have four out of six signatures. In the ordering phase, the order accepts the endorsed transactions and commits them to the ledger. The last phase is validation, which takes a block containing a set of transactions and validates the results’ correctness, including if the endorsement policy goal was met. Also, it is validated the double-spending [68].

The current blockchain for the proposed architecture will have at most two of three properties based on the scalability trilemma problem. Hyperledger Fabric was designed to have more scalability in exchange for decentralisation. So, this means that the proposed will have at most security and scalability. However, this does not mean that the proposed architecture does not have decentralisation. It is partly decentralised compared to other blockchain frameworks, and it will not affect the objective of the proposed architecture. In chapter six and seven, it will be discussed these properties more in detail.

5.4. Blockchain Architecture Components

As for the blockchain components in the proposed architecture, the T&T Kernel has three identical components: Business Rules Model, Database and User authentication. The only different component is the blockchain network, as shown in Figure 24.

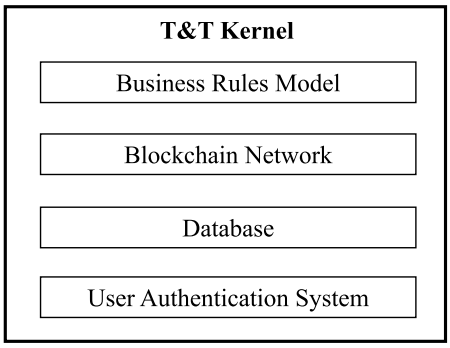

Figure 24 - Blockchain components in the proposed T&T architecture

The Business Rules Model is composed of smart contract and consensus protocol (Figure 25). These two components are responsible for ensuring the correct behaviour of the blockchain. They also have implemented behaviours for the traceability system.

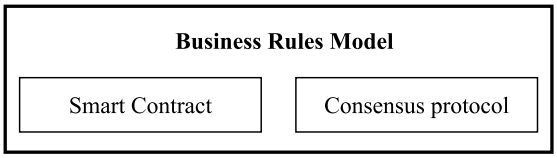

Figure 25 - Business Rules Model components

The smart contracts are responsible for carrying out transactions between two entities. In Hyperledger Fabric, a smart contract is called *chaincode*. The smart contract contains the logic of the transaction, where assets are created and updated. The smart contract also allows the node application to interact with the ledger, and it is installed on every endorsed peer on the channel [69]. When creating a smart contract in Hyperledger Fabric, there are two essential

methods. One is ***Init***, which is used when any node application initialises the smart contract execution or upgrades a transaction. The other method is called ***Invoke*** and is used when it is needed to process any transaction proposals. In terms of interactions, the smart contract is connected to a peer, where the node application can invoke it through a channel [70]. It is important to mention that the smart contract must have ownership. Smart contracts without ownership can lead to security issues in enterprise blockchains. For the proposed blockchain architecture the smart contracts will have shared custody ownership where the two entities involved in the agreement are responsible for the administrative actions over the contract.

The consensus protocol is a must component in any blockchain. It plays a significant role in validating the transactions inside a block, allowing a block to be or not published on the blockchain [51].

The blockchain network has multiple components such as ledger, peer nodes, ordering service, channel and gateway (Figure 26).

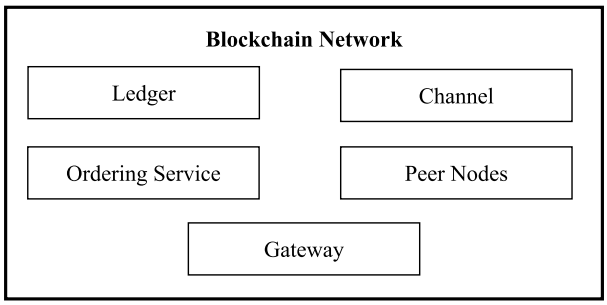

Figure 26 - Blockchain network components

The first component being analysed is the ledger. As mentioned in the blockchain chapter, a ledger contains the transaction data from a specific set of blocks or all the blocks published on the blockchain. There is a ledger per peer, where the ledger communicates with the node application through a channel. This communication is mediated by a gateway [71].

The blockchain network contains a set of peers. The peers have an essential role in the blockchain network because they hold the ledgers and smart contracts, and since the peer holds the ledgers and smart contracts instances, the node applications must interact with the peer to access these resources [72].

A set of orderer nodes forms the ordering service. It orders the endorsed transaction/s broadcasted by the application through a channel, creates a block containing the transaction/s, and sends the block to all peers on the channel to validate the transactions contained within the block [67].

The channel is where private communications occur between two or more network members to ensure that the information exchanged is private and confidential. Each transaction is executed on the channel, where each party must be previously authenticated by a membership service provider (MSP) to transact on that channel. It is essential to mention that the blockchain network can have multiple channels, where a peer can belong to one or more channels. Thus, it maintains multiple ledgers and smart contracts except that the ledger data cannot pass from one to another channel. This exception is defined in the smart contract configuration [73].

For last, the gateway manages the network interaction on behalf of the node application. It has a set of policies related to the user's authentication and management in the system. A gateway can either be static or dynamic. The static gateway has a good view of the network (has defined all peers and orderers from the participating organisations) to get the transactions endorsed and distributed. The dynamic gateway needs only one peer identified to start the process. The rest of the peers will be discovered through a service discovery [74]. The gateway is composed of a connection profile and a service discovery, as shown in Figure 27.

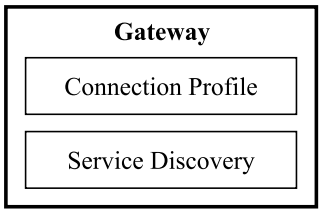

Figure 27 – Gateway components

In order to configure the gateway, a connection profile is needed. The connection profile has described the peers, the orderer, the certificate authorities, the channels, and the organisations participating in the network [75]. The service discovery is used only in the dynamic gateways. It allows the node applications to dynamically discover the endorsement policies' configuration details and the smart contract it needs to use. The use of service discovery increases the node application side's availability and resiliency because it does not need to be reconfigured each time a configuration detail is changed [76].

As mentioned previously, blockchain has distributed ledgers in terms of database, which means that all the information is stored and located in different network nodes [68]. Besides the distributed ledgers, blockchain also has a database called state database. The state database contains the ledger's current state data, which means that it is available the latest key values known to the channel. When a smart contract is invoked, it executed the transaction against the current state data, making the smart contract interactions efficient during the transaction process [77]. There are two options as a state database, a Level DB, and a CouchDB. A Level DB is a

default database embedded in the peer process and can store smart contract data as a key-value pair [77]. The CouchDB is an optional and alternate state database, which allows for the development and deployment of indexes with the smart contract to make queries more efficient when querying large datasets [78].

The User Authentication System is composed of a membership service provider (MSP) and a certificate authority (CA) (Figure 28), where both components are responsible for the user's authenticity in the blockchain.

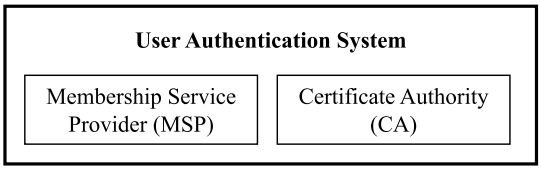

Figure 28 - User Authentication System components

The MSP is responsible for verifying a blockchain participant's identity to allow the participant to transact on the network. Also, MSP contains the peer's public key transmitted by a CA to verify that the transaction's signature is valid, thus validating the member's identity [79].

The CA plays a significant role in the user authentication system since it issues X.509 digital certificates for the participating organisations. The organisations can use digital certificates to sign transactions, indicating that the organisation is endorsing the transaction. There is usually more than one CA involved in this process, where there are different CAs for different organisations. The CA works together with the MSP, where the MSP is responsible for mapping the certificates to member organisations [80].

Besides those components, it is essential to describe the node application's role in blockchain T&T architecture. The node application is responsible for interacting with the blockchain network and can invoke smart contracts to submit a transaction to a ledger or querying ledger content [81]. The node application has a set of components, as shown in Figure 29.

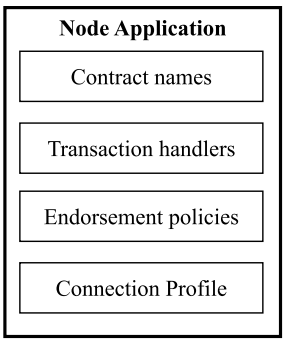

Figure 29 - Node Application components

The node application has contract names. Each smart contract has its own name that identifies it within the rest of the smart contracts, making it easier for the application when searching for a particular smart contract [82].

It has transaction handlers which are key points implemented in smart contracts. These key points control the invoked smart contract at specific points (before and after the transaction). There are three kinds of transaction handlers, a before handler, an after handler, and an unknown handler. The before handler is called before invoking the smart contract transaction. The after handler is called after invoking the smart contract. An unknown handler is called when a not defined attempt is invoked during the transaction, producing a failure record of the invocation [83].

The application nodes have endorsement policies responsible for defining the set of organisations required to endorse a transaction to validate it. The organisation endorsing peers are responsible for running the smart contract and signing the transaction to produce an endorsed transaction. Later, the endorsed transaction is validated by the committing peers, where each one confirms if the endorsements fulfil the endorsement policy [84].

For last, it has a connection profile that plays a similar role to the connection profile of the gateway mentioned above. This connection profile is configured to be used by the application node. More precisely, it is defined and configured as a gateway to handle all the application's network interactions. Also, the connection profile comes with connection options, where it is possible to control the interaction between the gateway and the blockchain network [75].

After explaining all the components in the blockchain architecture, it is still important to demonstrate how they interact with each other and how they are disposed of in the architecture (Figure 30).

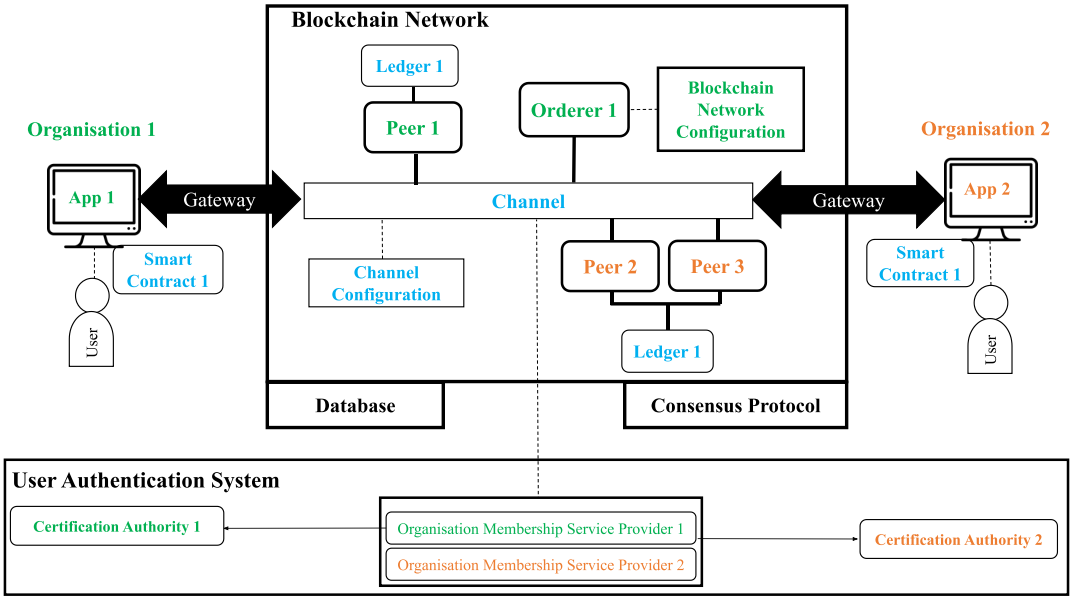

Figure 30 – Example of interactions between the different blockchain architecture components

Figure 30 shows an example of the interactions that the different blockchain components can have. Still, it is important to refer that the architecture can be very different in each supply chain. Each organisation must have at least one peer with the option to include more peers. Peers from different organisations may have the same or different smart contracts and ledgers. For example, imagine that we have three organisations: a supplier, producer and retail. The supplier and the producer can have one peer with a ledger one. This peer is related to the transactions between the supplier and producer. However, the producer can also have a peer connected to a different channel with smart contract two and ledger two, both related to the transactions between the producer and the retail. This example should give an idea that one organisation may have multiple peers with different functions connected to different channels. There is also the orderer in the blockchain network, which may be one (usually controlled by the organisation that deployed the blockchain) or more.

Besides the mentioned, each organisation has one application node capable of connecting to one or more peers in the network.

As for the user authentication system, it is possible to have also different scenarios. In the entire architecture, it is possible to have only one CA responsible for all the participating entities' digital certificates, or each entity can have their own CA. For each CA, there will be one membership service provider for that organisation.

5.5. Transactions in the proposed architecture

The transaction is an essential element that makes possible the business activity in the Hyperledger Fabric network and other blockchain frameworks.

Transactions can be created by nodes or node applications. Additionally, the node application creates a transaction responsible for invoking functions outlined in smart contracts, which will produce transaction data. This transaction data is kept inside blocks, where each block is chained along with other blocks, making the data inside the transactions immutable [52], [85].

In Figure 31, **(1)** the client application starts to generate a transaction proposal. This proposal requests to invoke a smart contract function with specific input parameters to read or update the ledger. **(2)** Once the endorsing peers receive the transaction proposal, they must verify that the proposal is well-formed, verifying if the transaction proposal was not submitted already in the past (protection against replay-attacks). They also validate the transaction proposal's signature by using MSP and confirming that the transaction's submitter is authorised to perform the request on the channel. After all the verification process, the transaction is simulated with the proposal inputs as arguments against the current state database to produce a transaction result containing a response value, a read and write set (RW set). **(3)** If the simulation is successful, then the endorsing peers digitally signed the transaction proposal, sending back to the node application an endorsed transaction. **(4)** The node application validates the endorsing peer signatures and compares the proposal responses from the endorsing peers to determine if they are the same. In this step, if the smart contract is querying the ledger, then the node application would not send the endorsed transaction to the ordering service, which means that the transaction process ends here. Otherwise, if the smart contract is submitting to the ledger, then the transaction flow confirms if the endorsed peers are specified in the endorsement policy. **(5)** The node application broadcasts the endorsed transaction to the ordering service, where the transaction contains the endorsing peer's signatures, channel ID and read/write sets. **(6)** The ordering service orders the transaction/s chronologically and creates a block of transaction/s. **(7)** The ordering service sends the block of transaction/s to all peers on the channel. **(8)** The transaction/s within a block is validated to ensure that endorsement policy is fulfilled and that the ledger state for the read set variable is the same as the read set generated by the transaction execution. The block transactions are set as valid or invalid, and once done, the peers commit the block to the channel chain, and all the peers on that channel update their ledger. **(9)** For last, each peer notifies the node application that the transaction was appended to the chain. It also notifies if the transaction was validated or invalidated [69], [85], [86].

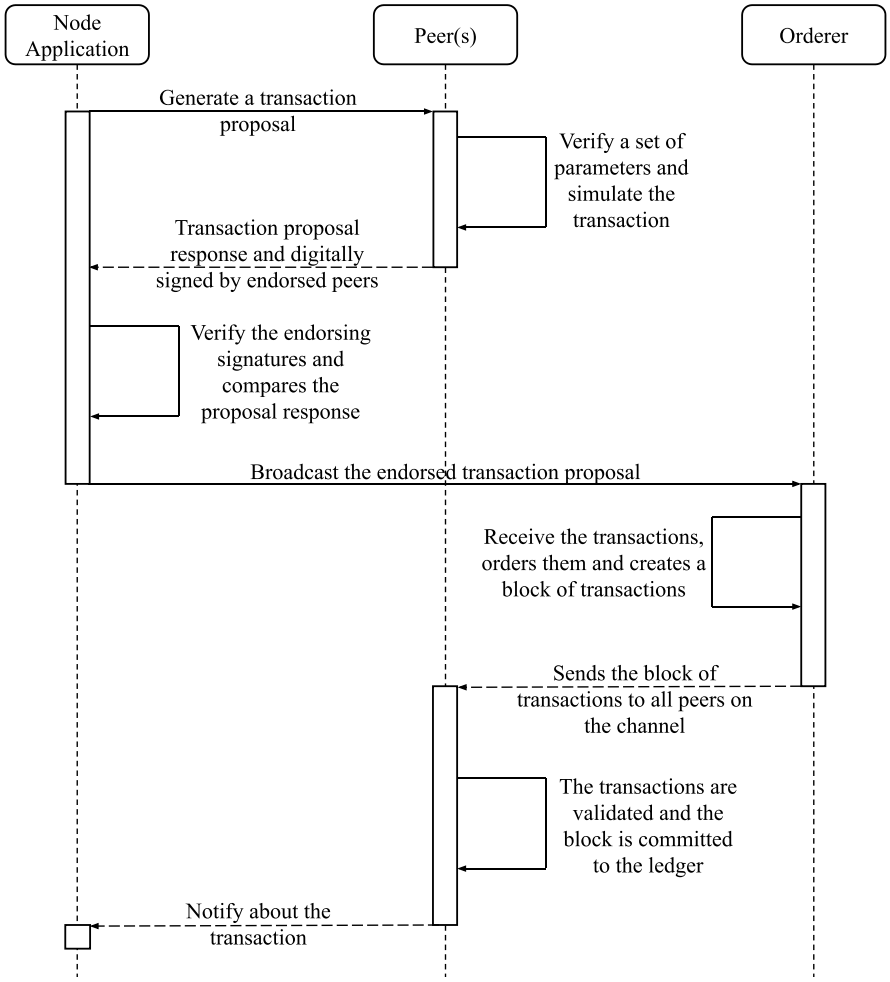

Figure 31 - Transaction flow in Hyperledger Fabric

Also, there is an endorsement policy in transactions, which has a key role in the transaction process. The policy contains a list of endorsing peers and the number of endorsements required to validate a proposed transaction. The endorsement policy informs the committing peers about the validity of the proposed transaction, and that same validity depends on simulation results, endorsing peer signatures, and authorisation certificates [85].

5.6. Integration of T&T Technologies in Blockchain Smart Contracts

A combination of T&T technologies (auto-ID technologies) can be used in supply chains, for example, the usage of RFID with GPS tracker, where both can cover different parts of the supply chain network with a QR Code attached to the product [12], [87]. The combination of different auto-ID technologies is essential for a level three traceability system since those technologies are responsible for the trace of the whole supply chain system.

In centralised supply chain systems, each entity records its data in a centralised ledger stored locally. A central entity ensures the storage and management of that data. However, this type

of systems can have issues related to falsified data. On this scenario, product traceability can be easily interrupted due to the high possibility of tampering data, and this interruption may cause inconsistency of traceability information between the participating nodes [88]. In the proposed architecture, the implementation of smart contracts along with an integration of IoT and T&T technologies, can solve this problem.

A blockchain can have multiple smart contracts for different purposes. For example, different node applications using different IoT devices can trigger different smart contracts. Figure 32 represents a smart contract process between two entities, a seller and a buyer, both in the blockchain. On the smart contract, the transaction is declared completed when the seller receives the buyer's payment, and the buyer receives the goods from the seller. Once the transaction is declared completed, the smart contract is executed, and the transaction is recorded in the blockchain [89].

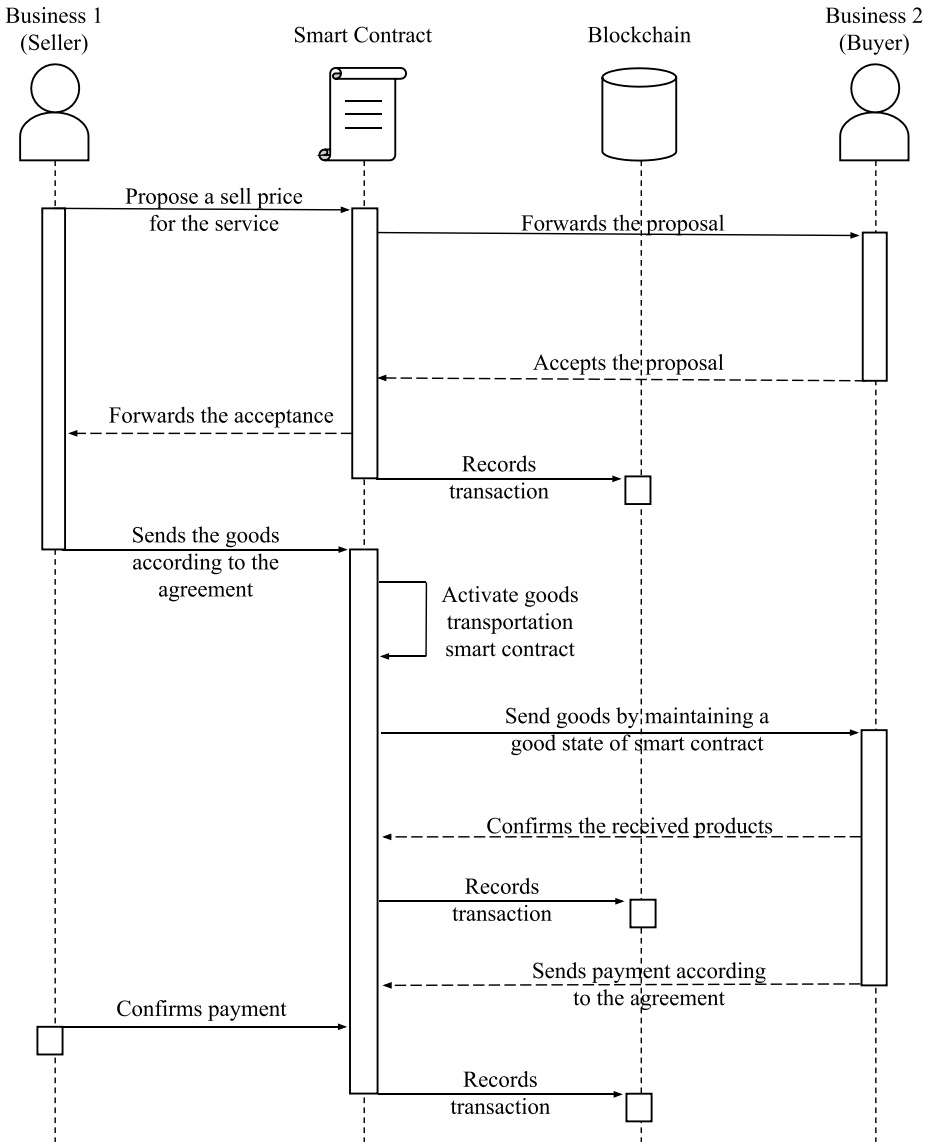

Figure 32 - Smart Contract Process between two entities

There are apparent differences between the smart contract process and the traditional negotiation process. There is no intermediary involved in the smart contract process, allowing direct communication between the participants. Also, there is a cost reduction in the process because there is no middle man involved. There is no loss of data on the transactions during the process, and the transactions are kept in sequential order in the blockchain. The smart contract makes the business agreements more trustworthy, and no one can change the smart contract besides the participants, which makes this process more secure against frauds. Also, a smart contract ensures autonomy because there is no trusted third party mediating the transactions [54].

As shown in Figure 32, other smart contracts can be activated during the smart contract process. When the seller is sending the goods to the buyer, a distributor entity is responsible for the goods' transportation. In this transportation phase, it is activated a smart contract that records a set of values related to the temperature and the goods' location during transportation. A temperature sensor technology can measure the temperature alongside a particular smart contract called Oracle that receives and relay information about the outside world. An oracle is used in this case because the smart contracts cannot interact with any application programming interface (API) outside of the blockchain network for security reasons [90]. In the same contract, it can be used a GPS responsible for giving the coordinates of the goods. It is essential to mention that the smart contract can end at any time if any rule is violated in the state of the contract. The contract state can be bad if the distributed goods' location is wrong or if the stored goods' temperature was much higher or lower than the defined in the contract. If the contract is in a bad state, the transaction is cancelled [91]. Also, it is important to mention that the smart contract saves the transaction state multiple times in the blockchain. The transaction state is saved multiple times because if any error or data loss occurs during the transaction, then it is possible to recover the saved state from the blockchain.

There are other types of smart contracts that are important to mention that can be activated during the proposed architecture events. These events are not related to the transaction between two entities. Instead, they are related to the tracking and tracing of the products in the whole supply chain. For example, in the registration event, a product registration smart contract is either activated by the supplier for the raw material registration or by the producer for the product registration. There are parameters related to the T&T technologies on this smart contract, for example, the barcode data, the RFID tag data, or the QR Code data.

5.7. Integration of T&T Technologies in the Blockchain Supply Chain

After explaining how the T&T technologies are integrated into blockchain smart contracts, it is also essential to demonstrate how the blockchain and these technologies fit and interact in the proposed architecture. Figure 33 demonstrates how the blockchain and T&T technologies are integrated into the proposed Blockchain Supply Chain architecture and their interaction with the other architecture components.

Figure 33 shows the supply chain from the supplier to the consumer. There is an interaction of the T&T technologies between each participant, where different T&T technologies are used depending on the supply chain stage.

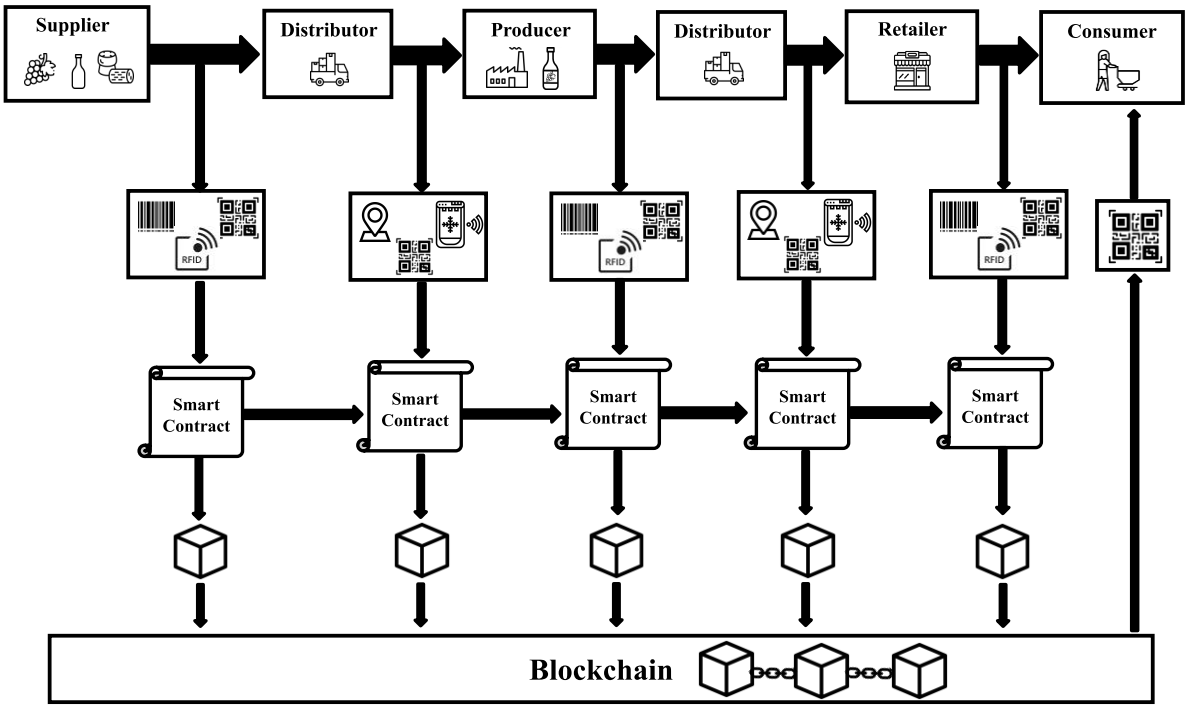

Figure 33 - Proposed T&T architecture with the implementation of Blockchain and T&T technologies

These T&T technologies collect information about the raw materials or the product, where this information is posteriorly stored in a smart contract. As for the supplier, producer, and retailer, the T&T technologies used are either a barcode or an RFID with a QR Code. For example, barcode and RFID can be used mainly to track and trace the inventory of raw materials or products. On the QR Code, it can be inserted information about the raw material or product conditions. For example, the distributor can use IoT and T&T technologies such as GPS, temperature sensors, and QR Code. Only the essential data about GPS coordinates and the temperature which the raw material or product was transported will be inserted on the QR Code. For last, the consumer can use its smartphone with a QR Code reader application to see all the

product details. The QR Code contains a link for the correspondent block, where that block should contain the same information as written in the QR Code. If the information is different on both sides, the sold product is counterfeit, or there was an error during the insertion of data in the QR Code.

The information collected by the T&T technologies is inserted into the smart contract. The smart contract executes a transaction containing all the information collected to publish a block in the blockchain. It is essential to mention that the smart contract information is carried over to the next smart contract along the supply chain cycle, where only the essential information will be put in a block.

5.8. Comparison Between Centralised and Blockchain Supply Chain

The comparison between a centralised supply chain architecture and a blockchain supply chain architecture evaluates different characteristics of each architecture, where it can be an advantage or a disadvantage. Table 3 compares both architectures in different points, where the symbol plus means an advantage and the symbol minus means a disadvantage of that architecture compared to the other.

Table 3 - Comparison between Centralised and Blockchain Supply Chain Architectures

Features	Centralised Supply Chain	Blockchain Supply Chain
Trust-Building [1], [92], [93]	−	+
Transparency [13], [92]–[98]	−	+
Implementation Costs [92]	+	−
Cost Reduction [1], [92], [93], [95], [99]	−	+
Performance and Efficiency [92], [100]	+	−
Smart Contracts [92]–[94], [97], [98]	−	+
Legal and cultural procedures [92]	+	−
Auditability [13], [92], [93]	−	+
Security [1], [93], [98], [99], [101]	−	+
Scalability [1], [95], [98]	+	−
Privacy [92], [93], [95]	+/−	+/−

The first compared feature is trust-building. There are indeed factors that justify the advantages of trust-building in a blockchain supply chain over the centralised supply chain. First, the blockchain transactions are more transparent since those cannot be altered or tampered once completed, which means that no one can manipulate the product prices and supplies information, leading to increased trust within the system [92]. Second, there is a lack of trust related to the tracking and tracing a product on a centralised supply chain. For example, by using blockchain, if some raw material is exposed to a very high temperature or acidity, no one in the middle of the chain will be able to hide it from the final consumer. In the blockchain supply chain, this lack of trust may be lower than the centralised supply chain since it can keep immutable information from the raw material to the end consumer [93]. For last, the blockchain supply chain, besides having an internal supply chain trust, it has improved trust with the end consumer since the end consumer can confirm the provenance of the bought product [1].

The blockchain transactions are transparent since the participating nodes can view the transaction made while maintaining some degree of privacy on some transaction data [13], [92], [97]. On the other hand, a centralised supply chain does not offer the same level of transparency as a blockchain supply chain, wherein in some cases, if not most, the transactions are kept confidential from the rest of the participants of the supply chain due to the competition in the market [92]–[94]. This transparent feature in a blockchain supply chain system does not apply only to one transaction, but instead, it is applied to all the transactions made up to date. So, it is possible to confirm the origin and quality of the final product [93]. This feature also leads to decreased fraudulent actions and conduct violations in the supply chain system [13].

On one hand, the implementation blockchain technology in a supply chain can be very costly compared to a centralised supply chain system, which means that it is essential to evaluate the possibility of implementing costs [92]. The implementation is expensive because, since this is a new technology, few professionals are capable of implementing such systems (therefore these professionals are more expensive). On the other hand, blockchain technology brings many benefits to the cost reduction compared to a centralised supply chain system [93]. The increased transparency and trust can make up for the implementation cost, reducing the cost over time. Also, there is a cost reduction due to smart contracts since those are responsible for executing transactions automatically, saving time and money on the process [1], [92].

So far, performance is the main weakness of blockchain, mostly when compared to a centralised system. However, this subject is being widely studied and for supply chain, and so far, it was not detected any prohibitive bottleneck [92], [100].

Typically, the centralised supply chain is prone to human errors, fraud, and failure, which decreases the overall system performance. Blockchain is less prone to those errors since all the system's actions involve transactions. Optionally smart contracts accelerate the information flow either without or fewer errors than the centralised transactions, thereby increasing the system performance [93].

As for smart contracts, they are enhanced in the implementation of blockchain. The Hyperledger Fabric framework allows for easy implementation and deployment of smart contracts. The smart contracts will play a significant role in the efficiency of the overall supply chain system with the potential to be used in different phases of a supply chain such as the validation of shipments, the tracking and tracing of products, and the validation of transaction information [92], [94], [97].

In terms of legal and cultural procedures, those are still a challenge for the implementation of blockchain in a supply chain system. Since blockchain is in its infancy, there is a lack of studies demonstrating the application and implementation of blockchain in supply chains, which creates a barrier in terms of cultural procedures. This cultural barrier is related to the difficulty of changing people's mindsets to implement blockchain and adopt specific procedures related to the blockchain [92]. Those barriers demonstrate that centralised supply chain is still preferred among the organisations regarding legal and cultural procedures, even with the high hype over blockchain (due to its usage in bitcoin).

Blockchain systems provide a better auditability than a centralised one. It can enhance the auditability of the supply chain since the data stored in immutable blocks (block data cannot be tampered), and also, the smart contracts are immutable, and their rules are available for the exchanging parties [13], [92], [93].

Another essential and concerning feature among the supply chain organisations is security. Typically, centralised supply chains have some degree of security implemented, but when compared to a blockchain supply chain, blockchain's implementation enhances the supply chain's overall security. The blockchain supply chain is more secure than a centralised supply chain because of the decentralised system feature that comes with blockchain.

Aforementioned, blockchain already has an integrated authentication system, and therefore it reduces security problems. Not all centralised systems are careful to implement an equivalent authentication mechanism. Therefore, it is essential to note that centralised systems can be as safe as those that use blockchain. However, there is no guarantee that centralised systems are always secure as blockchain systems (in many cases, there are certifications that carry out this guarantee). In the case of blockchain, this feature is native to the solution. Also, in terms of

blockchain security, multiple nodes store the transaction information in a ledger. This ledger is immutable, which means that the transaction information, once published it cannot be tampered, where any attempt of modification or fraud could be easily detected [1], [93], [101].

Comparing scalability in both architectures, based on literature, the authors refer that scalability is still a challenge in blockchain applications. Current centralised systems in centralised supply chains are more scalable than a decentralised system blockchain supply chain. There are scalability problems related to the throughput limit, latency, and block size. The proposed architecture uses as a framework, the Hyperledger Fabric, which has a high throughput. However, it is not high as a centralised system, which means that the current blockchains do not process the information faster than centralised supply chains. The latency is another problem that affects the scalability but only for public blockchains. Hyperledger has a low latency even with a high number of transactions, which means that latency is not a problem in the proposed architecture. So, it will not affect the scalability in this case. Another scalability problem is related to the block size, where the size grows with the number of transactions stored in a block, where bigger block sizes affect the performance and throughput of the blockchain. Therefore it affects the scalability [1], [95]. These types of scalability issues can be solved in different ways. For example, it can be increased the block size, and the number of bytes of information for each block can be reduced to increase the transaction throughput [98]. Those solutions should give a perspective that scalability is not a drawback when implementing blockchain in a supply chain.

For last, there is the privacy feature, which can or cannot be assured in both architectures, depending on the scenario. Privacy can be seen as a challenge by blockchain experts [92]. There are examples where it is possible to assure privacy and other examples where it is impossible to achieve that feature. For example, in blockchain, it is impossible to achieve privacy in public blockchains like bitcoin, where all the transactions are transparent to the other participants. On the other hand, it can be possible to achieve privacy in Hyperledger Fabric framework, since this framework was designed to give privacy in the transactions between participants. The centralised systems can face the same dilemma, where privacy is not guaranteed, but it can be implemented. Overall, it is important to refer that privacy faces a trade-off with transparency, and that trade-off should be taken into consideration when implementing both systems.

5.9. Off-Chain Supply Chain: An alternative solution for the Application Nodes

It is necessary to make several different systems to communicate with each other to implement a level three T&T system. For example, a food supply chain could demand different applications for the farmers, drivers of distributors, distribution warehouses, producer warehouses, production line, package suppliers, retailer, and the final consumer. For several reasons (costs, limitation of knowledge, legacy systems, etc.) can be a management challenge to implement some of these applications using blockchain technology. Even though the proposed architecture can be used in this scenario, but with an adjustment.

In this section, we will propose an extension of application nodes to be part of the blockchain supply chain. For this extension, we call it off-chain supply chain because the transactions can occur either inside and outside of the blockchain. The application nodes will centralise the communication of a group of applications. It receives all the generated data and processes them through smart contracts. Figure 34 shows how this alternative solution is implemented in the proposed T&T architecture.

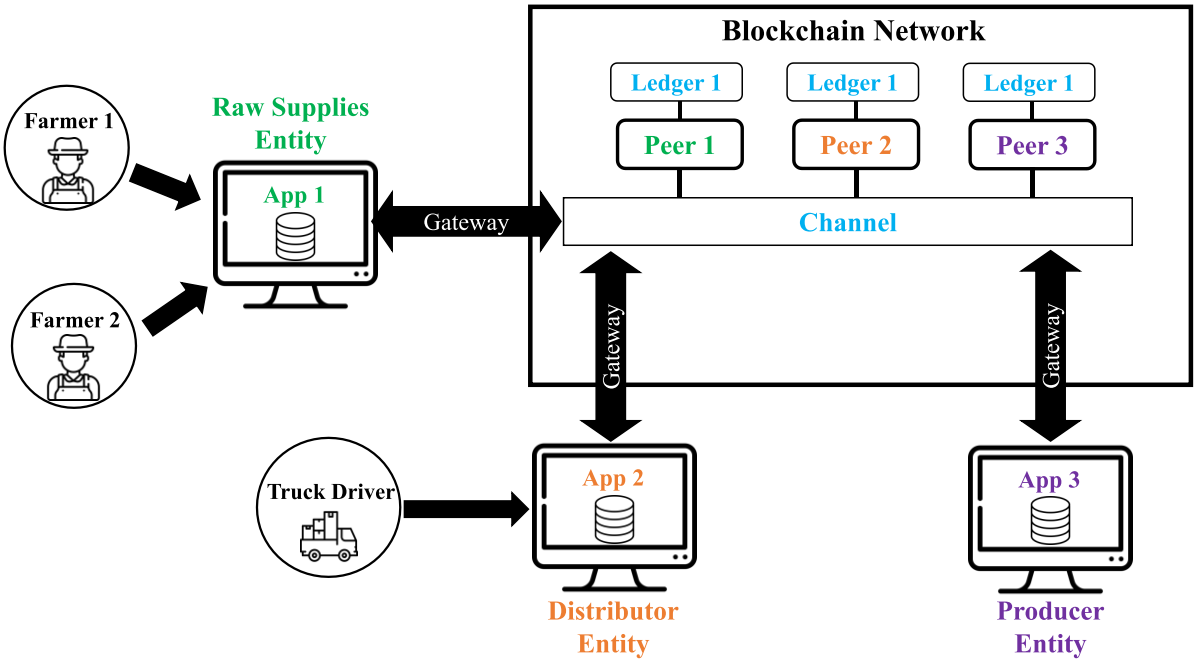

Figure 34 – Off-chain T&T architecture

In Figure 34, farmers and truck driver applications act like a child application (child of application node). They produce the data independently from the blockchain (can be a legacy system) and send it to the application node responsible for main storage. The main database is managed by the application node (e.g. Raw Supplies Entity or Distributor Entity). Posteriorly,

during a transaction, the application node must provide the information stored in the database to store it in the blockchain ledger.

It is important to highlight that the components outside of blockchain lose some important features such as integrity and immutability of data described for the kernel. It loses both features because the children application writes the data first in a database before its commitment to the ledger. There are no guarantees that the data stored in the database is tampered or modified during this process.

5.10. Real Use Cases

Nowadays, numerous sectors and organisations have tried to implement blockchain in their supply chains as an alternative to traditional supply chains.

In 2017, South Korea Hyundai Merchant Marine has conducted its first blockchain technology pilot voyage from shipment booking to cargo delivery. On this pilot voyage, it was combined the blockchain with IoT technology to test and review the real-time monitoring [102]. In 2018, Walmart started to use blockchain in its supply chain to reduce the time to trace the mango shipment from seven days to 2.2 seconds. In the same year, Walmart used blockchain in pork chain across China to assure food safety and quality by tracking and tracing the supply chain from farm to fork [103]. Another interesting example comes from the French retailer Carrefour, where they implemented a blockchain in the supply chain so the customers could trace the origins of the products in the store. The customers could check the product information by scanning a QR Code present in the product and see all the details about the product flow from the origin to the customer's location. This blockchain initiative raised the sales of the products targeted by blockchain and outperformed the other products that had no blockchain implemented [104].

Besides those examples, other organisations have already implemented blockchain in the supply chain. However, there is still a lack of blockchain implementation in supply chains due to the blockchain infancy. As mentioned earlier, the current sectors and organisations may face some obstacles related to the implementation costs, limitation of knowledge, legacy systems, etc.

6. Security in T&T Systems for Supply Chain

Security is a fundamental property that every digital system must have and is natively implemented in blockchains. Over the years, blockchain has been widely used for different purposes (cryptocurrency, healthcare, insurance, asset management), and with this increased usage, various types of attacks have emerged. The reality is that blockchain technology is still a new topic, and the tendency is that more organisations will use blockchain to solve or improve some of the organisation's needs [105].

The main security properties that a blockchain system can assure are confidentiality, integrity, availability, authentication, and non-repudiation. Confidentiality is assured when the information is kept private to trusted users. Integrity ensures that the message has not been modified during his transmission. Availability ensures that all the means are provided for authorised users to access and communicate in the network. Authentication validates network users' identity, and non-repudiation ensures that the users cannot refute their actions on the network [106]. Blockchains can only assure some of the mentioned properties. For example, Bitcoin cannot assure confidentiality [41].

Since this topic is about blockchain and its security, it is essential to mention some blockchain elements that have a key role in security and operation correctness.

The first element is asymmetric-key cryptography, also called public-key cryptography, that uses a pair of keys, one called public-key, and the other is called private-key [51]. Another crucial element is the digital certificate, which confirms the certificate holder's real identity, providing a trust relationship on the network. In digital certificates, every certificate holder has an asymmetric key pair that can be used later to exchange information in a confidential way [107].

To further understand this topic, it is essential to give an inner view of each element, explaining its role on the blockchain and its interactions with other blockchain elements.

6.1. Cryptography as the basis of security

Cryptography can be described as a set of principles and techniques used to secure information and communications. It is possible to achieve the essential components in security with cryptography, such as confidentiality, integrity, authenticity, and non-repudiation. We can use cryptography in different flavours to achieve these security components, such as symmetric-key cryptography, asymmetric-key cryptography, and hash functions [108]. In this section, we

will briefly mention the hash functions and the asymmetric-key cryptography, in particular the Elliptic Curve Digital Signature Algorithm (ECDSA).

Asymmetric cryptography, also called public-key cryptography, is a cryptography scheme that uses a pair of keys for encryption and decryption. From that pair of keys, one key is called public-key, and the other key is called private key. The public key can be shared with anyone, and the private key is private because it must be kept in secret (only for the owner) [109].

In Figure 35, it is shown an asymmetric-key cryptography scheme assuring only confidentiality on the process. In this scheme, **(1)** Alice generates a key pair, keeps the private key secret, and **(2)** sends the public key to Bob. **(3)** Once Bob has Alice's public key, he can use that public key along with an encryption algorithm to encrypt a document and **(4)** send it to Alice. Finally, **(5)** Alice receives the encrypted document and uses her private key along with the decryption algorithm to decrypt the document sent by Bob.

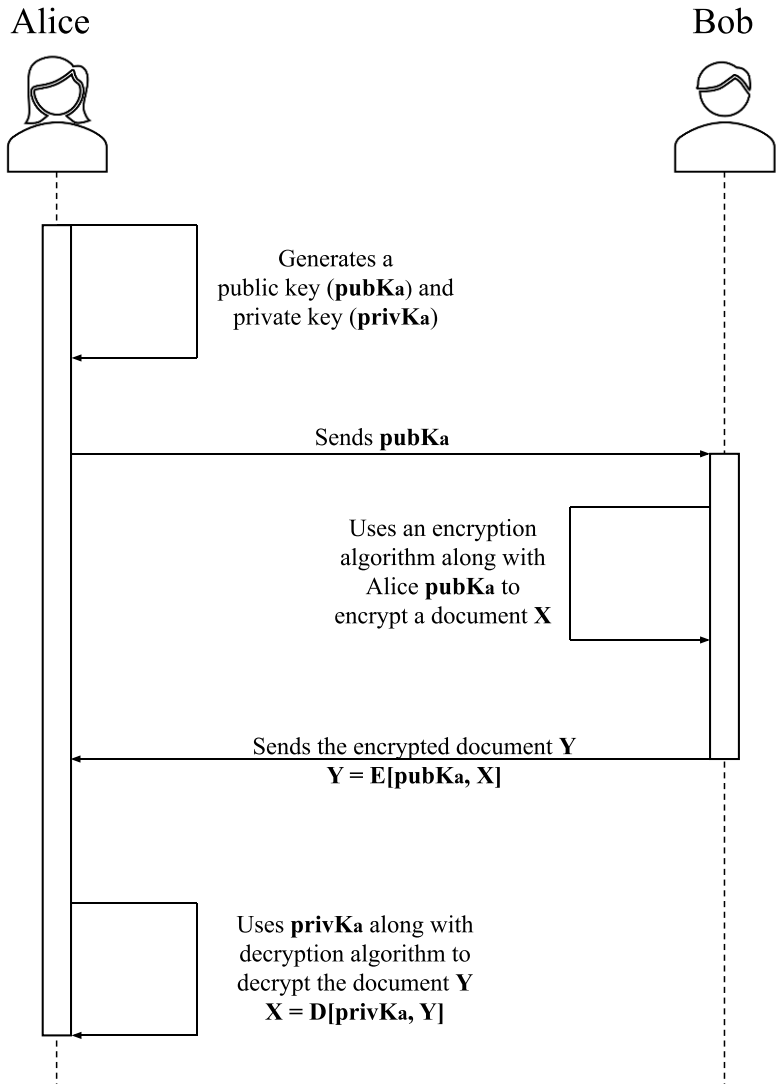

Figure 35 - Asymmetric-Key cryptography scheme assuring only confidentiality

Suppose a user wants authenticity instead of confidentiality. In that case, the user must encrypt the information with his/her private key. The receiver decrypts it with the user's public key, ensuring that it came from that specific user and not from another user.

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a combination of Digital Signature Algorithm (DSA) with Elliptic Curve Cryptography (ECC) and is mainly used for digital signatures. This algorithm will assure data integrity, data origin authentication, and non-repudiation when compared to RSA. Elliptic Curve keys have a smaller size for the same security parameters, which means that it is more efficient to compute a key generation by using ECC algorithm or an algorithm that uses ECC derivative. ECDSA is used in three digital signature phases: key generation, signature generation, and signature verification [110].

For last, it is essential to refer the hash functions since they are used in the signature generations and for signature verification. The hash functions take a variable-length input, for example, a text with any length, and produces an alphanumeric fixed-length output. For example, we have a document with a specific hash value. Suppose any information is changed on that document. In that case, the hash value produced is completely different from the original document, which means that the hash function is essential to ensure data integrity [109]. According to the National Institute of Standards and Technology (NIST), hash functions should be used at least a Secure Hash Algorithm 1 (SHA-1) or better for non-digital-signature applications or Secure Hash Algorithm 2 (SHA-2) or better for all hash function applications [111]. SHA-1 is disallowed for digital signature generation since it was already proven that SHA-1 is a broken hash function [112].

Cryptography plays a fundamental role in securing communications and information between multiple entities. As a part of cryptography, there is asymmetric cryptography and hash functions, which will be used for digital signatures, an essential component in digital certificates.

6.2. Digital Certificates and Digital Signatures

A digital certificate, also called a public-key certificate, is an electronic document that identifies an entity (an individual, a server, a company, or another entity) and associates that identity to a public key. Digital certificates are issued by certificate authorities (CA), and it contains a unique feature called digital signature. This digital signature addresses the problem of impersonation [113]. The digital certificate will enhance the communication's security by assuring the

authentication of the entities on the network, assuring the confidentiality and integrity of any message transmitted.

The standard format for the digital certificate is the X.509 certificate, which was first published in 1988 as part of the X.500 directory recommendations, and it was called X.509 certificate version 1. Version 2 was published in 1993 due to a revision of X.500, where two more fields were added, and three years later, it was published version 3, where it was added additional extension fields on the certificate [114]. Nowadays, X.509 certificate version 3 is widely used in web browsers that support the Transport Layer Security (TLS) protocol providing authentication and confidentiality on the network traffic. Also, it is included in different types of technologies such as in e-mails, in various code-signing schemes and e-commerce protocols [115]. The X.509 version 3 certificate has the following structure:

Data:

Version: 3

Serial Number: 123

Signature Algorithm: sha256WithECDSA

Issuer: Country Name (CN)= US, State (ST)= New York, Locality(L)= Armonk, Organisation (O)=IBM, Organisational Unit (OU) = HQ,
Common Name (CN) = IBM Headquarters

Validity:

Not Before: Apr 29 17:34:21 2020 GMT

Not After: May 30 17:34:21 2021 GMT

Subject: CN = US, ST = New York, L = Poughkeepsie, O = IBM, OU = TPF, CN = John Doe

Subject Public Key Info:

Public Key Algorithm: ECDSA

ECDSA Public Key: (256 bit)

Modulus (256 bit):

41:14:41:53:56:a5:48:e6:4c:84:6f:95:49:46:6d:c7:64:84:79:e5:59:14:4
1:14:62:d6:7a:44:41:94:54:94:41:14:42:24:4d:63:34:47:7a:e3:4d:83:4a
:85:77:84:52:a4:38:93:74:35:66:f6:78:13:71:93:74:46:33:84:4c:c6:65:
16:53:54:2b:35:2b:c7:78:f2:2b:64:50:04:53:27:37:34:58:24:56:b6:6e:6
4:39:54:67:d2

Exponent: 45342

Signature Algorithm: sha256WithECDSA

35:73:55:13:53:a5:48:e6:4c:84:6f:95:49:46:6d:c7:64:84:79:e5:59:14:41:14:62:d
6:7a:44:21:94:23:94:31:14:42:84:4d:63:34:47:7a:e4:3d:83:4a:85:77:84:52:a4:3
8:93:74:35:66:f6:78:13:71:93:71:46:33:84:4c:c6:65:16:53:54:2b:35:2b:c7:78:f2
:2b:64:50:04:53:27:37:34:58:24:56:b6:6e:64:39:54:67:e3

Figure 36 - Adapted X.509 version 3 certificate structure example [116]

In Figure 36, all the values were created only for demonstration purposes. On the *version* field, it is specified the version of the X.509 certificate, where the version describes the syntax of the certificate. The *serial number* field contains a unique number attributed by the certificate issuer. The *signature algorithm* describes the digital signature algorithm used to protect the certificate. The *issuer* field contains information about who generated the certificate, and the *validity* field contains information about when the certificate becomes valid and when the certificate expires. Also, on the certificate, there is a *subject* field containing the information about the holder of the certificate, and the subject public key info contains the algorithm used to generate the public key and the public key of the certificate holder. For last, there is a *signature algorithm* along with the signature from CA.

From the fields mentioned, all of them are used in all versions of the X.509 certificate. On version 2 and version 3, the certificates have two fields called *issuer unique ID* and Subject unique ID, which contains a unique ID to handle the reuse of subject names or issuer names over time. However, this field was proven to be an unsatisfactory solution, where it is not recommended the inclusion of this field on the certificate. The version 3 certificate has one more optional field called *extensions*, containing one or more extensions, including an extension identifier, a criticality flag, and an extension value [117].

Not only is it essential to know the contents of a digital certificate, but it is also essential to know who issues the digital certificates and the role of that entity in the process.

The certificate authority (CA) is responsible for providing digital certificates that will be used to identify an entity, making the CA a trustworthy third party that will assure that all the confidential information is secured against any misuse. The CA provides a digital certificate by signing a certificate with the CA private key, but it is only signed if the entity can prove its identity. If there is a CA signature on the digital certificate, then the CA confirms that the owner of the public key is the entity mentioned on the certificate specifications [118]. It is essential to mention that the CA also has a certificate, which means that it is possible to verify the identities that issued that CA certificate. Those identities can be a Root CA or an Intermediate CA. The Root CA distributes many certificates for users, and this distribution process is spread across

intermediate CA. The intermediate CA has its certificate issued by another intermediate authority or by a root CA to establish a “chain of trust” for any certificate issued by any CA in the chain [80].

What if a certificate expires or an external entity requests an entity’s identity based on a public key? CA cannot do that work, and that is where public key infrastructure comes to help.

The public key infrastructure (PKI) is comprised of CA, which issues digital certificates, as mentioned before, and a certificate revocation list (CRL), which contains a list of all revoked certificates. Also, PKI manages the public keys by binding the entities’ identities with their respective public keys, and this binding is done by having a CA issuing certificates [63].

It is mentioned that there are signing and verification processes on digital certificates, but how is this process done in reality?

First, the CA sign the certificates with a digital signature to issue a digital certificate, which can be later verified to confirm whether the digital certificate is valid.

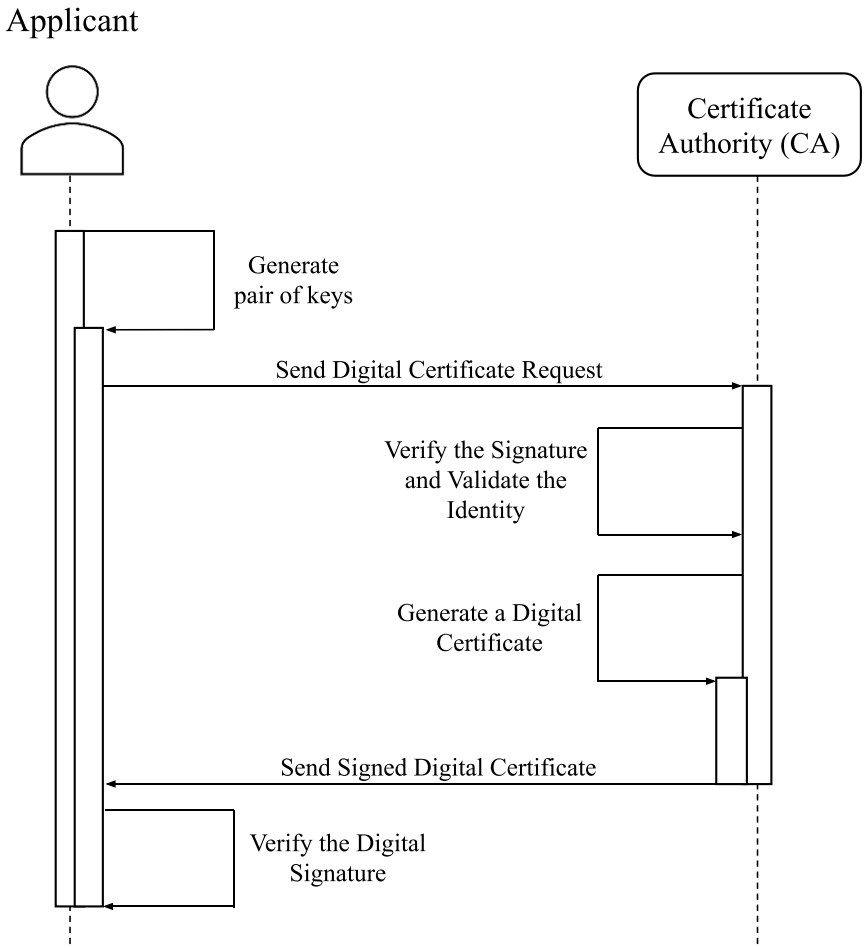

Figure 37 - Digital certificate acquisition process

Figure 37 shows a digital certification acquisition process between an entity and the CA, more precisely how an entity can obtain a CA's digital certificate. (**1**) An entity should generate a public and a private key that will be used for the digital certificate. (**2**) The entity sends a request to the CA, and this request has included a unique identifier called Distinguished Name (DN), the entity public key, and a signature from the entity. (**3**) The CA then verifies the signature by using the entity public key and verifies its identity to validate the request. After all the verification process, (**4**) the CA generates a signed digital certificate containing all the entity's information and containing the CA that issued the certificate along with the CA signature. For last, (**5**) the CA sends the signed digital certificate to the entity, and then (**6**) the entity verifies the digital signature of the signed digital certificate to confirm that the CA that issued the certificate is legitimate and trustworthy [119].

The digital certificate is associated with the digital signature, which is an electronic signature used to ensure authenticity and integrity over the transmitted data. The applicant can create digital signatures with the private key generated for the digital certificate. The digital signature uses asymmetric key cryptography, and it is being used in blockchain for authenticating transactions and validating user's transactions [58], [120].

Figure 38 and Figure 39 show the signing and the verification process of digital signatures, respectively.

For the signing of a digital signature (Figure 38), the signer first uses a hash algorithm on data to generate a hash. After that, the signer uses its private key to encrypt the generated hash creating an encrypted hash, also known as a digital signature. For last, the digital signature is combined with the signer certificate and with the data to create digitally signed data [120].

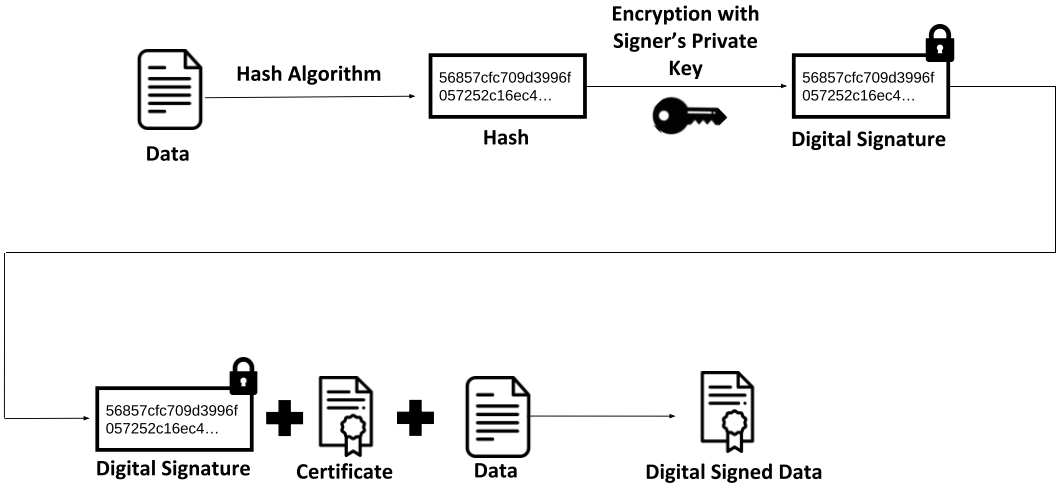

Figure 38 - Digital signature signing process

As for the digital signature verification (Figure 39), the entity that receives the digitally signed data uses a hash algorithm in data to produce a hash of the data. It also uses the signer's public key to decrypt the digital signature to get a hash of the data. Posteriorly, the two hashes values obtained are compared, where if they match, then the signature is valid. If the two values do not match, then the signature is not valid, which means that the data was tampered [120].

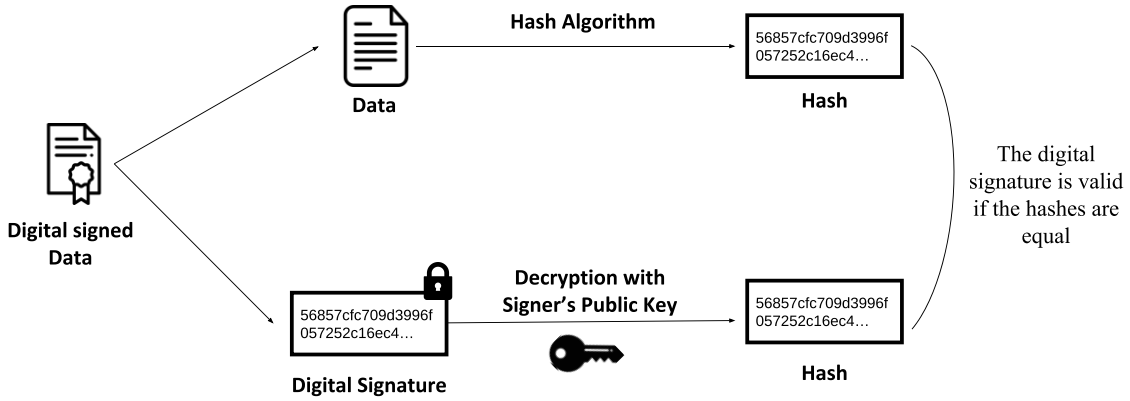

Figure 39 - Digital signature verification process

6.3. Implementation of Digital Certificates in Blockchain Supply Chain

In the previous sections, we have contextualised in a generic way how cryptography, digital certificates, and digital signatures can be used for any system (even if it is not a T&T system). From now on, we will discuss how to implement digital certificates in the blockchain supply chain.

There are two different workflows for digital certification that can be used in the Blockchain Supply Chain. Each workflow has its respective applicability, which should give an idea of where it is possible to implement.

The first workflow model is a centralised CA model (Figure 40), which means that only one CA issues the digital certificates for all the blockchain network entities. That same CA belongs to an organisation, and it is connected to a Membership Service Provider (MSP) that will do a mapping of certificates to member organisations [121], [122].

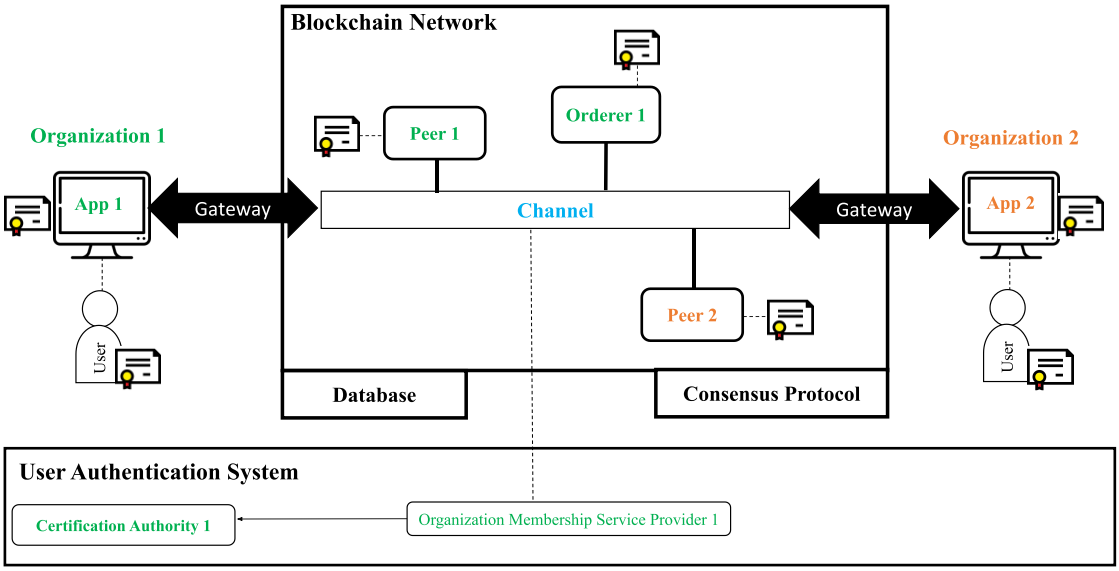

Figure 40 - Centralised CA workflow model

This first model can be applied, for example, when one organisation is trusted by all of the other organisations, especially when the trusted organisation is an accredited entity. Also, this approach is suitable for the off-chain application nodes scheme presented in Section 5.9.

The second workflow model is a multiple CA's architecture model (Figure 41), where each organisation has its own CA, and each CA is connected to their MSP. Each organisation entity has a digital certificate issued by its organisation CA [121], [122].

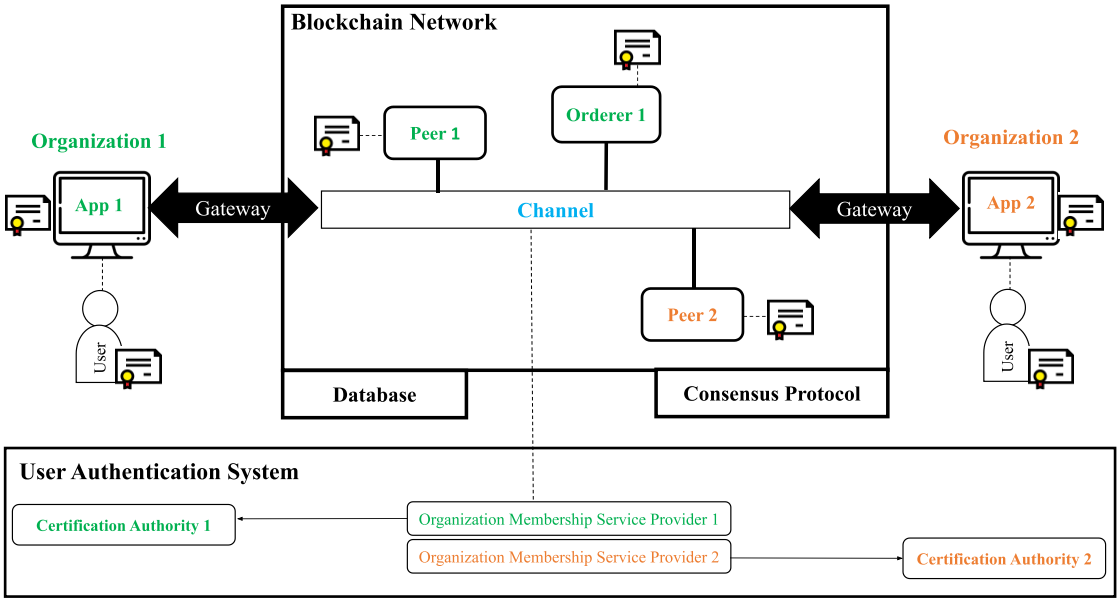

Figure 41 - Multiple CA's workflow model

This model can be applied to cases where there is no trust between organisations and no accredited entity on the network. The second model is better suitable for a Blockchain Supply Chain.

6.4. Security Concerns Towards Quantum Computing

Some authors are worried about the impacts of quantum computing on blockchain security. Multiple reports are stating and measuring the real impacts of quantum computers in the current blockchains. The real concerns are focused on the cryptographic features, where the practical quantum computer systems could weaken or even break some of the existing cryptographic algorithms.

Based on a NIST report [51], quantum computing could impact seven types of cryptographic algorithms: AES, SHA-2, SHA-3, RSA, ECDSA, ECDH, and DSA. As for the Elliptic Curve Cryptography (ECDSA and ECDH) and Finite Field Cryptography (DSA), these algorithms are no longer secure with the introduction of quantum computers. However, the impact around AES, SHA-2, and SHA-3 algorithms can be solved by increasing the AES's key size and by increasing the output in SHA-2 and SHA-3. In a technical report [24], the authors described two quantum algorithms that pose a threat to the existing blockchain systems, where these algorithms are Grover's algorithm and Shor's algorithm. Grover's algorithm is responsible for known attacks such as full collision attack and mining time attack, and Shor's algorithm is responsible for the attacks on RSA encryption. Explaining in a more detailed way, on Grover's full collision attack, it searches for hash collisions using a brute force search. For the mining attack, the algorithm speeds up the generation of nonces to the point of recreating the entire chain of records with consistent modified hash values to undermine the integrity of the blockchain. As for Shor's algorithm, this algorithm can break the security of RSA encryption. Once the public/private keys are discovered, the information exchanged between the parties or the digital signatures is no longer secure/valid.

As already mentioned, most blockchains use Elliptic Curve Cryptography for signatures and key exchange in the network. So, the authenticity of each blockchain node can no longer be assured. Since this type of cryptographic algorithm is no longer secure with quantum computing, there is a need to replace such an algorithm if quantum computing becomes a reality. In the same technical report [123], it is discussed a few possibilities for the replacement of both hash and encryption algorithms in blockchain systems, what the authors called the post-quantum cryptography.

7. Theoretical Analysis of Blockchain Supply Chain

This chapter discusses the Blockchain Supply Chain architecture properties, such as privacy, auditability, transparency, scalability, and performance. Each one of these properties is analysed in a theoretical way. It is explained how each property is present in the proposed architecture and how this property contributes to the proposed architecture. Also, we analyse the benefits of the accreditation and certification in the proposed architecture as well as the role of trust as a subjective property. Trust is a subjective property because it is related to how well the system performs in the other analysed properties such as auditability, privacy, transparency, security, etc.

7.1. Privacy

Privacy is a desired property since it is responsible for assuring that sensitive information is exchanged only between the authorised entities. There is a trade-off between data consistency and privacy. The first one is achieved by sharing the data between all nodes. However, since the data is exposed to all nodes, privacy can be an issue for blockchain. However, privacy was not neglected by blockchain technological solutions. For example, the Hyperledger Fabric framework has addressed this subject.

Nevertheless, there are challenges related to privacy. For example, if the security system fails, it means that there may have been a leak of confidential data. Another example of a privacy challenge is that data is shared by all nodes in a distributed system. The blockchain supply chain solution can address some privacy challenges. As mentioned above, blockchain has a security mechanism that protects confidential data between two entities. As for a distributed system, not all blockchains can assure privacy. However, in the Fabric framework, privacy is assured by a component named channel, assuring the participants' data privacy and confidentiality. In Hyperledger Fabric, a subset of nodes is designated to a specific channel. The peers who participate in that channel are the only ones that can store any transaction data. The other peers cannot access the transaction data. Only it is provided with the hashes of the transaction data [86].

Another concerning topic when referring to privacy is the General Data Protection Regulation (GDPR). It is essential to take into account this European Regulation when talking about privacy. However, in this work, we will not cover this topic.

7.2. Auditability

In the proposed architecture, the blockchain itself has an audit capability, where audit can be defined as a "systematic, independent and documented process to obtain evidence by evaluating it objectively to monitors whether the audit criteria are fulfilled" [62]. In the blockchain, the data about the transactions are available to audit at any time. This transaction data is immutable, which means that the data cannot be modified or erased by anyone.

On the proposed architecture, the transaction data is private only for the peers of a specific channel. For that reason, there must be a way for the auditor to audit the private transactions in different channels. This audit capability on the proposed architecture can be achieved in different ways. The first one is that the organisations could share the certificates with the auditor, allowing him to access their peer nodes and posteriorly query the ledger history on that peer channel. The second option is an auditor that maintains a peer node on each channel or a peer node with access to all channels with the condition that the auditor peer(s) cannot act as an endorser for smart contract transactions. By being on the channel, it would commit all the transactions to its ledger. The third and last option would be in the audit time, the auditor could join as a peer in the channel to receive all the transaction data, and once the audit is done, the auditor is removed from the channel. From the three options, the one that gives more privacy is the third one since the auditor can only access the transactions data during the audit. In contrast, in the other options, the auditor can have access at any time, leading to privacy issues.

7.3. Transparency

The blockchain in the proposed architecture is the one that gives transparency to the supply chain. Blockchain is supposed to be a transparent technology, where anyone can join the network and view all the information on that network. However, transparency is tangled with privacy, and so, the higher the transparency, the lower the privacy and vice-versa (trade-off) [124]. This trade-off can be seen as a challenge for current T&T systems and in some blockchain systems. There is a dilemma around this topic since it can either be assured full or partial transparency in the blockchain. It depends whether the information is disclosed publicly or disclosed only to all the network's participant entities.

In the proposed architecture, it is indeed essential to balance privacy with transparency. Some degree of privacy is already implemented in the blockchain supply chain architecture. Only the participants of a specific channel can store the transaction data on the ledger. The other participants will only store the hash value of that data in the ledger. This solution will only give

partial transparency in exchange for the transaction's privacy made between two or more organisations. At least some transparency is essential between the blockchain participants and the end consumer. When the end consumer retrieves data about the product, it is essential to maintain some degree of privacy on the retrieved data.
It is essential to remember that more transparency equals to more trust. However, there always be necessary to include some privacy in the systems.

7.4. Scalability and Performance

Scalability is a desirable attribute in any system, network, or process. It is defined as "the ability of a system to accommodate an increasing number of elements or objects, to process growing volumes of work gracefully, and/or to be susceptible to enlargement" [125]. There is no global definition of performance since it can be applied in different fields. For example, performance can be applied to a human, team, organisation, systems, etc. According to the Oxford English Dictionary, performance is defined as "the act or process of performing a task, an action, etc." Based on this definition, a higher performance is related to a faster process of performing a task, and a lower performance is the opposite.
It is important to discuss scalability and performance because they are correlated. Poor scalability can result in poor system performance [125]. The analysis of scalability and performance is based on the Hyperledger Fabric framework since this is the framework used in the proposed blockchain supply chain architecture.
The Fabric framework was designed to increase scalability in the blockchain. For example, the blockchain transactions are executed in parallel by the endorsers, which increases the performance. This framework uses channels responsible for splitting the blockchain into many private blockchains, thus increasing the system's scalability. Considering the different blockchain types and their scalability, Hyperledger Fabric sacrifices some decentralisation to improve the scalability and performance compared to other blockchains. However, there are scalability and performance constraints in Fabric related to the block size and endorser scaling. The block size impacts the performance of the transactions made per second. The throughput of a transaction can be increased by increasing the block size, but at some point, the block size is already too bigger that the performance starts to decrease. The optional number of transactions per block is 100 transactions based on performance tests, with a maximum throughput of 350. Endorser scaling is another problem that impacts performance. Adding endorsers on different channels does not have an impact on the performance of a channel.

However, adding multiple endorsers to a single channel can significantly impact that channel's performance, where the more endorsers are on the channel, the fewer transactions per second occur [126].

7.5. Accreditation and Certification

Both accreditation or certification provides various benefits for the business industries. According to the European Accreditation Association, accreditation is defined as the formal recognition of a conformity assessment body's technical and organisational competence to carry out specific services following the standards or technical regulations [127]. An accredited authority can issue certificates to an organisation. For example, the certification body needs an accreditation license to issue certificates. Also, it is essential to mention that there is one accreditation body for each country. In Portugal, for example, the accreditation body is called Instituto Português de Acreditação (IPAC) [128]. Accreditation bodies must be compliant with ISO 17011, which is a standard that defines the process of accreditation according to European Accreditation Association [127]. The accreditation adds value to supply chains, where the businesses can maintain the level of confidence in the products while seeking to maximise the value and satisfying the contractual terms. Besides offering a range of services, accreditation can add value and manage the potential risks in supply chains by assessing certification, inspection, testing, and calibration services, which increases the trust relationship between the business partners in a supply chain [129].

As for the certification, according to ISO standards [130], certification proves that an organisation complies with a standard. For an organisation to be certified, an audit must be performed by an independent certification body. There are multiple benefits of being certified. It proves compliance to customers and interested parties, the company or the organisation is recognised for its efforts, and in some industries, certification is a legal or contractual requirement. As an example of certifications, ISO 9001, ISO 27001, ISO 20000, and ISO 27001, being the last one specific for Information Security Management Systems, are the most common standards. Also, there is an article [131] explaining the motives and the benefits of implementing a certification according to ISO 9001 from a Portuguese experience, where the benefits of certification are mainly the following: increase in customers satisfaction, increase in "on time" deliveries and improvement in the relationship with authorities and with communities. There are more benefits and motivations mentioned in that article.

7.6. Trust

Trust is perceived as a significant component in business relationships, where, over time, the use of trust in business emerged. So, the concept of trust has gained importance in sectors based on relational links, such as supply chain industries [132]. The fewer the vulnerabilities in the process, the higher the trust between the entities involved. For example, traceability data's adulteration is a vulnerability that a T&T supply chain system can have.

In the proposed architecture, all the participating entities must have a good trust relationship. This trust relationship is based on a combination of applications, as shown in Figure 42.

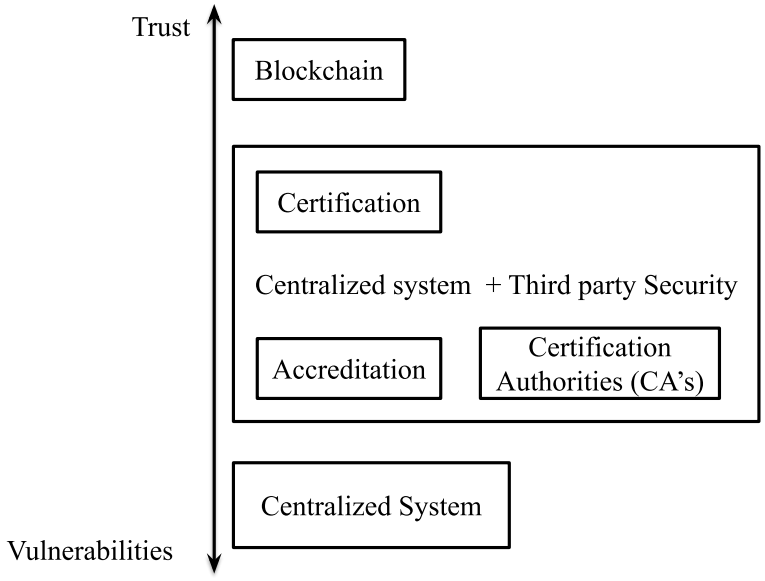

Figure 42 - Example of several applications and their relation between trust and vulnerabilities

In the proposed architecture, there are four components that will increase the trust relationship in the process. The first component in the proposed architecture is the blockchain. Blockchain plays a big role in this trust relationship between the different entities since blockchain assures all the published blocks' immutability, which means that it is impossible to change the contents of the block containing all the transactions once published. Another aspect is the capability of auditing a blockchain, which gives transparency of all actions done. These security and auditability capabilities make blockchain a suitable candidate for any application that requires the interaction between various stakeholders. Also, there is no third party involved in the transactions between the stakeholders. Implementing a blockchain will increase the overall trust between all the stakeholders on the process and, of course, increase consumer trust [133].

The second component that will increase trust is the accreditation and certification process mentioned in Section 7.5.

The third component is the decentralised infrastructure assured by the blockchain. The decentralisation property assures that a central authority gives the privileges to the subordinate authorities. In other words, decision-making privileges are delegated between different entities. The whole process does not have a single point of failure because multiple entities are managing the process, and the whole process is more transparent, which leads to increased trust between the stakeholders [133].

The fourth and last one is the certificate authority responsible for issuing digital certificates to all participating entities. Each entity must have a digital certificate from a trusted certificate authority to participate in the blockchain [63].

8. Conclusion

In this work, we have discussed a traceability system for a supply chain, emphasising a possible specific implementation using blockchain. We have built a traceability concept (at three levels) and discussed some concrete examples that exist for each level. We also have demonstrated a general architecture for implementing a traceability system for a supply chain of level three (the most complete) to maximise the confidence of the stakeholders involved in the process. This confidence can be improved thanks to the attention in the aspects of data quality (wide traceability), security, auditability, privacy, transparency, scalability and performance.

The choice to further analyse the use of blockchain in a decentralised implementation of the T&T architecture is because this technology presents excellent results in security, auditability, and privacy, without having signs of seriously compromising issues in transparency, scalability, and performance. Also, blockchain features such as immutability, data integrity, persistency, and consistency make it a good candidate for different applications and areas besides supply chain.

Also, broad traceability (level three) can be achieved by adding auto-ID and IoT technologies to application nodes (applications linked to application nodes). These technologies can help gather information about the product along the entire supply chain, from the raw materials to the end consumer.

A level three traceability system for a supply chain network brings numerous benefits to everyone involved. It expands access to data, bringing more engagement and confidence from the end consumers. It allows improvements in management since processes can be better understood, and predictions can be made in certain cases. It reduces the costs thanks to better flow control, and for last, it ensures a safer system, with less fraud and counterfeiting, due to the traceability of parts in this chain.

In this direction, we have proposed a conceptual system, which means that it was not implemented throughout this thesis. Currently, we do not know any system as complete as this one in use, and therefore, implementing it would be a challenge beyond this master thesis's scope. However, we still believe that the analysis conceptualises well the components of a level three traceability system for a supply chain and discusses the trade-offs of the theoretical aspects.

We believe that the absence of a system like this is due to the difficulty of convincing the diverse stakeholders in a supply chain network to adopt such a system due to costs (for implementation or adaptation of existing systems, training of operator, and eventual changes in operation) and

lack of confidence of the participants (in the system or other stakeholders in the chain). In other words, the greatest difficulty for the existence of such a system is, in our view, is more a question of management rather than a technological one.

Future research should focus on the practical implementation of the proposed architecture and, posteriorly, an analysis of the practical implementation in a real-world context.

References

[1] P. Costa, “Supply Chain Management with Blockchain Technologies,” University of Porto, 2018.

[2] GS1, “GS1’s framework for the design of interoperable traceability systems for supply chains,” *GS1 Global Traceability Standard*, 2017. [Online]. Available: https://www.gs1.org/sites/default/files/docs/traceability/GS1_Global_Traceability_Standard_i2.pdf. [Accessed: 20-Jul-2020].

[3] E. Kok *et al.*, “Traceability,” in *Chemical Analysis of Food: Techniques and Applications*, Elsevier Inc., 2012, pp. 465–498.

[4] J. Duan, C. Zhang, Y. Gong, S. Brown, and Z. Li, “A content-analysis based literature review in blockchain adoption within food supply chain,” *Int. J. Environ. Res. Public Health*, vol. 17, no. 5, pp. 1–17, 2020.

[5] Z. Eser, B. Kurtulmusoglu, A. Bicaksiz, and S. I. Sumer, “Counterfeit Supply Chains,” *Procedia Econ. Financ.*, vol. 23, pp. 412–421, 2015.

[6] WHO, “1 in 10 medical products in developing countries is substandard or falsified,” 2017. [Online]. Available: https://www.who.int/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified. [Accessed: 20-Jul-2020].

[7] Centers for Disease Control and Prevention (CDC), “Surveillance for Foodborne Disease Outbreaks United States, 2017: Annual Report,” Atlanta, Georgia, 2017.

[8] GS1, “The need for global standards and solutions to combat counterfeiting,” *White Paper*, 2013. [Online]. Available: https://www.gs1.org/docs/GS1_Anti-Counterfeiting_White_Paper.pdf. [Accessed: 28-Jul-2020].

[9] K. M. Karlsen and P. Olsen, “Problems and Implementation Hurdles in Food Traceability,” in *Advances in Food Traceability Techniques and Technologies*, Elsevier Ltd, 2016, pp. 35–46.

[10] A. H. M. Shamsuzzoha, M. Ehrs, R. Addo-Tenkorang, D. Nguyen, and P. T. Helo, “Performance evaluation of tracking and tracing for logistics operations,” *Int. J. Shipp. Transp. Logist.*, vol. 5, no. 1, pp. 31–54, 2013.

[11] B. De Cindio, F. Longo, G. Mirabelli, and T. Pizzuti, “Modelling a traceability system for a food supply chain: Standards, technologies and software tools,” in *10th International Conference on Modeling and Applied Simulation*, 2011, pp. 488–494.

[12] A. Shamsuzzoha, M. Ehrs, R. Addo-Tengkorang, and P. Helo, “Tracking and Tracing of

Global Supply Chain Network: Case Study from a Finnish Company," in *17th International Conference on Enterprise Information Systems*, 2015, pp. 46–53.

[13] S. Aich, S. Chakraborty, M. Sain, H. I. Lee, and H. C. Kim, "A Review on Benefits of IoT Integrated Blockchain based Supply Chain Management Implementations across Different Sectors with Case Study," in *International Conference on Advanced Communication Technology (ICACT)*, 2019, pp. 138–141.

[14] I. Giannoccaro and A. Capaldo, "Assessing the benefits of supply chain trust: NK Simulation-based methodology and application," *Emerg. Complex. Organ.*, pp. 1–11, 2017.

[15] GS1, "About GS1." [Online]. Available: https://www.gs1.org/about. [Accessed: 16-Nov-2020].

[16] I. Issuer, "New way of tracing tobacco products." [Online]. Available: https://idissuer.ee/?lang=en. [Accessed: 16-Nov-2020].

[17] A. Shamsuzzoha and P. Helo, "Real-time tracking and tracing system: Potentials for the logistics network," in *International Conference on Industrial Engineering and Operations Management*, 2011, pp. 242–250.

[18] IMR, "Qual a importância da rastreabilidade de alimentos?," 2019. [Online]. Available: https://www.imr.pt/pt/noticias/qual-a-importancia-da-rastreabilidade-de-alimentos. [Accessed: 11-Nov-2020].

[19] Cognex, "EAN-8 Barcodes." [Online]. Available: https://www.cognex.com/resources/symbologies/1-d-linear-barcodes/ean-8-barcodes. [Accessed: 19-Nov-2020].

[20] Cognex, "EAN-13 Barcodes." [Online]. Available: https://www.cognex.com/resources/symbologies/1-d-linear-barcodes/ean-13-barcodes. [Accessed: 19-Nov-2020].

[21] S. Qiao, Z. Wei, and Y. Yang, "Research on vegetable supply chain traceability model based on two-dimensional barcode," in *6th International Symposium on Computational Intelligence and Design*, 2013, vol. 1, pp. 317–320.

[22] L. Cruz, B. Patrao, and N. Goncalves, "Graphic code: A new machine readable approach," in *IEEE International Conference on Artificial Intelligence and Virtual Reality, AIVR*, 2018, pp. 169–172.

[23] INCM, "INCM está na Consumers International Summit 2019," 2019. [Online]. Available: https://www.incm.pt/portal/noticias.jsp?nid=1628. [Accessed: 10-Nov-2020].

[24] K. V. Singh and R. K. G. V. V, “Improving Manufacturing Enterprise Efficiencies Through Track and Trace Technologies,” *White Paper*, 2018. [Online]. Available: https://www.infosys.com/engineering-services/white-papers/documents/improving-efficiency-manufacturing.pdf. [Accessed: 28-Apr-2020].

[25] T. Lotlikar, R. Kankapurkar, A. Parekar, and A. Mohite, “Comparative study of Barcode, QR-code and RFID System,” *Int. J. Comput. Technol. Appl.*, vol. 4, no. 5, pp. 817–821, 2013.

[26] L. Bi, Z. Feng, M. Liu, and W. Wang, “Design and implementation of the airline luggage inspection system base on link structure of QR code,” in *International Symposium on Electronic Commerce and Security*, 2008, pp. 527–530.

[27] B. Ahmed, T. Sriram, K. V. Rao, and S. Biswas, “Applications of barcode technology in automated storage and retrieval systems,” in *22nd International Conference on Industrial Electronics, Control, and Instrumentation*, 1996, pp. 641–646.

[28] H. Y. Sun, “The application of barcode technology in logistics and warehouse management,” in *First International Workshop on Education Technology and Computer Science, ETCS*, 2009, vol. 3, pp. 732–735.

[29] S. A. Ali, H. H. Rizvi, T. Akram, S. M. Hamza, and A. Ifthikhar, “Calorie Consumer by using Barcode,” in *International Conference on Information Science and Communication Technology (ICISCT)*, 2020, pp. 1–3.

[30] S. Tiwari, “An introduction to QR code technology,” in *15th International Conference on Information Technology, ICIT*, 2016, pp. 39–44.

[31] R. Patel, N. Patel, and D. Patel, “Next Generation of Auto-ID: Applying RFID Technology,” in *IEEE International Advance Computing Conference*, 2009, pp. 2705–2710.

[32] J. Slovak, P. Vasek, M. Simovec, M. Melicher, and D. Sismisova, “RTLS tracking of material flow in order to reveal weak spots in production process,” in *22nd International Conference on Process Control, PC*, 2019, pp. 234–238.

[33] M. Z. Hoque, “Basic Concept of GPS and Its Applications,” *IOSR J. Humanit. Soc. Sci.*, vol. 21, no. 3, pp. 31–37, 2016.

[34] E. Hernández-orallo, P. Manzoni, and S. Member, “Evaluating how smartphone contact tracing technology can reduce the spread of infectious diseases : the case of COVID-19,” *IEEE Access*, pp. 1–15, 2020.

[35] J. Eriksson, “Towards a more efficient Supply Chain: A study at Bombardier Rail Control Solutions with a focus on centralizing their Supply Chain,” KTH Royal Institute

of Technology in Stockholm, 2017.

[36] H. Bhoir and Ranjana, “Cloud Computing For Supply Chain Management,” *Int. J. Innov. Enginnering Res. Technol.*, vol. 1, no. 2, pp. 1–9, 2014.

[37] L. Probst, L. Frideres, and B. Pedersen, “Traceability across the Value Chain - Advanced tracking systems,” Luxembourg, 2015.

[38] D. M. Bridgeland and R. Zahavi, “Business Rule Models,” in *Business Modeling: A Practical Guide to Realizing Business Value*, 2009, pp. 139–181.

[39] N. M. Iacob and M. L. Moise, “Centralized vs. Distributed Databases Case Study,” *Acad. J. Econ. Stud.*, vol. 1, no. 4, pp. 119–130, 2015.

[40] S. Haber and S. Stornetta, “How to Time-Stamp a Digital Document,” *J. Cryptol.*, vol. 3, no. 2, pp. 99–111, 1991.

[41] S. Nakamoto, “Bitcoin : A Peer-To-Peer Electronic Cash System,” 2008. [Online]. Available: www.bitcoin.org/bitcoin.pdf. [Accessed: 12-Sep-2019].

[42] V. Buterin, “A next-generation smart contract and decentralized application platform,” *Etherum White Paper*, 2014. [Online]. Available: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. [Accessed: 16-Feb-2020].

[43] B. Singhal, G. Dhameja, and P. S. Panda, *Beginning Blockchain : A Beginner’s Guide to Building Blockchain Solutions*. Apress, 2018.

[44] F. Masood and A. R. Faridi, “An Overview of Distributed Ledger Technology and its Applications,” *Int. J. Comput. Sci. Eng.*, vol. 6, no. 10, pp. 422–427, 2018.

[45] S. Masood, M. AlyasShahid, M. Sharif, and M. Yasmin, “Comparative Analysis of Peer To Peer Networks,” *Int. J. Adv. Netw. Appl.*, vol. 9, no. 4, pp. 3477–3491, 2018.

[46] D. Meva, “Issues and Challenges with Blockchain A Survey,” *Int. J. Comput. Sci. Eng.*, vol. 6, no. 12, pp. 488–491, 2018.

[47] K. Qin and A. Gervais, “An overview of blockchain scalability, interoperability and sustainability,” *Hochschule Luzern Blockchain Lab*, 2018. [Online]. Available: https://www.eublockchainforum.eu/sites/default/files/research-paper/an_overview_of_blockchain_scalability_interoperability_and_sustainability.pdf. [Accessed: 01-Oct-2020].

[48] A. Altarawneh, T. Herschberg, S. Medury, F. Kandah, and A. Skjellum, “Buterin’s Scalability Trilemma viewed through a State-change-based Classification for Common Consensus Algorithms,” in *10th Annual Computing and Communication Workshop and*

Conference, CCWC, 2020, pp. 727–736.

[49] G. Foroglou and A. L. Tsilidou, "Further applications of the blockchain," in *12th Student Conference on Managerial Science and Technology*, 2015, pp. 4–6.

[50] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *13th International Conference on Service Systems and Service Management*, 2016.

[51] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," *National Institute of Standards and Technology Internal Report 8202*, 2018. [Online]. Available: https://doi.org/10.6028/NIST.IR.8202. [Accessed: 09-Jun-2020].

[52] I. Priyadarshini, "Introduction to Blockchain Technology," in *Cyber Security in Parallel and Distributed Computing*, Scrivener Publishing, 2018, pp. 85–98.

[53] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *IEEE 6th International Congress on Big Data*, 2017, pp. 557–564.

[54] B. K. Mohanta, S. S. Panda, and D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology," in *9th International Conference on Computing, Communication and Networking Technologies*, 2018, pp. 1–4.

[55] R. Houben and A. Snyers, "Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion," 2018.

[56] K. Wüst and A. Gervais, "Do you need a Blockchain?," in *Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018, pp. 45–54.

[57] K. Sultan, U. Ruhi, and R. Lakhani, "Conceptualizing blockchains: Characteristics & applications," in *11th IADIS International Conference Information Systems*, 2018, pp. 49–57.

[58] B. Mackenzie, X. Bellekens, and R. I. Ferguron, "An Assessment of Blockchain Consensus Protocols for the Internet of Things," in *International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, 2018, pp. 183–190.

[59] G. T. Nguyen and K. Kim, "A survey about consensus algorithms used in Blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018.

[60] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in *Proceedings of the Symposium on Operating System Design and Implementation*, 1999, pp. 1–14.

[61] D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm," *White Paper*, 2014. [Online]. Available: https://ripple.com/files/ripple_consensus_whitepaper.pdf. [Accessed: 11-Dec-2019].

[62] P. W. Abreu, M. Aparicio, and C. J. Costa, “Blockchain technology in the auditing environment,” in *13th Iberian Conference on Information Systems and Technologies, CISTI*, 2018, pp. 1–6.

[63] R. Zhang, R. Xue, and L. Liu, “Security and Privacy on Blockchain,” *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–34, 2019.

[64] M. T. Quasim, M. A. Khan, F. Algarni, A. Alharthy, and G. M. M. Alshmrani, “Blockchain Frameworks,” in *Decentralized Internet of Things*, 2020, pp. 75–89.

[65] A. Panwar and V. Bhatnagar, “Distributed ledger technology (DLT): The beginning of a technological revolution for blockchain,” in *2nd International Conference on Data, Engineering and Applications (IDEA)*, 2020, pp. 1–5.

[66] Z. Akhtar, “From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild,” in *International Conference on Electrical, Electronics and Computer Engineering, UPCON*, 2019, pp. 1–6.

[67] Hyperledger, “The Ordering Service.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/orderer/ordering_service.html. [Accessed: 30-Jun-2020].

[68] Hyperledger, “Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus,” in *Hyperledger Architecture*, vol. 1, 2017, pp. 1–15.

[69] Hyperledger, “Transaction Flow.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/txflow.html. [Accessed: 06-May-2020].

[70] Hyperledger, “Smart Contracts and Chaincode.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/smartcontract/smartcontract.html. [Accessed: 30-Jun-2020].

[71] Hyperledger, “Ledger.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/ledger/ledger.html. [Accessed: 30-Jun-2020].

[72] Hyperledger, “Peers.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/peers/peers.html. [Accessed: 30-Jun-2020].

[73] Hyperledger, “Channels.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/master/channels.html. [Accessed: 30-Jun-2020].

[74] Hyperledger, “Gateway.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/developapps/gateway.html. [Accessed: 30-Jun-2020].

[75] Hyperledger, “Connection Profile.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/developapps/connectionprofile.html. [Accessed:

30-Jun-2020].

[76] Y. Manevich, A. Barger, and Y. Tock, “Service Discovery for Hyperledger Fabric,” in *Proceedings of the 12th ACM International Conference on Distributed and Event-Based Systems*, 2018, pp. 226–229.

[77] Hyperledger, “CouchDB as the State Database.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/couchdb_as_state_database.html. [Accessed: 30-Jun-2020].

[78] Hyperledger, “Using CouchDB.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/couchdb_tutorial.html. [Accessed: 09-Dec-2020].

[79] Hyperledger, “Membership Service Providers (MSP).” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/msp.html. [Accessed: 30-Jun-2020].

[80] Hyperledger, “Identity.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/identity/identity.html. [Accessed: 30-Jun-2020].

[81] Hyperledger, “Application.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/developapps/application.html. [Accessed: 30-Jun-2020].

[82] Hyperledger, “Contract names.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/developapps/contractname.html. [Accessed: 30-Jun-2020].

[83] Hyperledger, “Transaction handlers.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/developapps/transactionhandler.html. [Accessed: 30-Jun-2020].

[84] Hyperledger, “Endorsement policies.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/developapps/endorsementpolicies.html. [Accessed: 30-Jun-2020].

[85] O. Choudhury *et al.*, “Enforcing Human Subject Regulations using Blockchain and Smart Contracts,” *Blockchain Healthc. Today*, pp. 1–14, 2018.

[86] N. Gaur, L. Desrosiers, P. Novotny, V. Ramakrishna, A. O’Dowd, and S. Baset, *Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer*. Packt Publishing, 2018.

[87] D. M. Tavares, S. J. Bachega, and G. A. de P. Caurin, “Architecture Proposal For The Use Of QR Code In Supply Chain Management,” *Rev. Científica Eletrónica Eng. Produção*, vol. 12, no. 1, pp. 73–90, 2012.

[88] S. Wang, D. Li, Y. Zhang, and J. Chen, “Smart Contract-Based Product Traceability

System in the Supply Chain Scenario," *IEEE Access*, vol. 7, pp. 115122–115133, 2019.

[89] H. Sheikh, R. M. Azmathullah, and F. Rizwan, "Smart Contract Development , Adoption and Challenges : The Powered Blockchain," *Int. Res. J. Adv. Eng. Sci.*, vol. 4, no. 2, pp. 321–324, 2019.

[90] A. Knecht, "Securing Goods Distribution with Smart Contracts and Sensors," University of Zurich, 2016.

[91] P. Karhula, V. Vallivaara, N. Lehto, V. Pentikäinen, and J. Aikio, "Asset Tracking With Smart Contracts," in *IEEE Wireless Communications and Networking Conference*, 2019.

[92] Y. Wang, M. Singgih, J. Wang, and M. Rit, "Making sense of blockchain technology: How will it transform supply chains?," *Int. J. Prod. Econ.*, vol. 211, pp. 221–236, 2019.

[93] A. Litke, D. Anagnostopoulos, and T. Varvarigou, "Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment," *Logistics*, vol. 3, no. 5, pp. 1–17, 2019.

[94] S. Yahiaoui, F. Fedouaki, and A. Mouchtachi, "How Blockchain Make Better the Supply Chain in the Automotive Industry," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 3, pp. 2912–2917, 2020.

[95] S. E. Chang, Y. C. Chen, and M. F. Lu, "Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process," *Technol. Forecast. Soc. Change*, vol. 144, pp. 1–11, 2019.

[96] S. E. Chang and Y. Chen, "When blockchain meets supply chain: A systematic literature review on current development and potential applications," *IEEE Access*, vol. 8, pp. 62478–62494, 2020.

[97] J. Chang, M. N. Katehakis, B. Melamed, and J. (Junmin) Shi, "Blockchain Design for Supply Chain Management," *SSRN Electron. J.*, pp. 1–35, 2018.

[98] H. Kohad, S. Kumar, and A. Ambhaikar, "Scalability Issues of Blockchain Technology," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 3, pp. 2385–2391, 2020.

[99] C. A. Alexander and L. Wang, "Cybersecurity, Information Assurance, and Big Data Based on Blockchain," in *SoutheastCon*, 2019, pp. 1–7.

[100] J. S. Kim and N. Shin, "The impact of blockchain technology application on supply chain partnership and performance," *Sustainability*, vol. 11, 2019.

[101] X. Guo, Z. Yang, and C. D. Tan, "Emerging Information Technologies Usage: Opportunities and Challenges for Supply Chain Vulnerability," in *IEEE International Conference on Industrial Engineering and Engineering Management*, 2019, pp. 845–849.

[102] HMM, “HMM Completes its First Blockchain Pilot Voyage,” 2017. [Online]. Available: https://www.hmm21.com/cms/company/engn/introduce/prcenter/news/1202833_7540.jsp. [Accessed: 02-Oct-2020].

[103] R. Kamath, “Food Traceability on Blockchain: Walmart’s Pork and Mango Pilots with IBM,” *J. Br. Blockchain Assoc.*, vol. 1, no. 1, pp. 1–12, 2018.

[104] E. Thomasson, “Carrefour says blockchain tracking boosting sales of some products,” *Reuters*, 2019. [Online]. Available: https://www.reuters.com/article/us-carrefour-blockchain/carrefour-says-blockchain-tracking-boosting-sales-of-some-products-idUSKCN1T42A5?mc_cid=a41c15e70c&mc_eid=295ead2126. [Accessed: 28-Oct-2020].

[105] H. Wang, Y. Wang, and Z. Cao, “An Overview of Blockchain Security Analysis,” in *Communications in Computer and Information Science*, vol. 970, Springer, 2018, pp. 55–72.

[106] M. M. Alhassan and A. Adjei-Quaye, “Information Security in an Organization,” *Int. J. Comput.*, vol. 24, no. 1, pp. 100–116, 2017.

[107] U. Abubakar Idris, J. Awwalu, and B. Kamil, “User authentication in securing communication using Digital Certificate and public key infrastructure,” *Int. J. Comput. Trends Technol.*, vol. 37, no. 1, pp. 22–25, 2016.

[108] S. Y. Yan, *Cybercryptography: Applicable cryptography for cyberspace security*. Springer, 2018.

[109] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, Third edit. Springer, 2015.

[110] A. Khalique, K. Singh, and S. Sood, “Implementation of Elliptic Curve Digital Signature Algorithm,” *Int. J. Comput. Appl.*, vol. 2, no. 2, pp. 21–27, 2010.

[111] E. Barker, A. Roginsky, G. Locke, and P. Gallagher, “Transitioning the Use of Cryptographic Algorithms and Key Lengths,” *NIST Special Publication 800-131A Revision 2*, 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf. [Accessed: 14-Sep-2020].

[112] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, “The first collision for full SHA-1,” *Lect. Notes Comput. Sci.*, vol. 10401 LNCS, pp. 570–596, 2017.

[113] IBM, “What is a digital certificate.” [Online]. Available: https://www.ibm.com/support/knowledgecenter/SSB23S_1.1.0.2020/gtps7/s7what.html. [Accessed: 23-Apr-2020].

[114] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” *RFC 5280*, 2008. [Online]. Available: https://tools.ietf.org/html/rfc5280#section-3.1. [Accessed: 01-May-2020].

[115] S. Sejwani and S. Tanwar, “Implementation of X.509 Certificate for Online Applications,” *Int. J. Res. Advent Technol.*, vol. 2, no. 3, pp. 250–254, 2014.

[116] IBM, “Digital Certificate Contents.” [Online]. Available: https://www.ibm.com/support/knowledgecenter/SSB23S_1.1.0.2020/gtps7/s7cont.html. [Accessed: 27-Apr-2020].

[117] D. R. Kuhn, V. C. Hu, W. T. Polk, and S.-J. Chang, “Introduction to Public Key Technology and the Federal PKI Infrastructure,” *NIST Special Publication 800-32*, 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf. [Accessed: 19-Sep-2020].

[118] J. Lintner and F. Kascak, “The Place and Roles of the Certification Authority,” *BIATEC*, vol. 10, no. 5, pp. 24–27, 2002.

[119] IBM, “Digital certificates and certificate authorities.” [Online]. Available: https://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.sec.doc/doc/c0053515.html. [Accessed: 24-Apr-2020].

[120] J. Thangavel, “Digital Signature: Comparative study of its usage in developed and developing countries,” Uppsala University, 2014.

[121] Hyperledger, “Blockchain Network.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/network/network.html. [Accessed: 26-Apr-2020].

[122] N. Shah, *Blockchain for Business with Hyperledger Fabric: A complete guide to enterprise blockchain implementation using Hyperledger Fabric*. 2019.

[123] B. Rodenburg and S. P. Pappas, “Blockchain and Quantum Computing,” *Mitre Technical Report*, 2017. [Online]. Available: https://www.mitre.org/sites/default/files/publications/17-4039-blockchain-and-quantum-computing.pdf. [Accessed: 10-Dec-2020].

[124] A. Akram and P. Bross, “Trust, Privacy and Transparency with Blockchain Technology in Logistics,” in *12th Mediterranean Conference on Information Systems(MCIS)*, 2018.

[125] A. B. Bondi, “Characteristics of scalability and their impact on performance,” in *2nd international workshop on Software and performance*, 2000, pp. 195–203.

[126] M. Scherer, “Performance and Scalability of Blockchain Networks and Smart

Contracts," Umeá University, 2017.

[127] European Accreditation, "Accreditation a tool to support regulators," 2016. [Online]. Available: https://european-accreditation.org/wp-content/uploads/2018/10/accreditation-a-tool-to-support-regulators_1.pdf. [Accessed: 17-Jun-2020].

[128] Instituto Português de Acreditação (IPAC), "A Acreditação." [Online]. Available: http://www.ipac.pt/ipac/funcao.asp. [Accessed: 20-Feb-2020].

[129] E. Accreditation, "Accreditation : Adding Value to Supply Chains," 2020. [Online]. Available: https://european-accreditation.org/wp-content/uploads/2019/05/WAD-2019-brochure.pdf. [Accessed: 17-Jun-2020].

[130] ISO, "Certification & Conformity." [Online]. Available: https://www.iso.org/certification.html. [Accessed: 20-Feb-2020].

[131] G. Santos, B. Costa, and A. Leal, "Motivation and benefits of implementation and certification according ISO 9001 – the Portuguese experience," *Int. J. Eng. Sci. Technol.*, vol. 6, no. 5, pp. 1–12, 2016.

[132] A. Jabłoński and M. Jabłoński, "Trust as a key factor in shaping the social business model of water supply companies," *Sustainability*, vol. 11, no. 20, p. 5805, 2019.

[133] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in *IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering, AIEEE*, 2018, pp. 1–6.

[134] C. C. Agbo and Q. H. Mahmoud, "Comparison of blockchain frameworks for healthcare applications," *Internet Technol. Lett.*, pp. 1–6, 2019.

[135] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda : An Introduction," *White Paper*, 2016. [Online]. Available: https://www.corda.net/content/corda-platform-whitepaper.pdf. [Accessed: 02-Jul-2020].

[136] M. Valenta and P. Sandner, "Comparison of Ethereum, Hyperledger Fabric and Corda," *FSBC Working Paper*, 2017. [Online]. Available: http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf. [Accessed: 22-Jun-2020].

[137] B. Xu, D. Luthra, Z. Cole, and N. Blakely, "EOS: An Architectural, Performance, and Economic Analysis," 2018. [Online]. Available: https://whiteblock.io/wp-content/uploads/2019/07/eos-test-report.pdf. [Accessed: 02-Jul-2020].

[138] I. Grigg, "EOS - An Introduction," 2017. [Online]. Available: https://iang.org/papers/EOS_An_Introduction.pdf. [Accessed: 02-Jul-2020].

[139] F. Armknecht, G. O. Karame, A. Mandal, and F. Youssef, “Ripple: Overview and Outlook Frederik,” in *International Conference on Trust and Trustworthy Computing*, 2015, pp. 163–180.

[140] Hyperledger, “Hyperledger - Technology Projects.” [Online]. Available: https://www.hyperledger.org/use. [Accessed: 06-May-2020].

Appendix 1 – Comparison of blockchain frameworks

Table 4 - Comparison of blockchain frameworks by a different set of features [134]

	Privacy features	**Accessibility**	**Consensus**	**Speed**	**Scalability**	**Transaction cost**	**Incentive**	**Smart Contract**
Bitcoin	No private transactions	Public, access permission not required, more prone to attacks	PoW	7 transactions per second	Low transaction throughput	High	Cryptocurrency required	Not available
Ethereum	Private transactions, experimental zero knowledge proofs	Public, but supports permissioned networks	PoW and PoS	15 transactions per second	Low transactions throughput	High	Cryptocurrency required	Solidity
Hyperledger	Private channels, private transactions, zero knowledge proofs	Permissioned, granular access control, less prone to attacks	Multiple approaches	3000 transactions per second	Higher transaction throughput	Low	No cryptocurrency required	Java, Node.js, Go
Corda	Private transactions [135]	Permissioned and Private use cases [136]	Multiple approaches [136]	Billions of transactions daily [135]	Higher transaction throughput [135]	Low [135]	No cryptocurrency required [135]	Kotlin, Java [136]
EOS	Private transactions [137]	Both Public and permissioned use cases [64]	DPoS [64], [137]	1200 transactions per second [64]	Higher transactions throughput [64]	High [138]	Cryptocurrency required [138]	C++ [137]

Ripple (XRP)	No private transactions, but user identity is protected [139]	Public [139]	Ripple Protocol Consensus Algorithm (RPCA) [64]	1000 transactions per second [64]	Higher transactions throughput [64]	Low [64]	Cryptocurrency required [64]	Not available

Appendix 2 – Hyperledger Frameworks

Table 5 - Summary of Hyperledger frameworks with a description of its usage and applications [140]

Framework	Purpose	Use Cases
HYPERLEDGER INDY	In case you need to develop a set of decentralised identity and artefacts that are independent in any particular ledger.	Digital Documents, Secure Password-less Authentication (SPA), Employment Verification.
HYPERLEDGER FABRIC	It can conduct confidential transactions without the need for a central authority and allows components such as consensus and membership to be applied and run immediately.	B2B Contract, Manufacturing Supply Chain, Asset Depository.
HYPERLEDGER IROHA	This framework is more applied to mobile application development for Android and iOS, providing development in C++. However, it can be used for other types of blockchain developments.	Financial Applications, Insurance, Identity Management, Certificates in Education and Healthcare, Supply Chain
HYPERLEDGER SAWTOOTH	It provides high scalability on blockchain solutions with the option to change the consensus mechanism at any time (default is Proof of Elapsed Time (PoET)).	Seafood supply chain traceability, Asset Settlement, Digital Asset Exchange
HYPERLEDGER BURROW	Designed to be a permissionable smart contract machine that provides a smart contract application engine with a gateway, a consensus engine, and a blockchain application interface.	Smart Contracts development
HYPERLEDGER BESU	Ethereum client designed for both public and private permissioned blockchains.	Ether mining, Smart Contract development, Decentralised application development

Appendix 3 – Hyperledger Framework Tools and Libraries

Table 6 – Summary of Hyperledger framework tools [140]

Tools	Purpose
HYPERLEDGER AVALON	It a ledger independent implementation to enable the secure movement of blockchain processing off the main chain to dedicated computing resources.
HYPERLEDGER CALIPER	This tool allows the user to measure the blockchain implementation's performance with a set of predefined use cases.
HYPERLEDGER CELLO	It provides a toolkit that allows businesses to deploy Blockchain-as-a-Service.
HYPERLEDGER EXPLORER	It provides a tool for visualising blockchain operations, allowing anyone to explore the distributed ledger without compromising privacy.

Table 7 – Summary of Hyperledger framework libraries [140]

Libraries	Purpose
HYPERLEDGER ARIES	Focused on creating, transmitting, and storing verifiable digital credentials providing a shared, reusable, and interoperable tool kit.
HYPERLEDGER QUILT	Java implementation that enables payments across any payment network (implementation of payment logic).
HYPERLEDGER TRANSACT	It provides a standard interface for executing smart contracts that is separate from the distributed ledger implementation.
HYPERLEDGER URSA	It is a shared cryptographic library that avoids duplicating other cryptographic, increasing the security of the process.