Blockchain and IoT integrated approach for a trusted and secured process to manage the transportation of dangerous goods

Adnan Imeri
Luxembourg Institute of Science and Technology
University of Evry Val d'Essonne - Paris Saclay University
5, Avenue des Hauts-Fourneaux
L-4362 Esch-sur-Alzette, Luxembourg
+352 275 888 4908
adnan.imeri@list.lu

Nazim Agoulmine
University of Evry Val d'Essonne - Paris Saclay University
23, Boulevard de France
91034 – Èvry, France
+33 1 64 85 34 74
nazim.agoulmine@univ-evry.fr

Djamel Khadraoui
Luxembourg Institute of Science and Technology
5, Avenue des Hauts-Fourneaux
L-4362 Esch-sur-Alzette, Luxembourg
+352 275 888 2286
djamel.khadraoui@list.lu

ABSTRACT

The domain of transport and supply chain of goods is today strongly impacted by the digital technologies similarly to the logistic enterprises providing them. Due to their critical nature. Not only these services are required to be correct but a traceability of the end-to-end process of transportation has to be provided. The influence of cutting edge technologies such as the Internet of Things (IoT) and blockchain enables a new level of transparency and real-time verification of the process of transport. The impact of the IoT attributes to improving the quality of services in several domains so it does in transportation. The capacity of IoT devices to generate real-time information is essential to monitor process and other daily activities in the domain of transport. In the area of dangerous goods transportation, this is even more critical since stakeholders of the supply chain need to share and exchange information in a trustful manner. Sensitive information about the transportation process should verified before shared as well as protected from any unauthorized access and changes. For a trusted and transparent process of transport, the data captured by IoT devices to monitor the transportation of goods, should remain consistent, reliable and with proved integrity properties. In this paper, we present a research that highlights how the potential of the blockchain and IoT technologies can be efficiently integrated in order to secure information exchange in an end-to-end process of transport of dangerous goods (TDG). Firstly, we examine the process of TDG from the perspective of stakeholder collaboration i.e., information flow. Secondly, we propose a model that supports an end-to-end TDG based on the regulatory framework. Third, we integrate blockchain and IoT technologies for securing information sharing during the process of TDG. Hence, we show how the transparent provides the righ level of abstractions to the process of TDG. A proof of concept applying our approach has been developed and tested.

CCS Concepts

•**Information systems** → **Blockchain Technology;** • **Computing methodologies** → **Secure and smart computer simulations;** •**Networks** → *Peer-to-peer network;*

Keywords

Blockchain, IoT, Transport, Traceability, Transparency, Dangerous Goods

1. INTRODUCTION

In today's Logistics and Supply Chain activities, there is an enormous need for an advanced organization in order to allow business community to efficiently respond to retailers and other involved parties. Supply Chain is a complex process in the sense that, the collaboration between stakeholders requires an accurate and on-time exchange of reliable information. In recent years, we observed many changes in the technological domains, which have transformed the traditional ways of performing business processes. New emerging technologies such as the Internet of Things (IoT) and more recently the blockchain, have enabled the transformation of these business process. The IoT is the technology by which passive objects become connected objects with the help of integrated communication and processing devices that are able to collect and send specific information about the state of the object and its environment to other objects or back-end applications [13]. These devices empowered the emergence of numerous technological concepts, such as "Smart Manufacturing", "Smart City", "Smart Home", "Smart Offices", etc. [9] [44]. The usability of IoT technology, boosted by the

huge progress in electronics and radio communications technologies is allowing a much better management of enterprise activities, by allowing them to monitor the active processes they are performing. The new emerging concepts such as Industry 4.0, eventually intends to transform the way of managing manufacturing, management of logistics and transport [23]. This is also true in the area of urban activities where there is an increasing offer of services for daily activities and particularly activities related to transport. The use of IoT devices in this domain has already shown a huge potential to better managing these services, enhancing public information, monitoring transport activity, increasing safety and reducing accidents. Nevertheless, besides the benefits form IoT technology, main concerns remain regarding the privacy and security of exchanged information from IoT devices [41] [63] [7].
In this paper, we investigate the potential of blockchain technology for securing the information generated by IoT devices during the monitoring of the process of TDG. In particular, we address use case of cross-border TDG transportation between Germany, Luxembourg, and Belgium which have each their own regulations laws regarding this type of goods.

1.1 Dangerous Goods (DG)

First of all, we will introduce what are DG (Dangerous goods). DG are defined as substances that expose a high risk for humans, living organisms, environment and property. The evaluation of risk exposed by TDG is a challenging task as presented by scientific literature [14] [10] [42] [60]. DG are classified in categories such as "Explosives", "Gases","Flammable Liquid","Flammable solids", "Oxidizing substances and organic peroxides", "Toxic and infectious substances", "Radioactive material", "Corrosive substances", "Miscellaneous dangerous substances and articles" [2]. DG present a high risk during their transportation. Indeed, the challenge originates from the fact that any accident involving DG may have catastrophic consequences [58]. The percentage of TDG has been evaluated [56] and it appears that an important share of transportation statistics is related to TDG [18]. The governance of this process is subject of predefined national and international regulation which determine a sustainable process for the transportation of such a specific goods. Actually, these regulations intend to minimize the risk by standardizing the process of TDG [29]. An international regulatory document presented in [2] elaborates the procedures for packing, labeling, loading, transporting, unloading and warehousing of dangerous goods [28].

1.2 Legacy: The decision support systems as a management tool for TDG

The risk involved in TDG is strongly related to the nature of the goods. To evaluate the risk estimation and manage the process of TDG, decision support systems (DSS) as a computer-based solution have been developed. The basic idea behind DSS is to help stakeholders to measure the risk for TDG, save time on critical decision, monitor the process of transport [56], decrease the negative impact in case of accidents with dangerous goods [66], scheduling, planning and resource allocation [45] [20] [56] [45]. In general, the architecture of these systems is a compound of other sub systems: embedded systems in the objects to transport "Sensors", "GPS tracker", "RFID", "GIS (Geographic Information System) to locate the moving objects", and other related ones. all these systems are integrated with the DSS, providing it with specific information about the state of the process of TDG. The risk analysis, monitoring of the process of TDG and other related tasks are depended on the current state of the process of TDG thanks to IoT devices. For example, in case of an accident in the process of TDG, the IoT devices (GPS tracker, Sensors, RFID, Raspberry Pi) will collect and transmit information related to the accident in real-time to the DSS. These information are stored by DSS in a local database of the stakeholders and analyzed. Obviously, this raises several **concerns** in term of *the security of the information, its reliability, and trust issues regarding the sharing of theses information about the TDG process between stakeholders themselves and with the authorities of the different traversed countries* 1.3 [28]. We propose in this paper a new approach to manage the information related to the process of TDG and how this information is stored, managed and shared to achieve a higher level of security and transparency. It is worth noting that the proposed approach presented doesn't prevent any enterprise (stakeholder) to continue to use their own application (e.g. DSS) [28].

1.3 Specific challenges in cross-border TDG

As stated before, the TDG involves several challenges that are closely related to the categories of goods that are transported. Accidents with dangerous goods transportation may expose a high risk to human population, private and public properties, and environment as it usually pass through urban and non urban areas. For this reason, the process of TDG is strongly governed by specific rules and regulations, i.e., "regulatory framework", that are provided by competent authorities of regulation, representative of countries. Particularly, the process of transport and management of DG is governed by local and international competent authorities, which impose these regulations. This process should comply with regulations that are defined for a different mode of transport, such as ADR [57] or European regulation "No. 1003/2006" [47] for route transport of DG, RID [12] for rail transport of DG, IATA for air transport etc. The regulatory framework requires strict compliance of the process at its workflow [29]. As the most suitable way for TDG is by using roads (due to the low costs, compared to other modes of transport), the shipping (transport) organization usually select the route that minimizes its costs. This usually exposes problems because these routes passes through populated areas [56]. In addition, in the context of globalization, TDG to some specific destinations at most of the case, requires to cross-border, as presented in Figure 1, of several countries and therefore the process is automatically extended to the international level.

Among other important challenges of TDG in a local or international contexts, we identified two main challenges that are *a) Organizational aspects of the process of TDG* and *b) Information security aspect.*

1.3.1 Organizational aspects of the process of TDG

Regarding the organisational aspects of process of TDG [29] [30], we identify different important aspects to address such as:

- Administration of the process such as packaging, labeling, data entry, and loading DG;

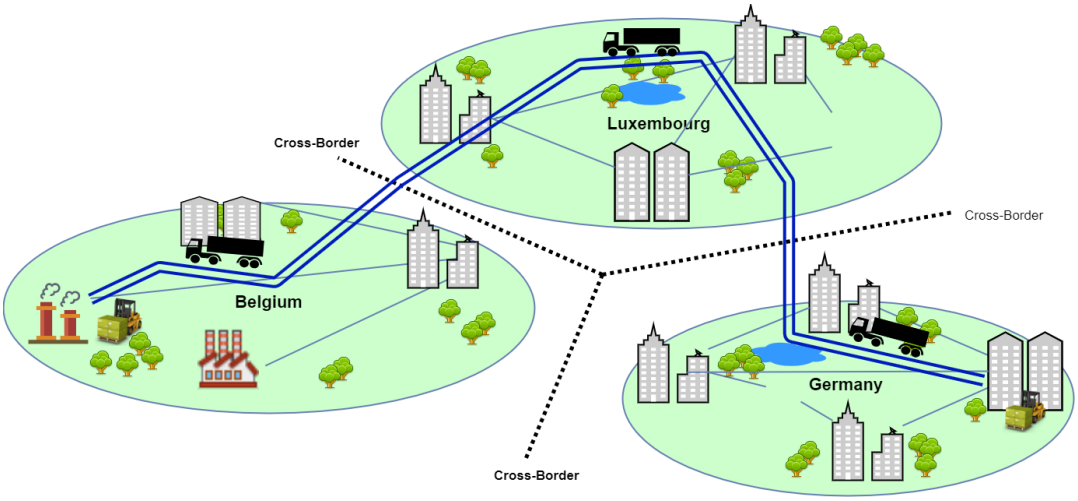

Figure 1: The transport map for DG in cross-border context.

- Manual and paperwork;
- Monitoring the process of TDG;
- Emergency responses.

1.3.2 The concern of security of information in TDG

The use of IoT devices significantly improves the quality of the process for TDG since it allows its monitoring, traceability as well as triggering appropriate actions in case of abnormal situations, i.e., accidents or other distribution on the process of TDG. The concern with the use of IoT devices is the security of the exchange of information and the trust in these information [41] [63] [7]. The current DSS systems are mainly designed as centralized system hosted in private data centre or in the cloud computing [7], they remain the only point of reference for data exchange. IoT frameworks such as Amazon Web Services (AWS) [1], Salesforce [40] and any many others [1], do not provide any formal way to verify the reliability and integrity of the stored data. Mainly, such frameworks use their cloud storage to store client data.

In the context of TDG, where "nuclear materials or nuclear waste, infectious materials e.g., medical or biological waste" might be among transporting substance, the security, confidentiality, auditing, and monitoring of processes in real-time are extremely important and it is important to be able to responsd to the following question *"Why do we need to secure the information transmitted by IoT devices ?"*.

The process of TDG is essentially an international activity, that crosses borders of countries whose stakeholders are involved. For this process, a different international and local regulatory frameworks are applied, and usually, the stakeholders involved are the ones with big market reputation [29]. In case of any accident or irregular process in TDG, the secured information captured from the IoT devices are currently not immutable, and this allows big market players to impact the process by possibly tampering the information. The design of current technologies that support the storage of IoT data does not guarantee this level of data integrity. To ensuring the objectives of such a system, one should answer to the following questions:

- How to remove the single point of failure problem of existing systems?

- How to efficiently collect the status of the transported DG using IoT devices?

- How to store and secure the information generated by IoT devices?)

- How to secure the information generated by stakeholders, e.g., exchange of documents by stakeholders of DG?

- How to audit all the operations related to TDG process to completion?

To answering properly these questions, we propose to combine IoT and blockchain technologies to bring the system the required functionalities to transparently and securely manage the process of TDG. The IoT technologies brings to the system the required digital transformation to automate the interaction with the physical aspects of the process while the blockchain brings to the system the required level of security and trust to sharing information.

The rest of the paper is organized as follows. Section 2 introduces and extensive study of the properties of the blockchain and IoT with a focus on the selected blockchain framework to develop later our proof of concept (PoC). In section 3, a collection of related work studies is presented. Our proposal of a trustful and secure process to manage TDG is presented in section 4. In the following section 5, we present the implementation of the PoC. Results of the performed tests in the PoC are presented in section 6. Finally, a conclusion and some future works are presented in section 7.

2. OVERVIEW OF BLOCKCHAIN AND IOT

This section introduces first the main characteristics of the main technologies used in this research namely blockchain technology and IoT technology. It then present the selected blockchain framework as well as its main features and characteristics. Finally, the section presents some examples of IoT devices and their application towards TDG.

2.1 Blockchain Technology

[1]There are many other IoT frameworks such as Microsoft Azure, IBM Watson IoT, Intel IoT, etc., see https://www.educba.com/iot-framework/

"A Blockchain is a distributed decentralized database between multiple distributed parties that allows to store immutable transaction data gathered into a chain of blocks. These data are generated by transactions executed by user of the blockchain. The 'block' is a data structure composed of several fields. A *timestamp*, stores the time the block was created (appended into the blockchain). A *previous hash* is the hash value of the previous block, e.g. the block *n* contains the hash from the header of block *n-1*. A *Nonce* is the value generated by the consensus algorithm, e.g., Proof of Work [65] [62]. Transaction Root is the root of all transactions received from the nodes in the network for a determined timestamp. These transactions are organized in a tree by using the so called Merkle Tree [54].

- *Decentralized*: Blockchain technology relies on a peer-to-peer mode of communication. It does not have any central authority for storing and retrieving data [65] [62].
- *Consensus Algorithm*: A consensus, in the blockchain technology, refers to the agreement of nodes in shared content to store in the blockchain. Different consensus algorithms are used, such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine fault tolerance (PBFT), etc.[54] [65].
- *Data Security*: The data stored in the blockchain are cryptographically checked. The blockchain technology uses digital signatures (public key cryptography) for signing and verifying transactions [65] [62] [61] [43].
- *Data Immutability*: The data recorded on blockchain are cryptographically checked and distributed over all nodes in the network. For changing a transaction in the blockchain, the user should change all transactions at the same time in all nodes in the network which is almost impossible. Furthermore, this is impossible since the consensus algorithm compares the hash root of the transaction and denies these changes. Therefore, the transaction recorded in blockchain cannot be altered or deleted [65] [62] [61] [43].
- *Auditability*: The timestamp of the validation transaction enables any user to trace the previous transaction executed by a specific user. This is possible by having access in the blockchain to any node in the network [62].
- *Smart Contracts (SC)*: A computer code deployed on the blockchain for performing specific tasks after some predefined conditions are fulfilled. SC can implement and fulfill the condition expressed in the business process. They might transfer an asset, execute other SC, interact with other external services (off-chain) [65] [62].
- *Process automation*: The usability of the *smart contracts* and their ability for self-execution when a specific condition is fulfilled, present one of the main technical features for the process automation.
- *Interoperability:* The core component of blockchain technology enables many parties to access blockchain under pre-defined conditions.
- *Low-cost maintenance*: Blockchain technology does not use any central authority for the exchanging of messages and validation of transactions. This enables low-cost operations when using blockchain since there is no need to develop server infrastructures for the validation of transactions. This is in contrast to traditional systems, which use central servers for messages exchange and validation, and which usually have high database maintenance costs (upgrade, backup) [65] [62].
- *Sustainability*: If several nodes fail or are disconnected, the blockchain is still available and works properly on the remaining nodes. When the "offline" nodes come back into "online" mode, they receive the latest state of the ledger [65] [62] [54] [61] [43].
- *Public blockchain:* In the public blockchain, access is without permission, and is considered fully decentralized. Any end user can join the network, execute the transaction or explore the block of the transaction conducted by other end users [65] [62].
- *Consortium blockchain:* This type of blockchain is mainly used by organizations, and is considered partially decentralized. For example, if there are 15 organizations that host this type of blockchain, a consensus may be achieved if 10 organizations sign the transaction. Further, access rights are granted in specific cases.
- *Private blockchain or permissioned blockchain:* In private mode, different levels of access and read and write permissions are presented. To access the private blockchain network, permission must be granted [65] [62].
- *Data management:* On-Chain vs Off-Chain. In the context of data management, the common practice in blockchain is to sort the raw data off-chain, and store the meta-data related to transactions, e.g., hashes of the transactions, on-chain [43] [61].

Since its invention, blockchain technology has influenced many industries. The technical specifications of the blockchain are the considered backbone for solving specific problem related to several target domains of application including Supply Chain Management [31]." [27]

2.2 Selection of the right blockchain framework

Among the main challenges when designing a blockchain-based solution is the selection of the right blockchain framework. Different parameters need to be taken into account before starting designing a blockchain-based solution. These parameters might be related to the performance of blockchain technology or to its governance management (i.e., access rights, privacy, and confidentiality).

For the TDG use case, we also consider these parameters. We propose the conceptual approach presented in 4. In this proposal, we aim to use IoT devices for capture data related to the goods transportation and and to validate transaction (this latter requires a certain level of performance). Furthermore, for a governance management of the stakeholders involved in the TDG, we aim to use the blockchain to support the security level required by the process of TDG in

such a way to satisfy the "legal contract" or "business agreements".

To select the most appropriate blockchain framework, we have performed several analyses of existing blockchain frameworks against the required properties from our use case. As a result, we found out that public blockchains such as Bitcoin or Ethereum are not appropriate solutions since the privacy and confidentiality issues are major issues of these frameworks [65]. Regarding the TDG use case, it is required that all stakeholders participating in the consortium need to be formally identified (certified identity). Any stakeholder that is requiring to be part of the consortium, initially, access should be required to the consortium, and they will be part of this consortium, only if this access is granted. Granting the access means for the stakeholder an opportunity to exchange transactions with other members of the consortium based on privacy defined. Authorities of each participating country may manage this consortium (e.g., Ministry of Environment, or Justice, depending on the type of DG to transport)

The blockchain type we have identified to satisfy the requirements for this use case is the "consortium blockchain". It allows forming a consortium of stakeholders with additional properties on privacy and confidentiality. As a result, Hyperledger Fabric (HL) has been selected as the blockchain framework to develop our solution. This framework is presented in the following section.

2.3 Hyperledger Fabric

Hyperledger[2] Fabric (HF) is a blockchain-based framework that provides the technological features for developing a consortium or private blockchain. HF is an open-source framework implemented in GoLang programming language, and it is supported by several tools such as Hyperledger Explorer, and also Hyperledger Composer[3] which simplifies the business logic over HF. HF has a modular and configurable architecture that allows users to adopt blockchain technology for their use case. Furthermore, it allows writing of smart contracts (SC) in general-purpose programming languages, e.g., Go, Java and Node.js and Python, which is beyond domain-specific language, provided by other SC enable blockchain platforms [4] [25] [32].

2.3.1 *The main components of Hyperledger Fabric (HF)*

The HF blockchain network is composed of nodes that are connected together in a peer-to-peer fashion. HF has different types of nodes, such as *Peer, Orderer, Certification Authority and Client.*

- **Peer** node (peers), is one of the HF blockchain node. It contains the ledger (blockchain) and there are hosted SC. Peers can contain one or more ledgers [4].
- **Orderer** node, its role is on ensuring the consensus of the HF. Basically, the role of the order is to keep the peer's ledgers consistent [4] [25] [32].
- **Certification Authority (CA)** nodes ensure identity delivery via digital certificates, typically required by each organization to enroll new members [4] [25] [32].
- **Client** nodes can connect to and interact with peers deployed over the network [4] [25] [32].

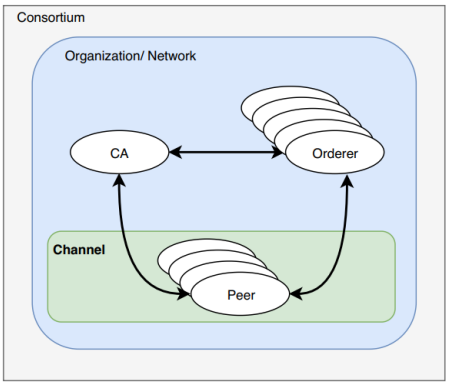

Figure 2: The overview of the key concepts of HF.

The HF can be managed by several organizations that constitute a consortium. Thus, each organization is responsible to manage its own nodes, and it is mandatory to have at least one Certification Authority (CA) node Orderer node. Figure 2, shows basically the interaction between HF components (Peer, Ordered, CA) in an organized consortium.

2.3.2 *Channels: Private Sub-Networks*

Channels enable a private communication link between peers. That is a way to separate the network into a private sub-network, composed of a subset of members/peers. Communications onto each channel are ciphered and controlled by Orderer nodes and CA nodes. Because the network is private and permissioned every action applied by organizations over the network must be done through a specific channel with the right permissions and credentials. It is mandatory that a SC be installed over a channel, which leads to install the contract on each peer belonging to that channel [4] [25].

2.3.3 *Performance analysis for HF*

From a performance point of view, Blockchain technology is not the most suitable technology, especially when public blockchains e.g., Ethereum or Bitcoin, are applied for a particular use case. There are several gaps in transaction throughput (number of transactions per second (tps)) and latency on confirming a new block on the blockchain. Contrary to the public blockchains, the private and consortium blockchains are much better in terms of performance. HF allows us to add some basic configuration such as choosing the block size (or block time), and that impacts the transaction throughput and latency [53]. For example, depending on the block size (e.g., 2 MB), Local Area Network (LAN) properties, and storage (SSD vs HDD), HF has high transaction throughput is in thousand (approx. 3000 tps) with latency on milliseconds. This makes HL a strong technology choice for developing our approach.

[2]Hyperledger is a consortium of different research and development communities which are gathered, (under the Linux Foundations) to contribute to many projects related to blockchain. Hyperledger provides open-source blockchain frameworks, tools, documentation, practical experiments, with a specific focus on business-oriented use cases [26].

[3]Hyperledger Composer has been deprecated. A similar-intention tool to Hyperledger Composer called Hyperledger Convector is currently provided

2.4 Internet of Things

In today's trendy technologies the Internet of Things (IoT) is recognized to be one the novel technology that has the main impact on the transformation of business process. Adding ability to physical objects to communicate with business applications, the IoT technology has enhanced different vertical domains by improving the quality of service (QoS). The Internet of Things (IoT) presents a set of devices that are able to collect, exchange and share information. The IoT devices enable sensing data from objects and their context, performing computing, establishing communication between devices and data transmission channels and actuation [59]. Mainly, the current IoT systems are composed of three different layers, as presented in Figure 3. The IoT devices part (sensing) which is composed of different devices that are responsible for gathering (sensing, measuring, identifying) specific data, for a given use case. The network layer enables the transmission of data to the application layer. The application layer stores the data captured by the IoT sensing layer, also transmitting instruction for the sensing layer [49].

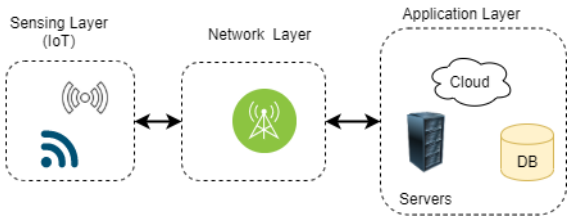

Figure 3: The overview of IoT systems. Inspired by [49].

In the context of our approach, we propose to use sensors for capturing the environment data, such as humidity, temperature, and field disturbance sensors. The RFID is used for object identification purposes (e.g., identify trucks and other objects inside trucks). GPS tracker devices monitor the location of trucks. For performing small computing calculation and storage, we strive to use Raspberry Pi. Smartphones (or tablets) are used for monitoring of the process and adding information as required by the process.

There are already well know concerns regarding IoT systems such as privacy and security of information generated by IoT devices [41] [63] [7]. In this research, we intend to show the potential of blockchain technology to securing the information generated by IoT devices during the monitoring of the TDG process. The convergence of these two technologies is presented in the following section.

3. INTEGRATION OF BLOCKCHAIN AND IOT

Several approaches use blockchain as immutable logs for the IoT data, and some others propose specific use case where both blockchain and IoT technologies are used. There exist also several surveys on blockchain integration with IoT [46] [11] [35] [19]. The research presented in [46] [21] shows challenges and opportunities on the integration of blockchain and IoT. The challenges are highlighted for the use cases that use public blockchain e.g., Bitcoin or Ethereum as an immutable log of IoT data, in the sense that these networks are not scalable. Furthermore, in such use cases, it might not be reliable if the nodes i.e., "miners" do not join the network. On the other hand, the private blockchain solves the issues of scalability and privacy, but the decentralization aspects decrease.

While the benefits are encountered in designing and developing solutions that incorporate data privacy, data integrity and designing systems that will be able to manage the identity of devices in a tamper-proof manner [46] [51]. The research from [24] proposes a way to manage IoT devices by using Ethereum blockchain. The defined policy (turn the device on/off in certain conditions, e.g., when the temperature is reaching certain value) and temperature updates are posted into the Ethereum network with the help of a smartphone and Raspberry Pi. Other devices are retrieving certain values from this policy, in a periodic way. The solution uses also SC for updating the temperature and adding policies about devices. In [36], the IoT devices are managed and monitored using blockchain and SC for managing the configuration files of the IoT devices. In this approach, the certified network administrators are allowed to add new or update configurations of IoT devices and then put it on the blockchain, which further raises an event to notify the targeted IoT devices. Further, the targeted IoT devices decipher the configuration using their private keys and add them to their configuration files. Authors in [52] advocate that blockchain technology has attractive properties for decentralizing the IoT, thus proposing an architecture that is based on the combination centralized-decentralized approach. The basic idea is to use intermediate servers between IoT devices and blockchain framework. The SCs are used to maintain the authentication, rules, and communication between involved parties [52].

In [38], four architectural styles for blockchain and IoT are presented namely "Fully Centralized", "Pseudo Distributed Thing", "Distributed Things", "Fully Distributed". The first two architecture styles use blockchain for recoding payment transactions and hosting blockchain node on cloud respectively, thus not benefiting entirely from the blockchain. On contrary to them, they remain architecture styles that benefit from blockchain technological abilities, consequently being robust and with data integration properties [38].

IOTA[4] based on the Tangle ledger uses a Directed Acyclic Graph (DAG) to add a transaction on the ledger. For adding a new transaction in the Tangle, nodes should select two previous transactions to be validated, then a small computing power is needed to add a new transaction. This way of adding a new transaction, and without the mining process improves the scalability while as many nodes joining the network, the transaction validation is faster [33] [6] [48].

The research in [64] highlights the "tendermint" consensus [55] suitable for combining IoT and blockchain. In [34] a cross-chain solution integrates different blockchain frameworks for managing the IoT data securely and efficiently. The idea behind this research is a decentralized access model based on a consortium blockchain that acts as a control system [34]. It uses other blockchain frameworks (several subnetworks), such as IOTA for IoT data management. The role of IOTA (Tangle) in this approach is to provide an immutable log for IoT devices, while the consortium blockchain role is to record and control any access to these data coming

[4]IOTA is known as "distributed ledger" for IoT [50] [22]

from IoT devices through blockchain frameworks, i.e., subtangle (IOTA) [34]. In Enigma [67], the privately shared data are stored on the "modified distributed hashtables". In this approach, a blockchain is also used for managing the access control, identities, and servers in an immutable way. This approach proposes that the public part of the data be stored on the blockchain while the private part be stored off-chain (on Enigma platform). This solution provides a certain level of scalability and is a good candidate to be used with IoT [5]. There are considered limitations, such as decentralized *off-chain distributed hash-tables* (DHT) [67]. The research from [8] showed that blockchain and smart contracts in combination with IoT have a significant impact on the automation of processes. In [39], a blockchain is used to secure a Long-Range wide-area network (LoRaWAN) IoT. The authors considered that since LoRaWAN for IoT is usually operated by private organisations, their approach proposes to store the data in the network servers before transferring them to back-end application servers. However, the approach is limited since it does not consider the throughput issues and latency. [49], highlights more explicitly the security risks in a use case of "autonomous vehicles" i.e., the internet of vehicles, and propose to solve these issues implementing three layers of IoT are presented: "perception layer", "network layer" and "application layer". For overcoming the security risk for IoT systems, authors propose a blockchain-based solution with the focus on the traceability of the IoT devices. This traceability is applied to the interactions of the IoT devices with the network (mobility) and the interactions of the IoT devices with the cloud (data) [49].

The research in [16] [17] proposes an optimized solution for a smart home use case with a specific focus on IoT security and privacy . They propose to deploy a "miner" in each home to manage the communication with the outside world. The miner manages all devices that are deployed inside the home.

To go beyond existing approaches, firstly, we propose in our approach a solution that avoids any dependency to any blockchain framework that needs a cryptocurrency incentive for their maintenance. Secondly, we propose a novel approach to performing secure transactions by using certified IoT devices and lightweight nodes as transaction validation. Thirdly, we propose a data flow model that is slightly different from existing approaches. Indeed, we propose to aggregate data on the lightweight nodes before sending them to the blockchain. Fourthly, we aim to overcome the manufacturer's (e.g., IoT solution providers) impact on designing and developing IoT based system. Fifthly, we propose to use the Blockchain as a full application layer in an IoT system. Finally, we propose to use open-source blockchains such as Hyperledger Fabric, which is scalable, support IoT data management, privacy, and confidentiality.

4. PROPOSED SOLUTION

4.1 Analyzing the end-to-end process of TDG

Initially, we examine the interaction model of the process of TDG from perspective of stakeholder's interactions. As we mentioned before the process of TDG is entirely governed by the regulatory framework and managed by the competent authorities of the representative countries. Therefore, in the context of the considered use case of TDG across several european countries, the process is fully based on the regulatory directives i.e., ADR [57] and European regulation "No. 1003/2006" [47].

The actors of the process of the TDG are a set of stakeholders that composes the Supply Chain of DG. More precisely, the Supply Chain of DG is composed of the following actors: "DG Provider", "DG Receiver", "Transporter", "Warehouses", " Local Authorities" and "Emergency Response Authorities" [30].

We have specified a business process model of this process [5] as presented in Figure 4. The model specifies the process flow and the interactions between the stakeholder during the entire life cycle of the TDG in a context of cross-border [6]. The "DG Provider" is responsible for managing DG, physical preparation, and to provide data entry regarding DG. At this stage, when the transport of DG is scheduled, the "Local Authorities" and "DG Receiver" should be notified. The "Transporter" follows the next steps and continues for TDG as they are scheduled. Depending on the long-distance between the departure site and the arrival site, intermediate stops might be scheduled and in any case, the necessary information should be transmitted to the stakeholders that are responsible for the monitoring this process. The "DG Receiver" is always informed whenever the DG crosses the country border to take the necessary precautions for preparing and properly hosting the received DG. Also, for safety reasons, the "Local Authorities" in the destination (or transit) country are informed about the arrival of DG in order to take all safety precautions to avoid accidents. When receiving the DG, the "DG Receiver" confirms the reception of DG. Further, the treatment of the DG is performed by "DG Receiver" following the legal procedures designated from the regulatory framework "No. 1003/2006" [47] [47].

4.2 3-layers conceptual architecture

The approach we propose a smart, secured and trusted process of TDG, aims to adapt the process of managing the TDG based on available information about security, integrity, and availability i.e., accessibility. We propose a new approach to exchange (share), manage and store information between stakeholders using blockchain technology. The core advancement behind our proposed solution is the decentralization mechanism, supported by a combination of blockchain technology and IoT devices. The proposed solution aims to respond efficiently to any security concerns in the TDG as presented in section 1.3.2. The Figure 5, shows our conceptual architecture for this smart, secured and trusted environment to support the process of TDG. This approach is an extension of our previous research works presented in [28].

The proposed conceptual architecture is composed of three layers, organized in a top-down manner as follows:

- *L3: IoT devices layer*

  This layer is composed of IoT devices that are deployed in the target geographic area (e.g., for object identifica-

[5]This model is specified using a standard for Business Process Model And Notation (BPMN) 2.0, https://www.omg.org/spec/BPMN/2.0/About-BPMN/ .

[6]In this Figure, for simplification, we only present the BPM involving TDG trough two countries (Luxembourg-Germany). The model has been also extended to the multi-country scenario.

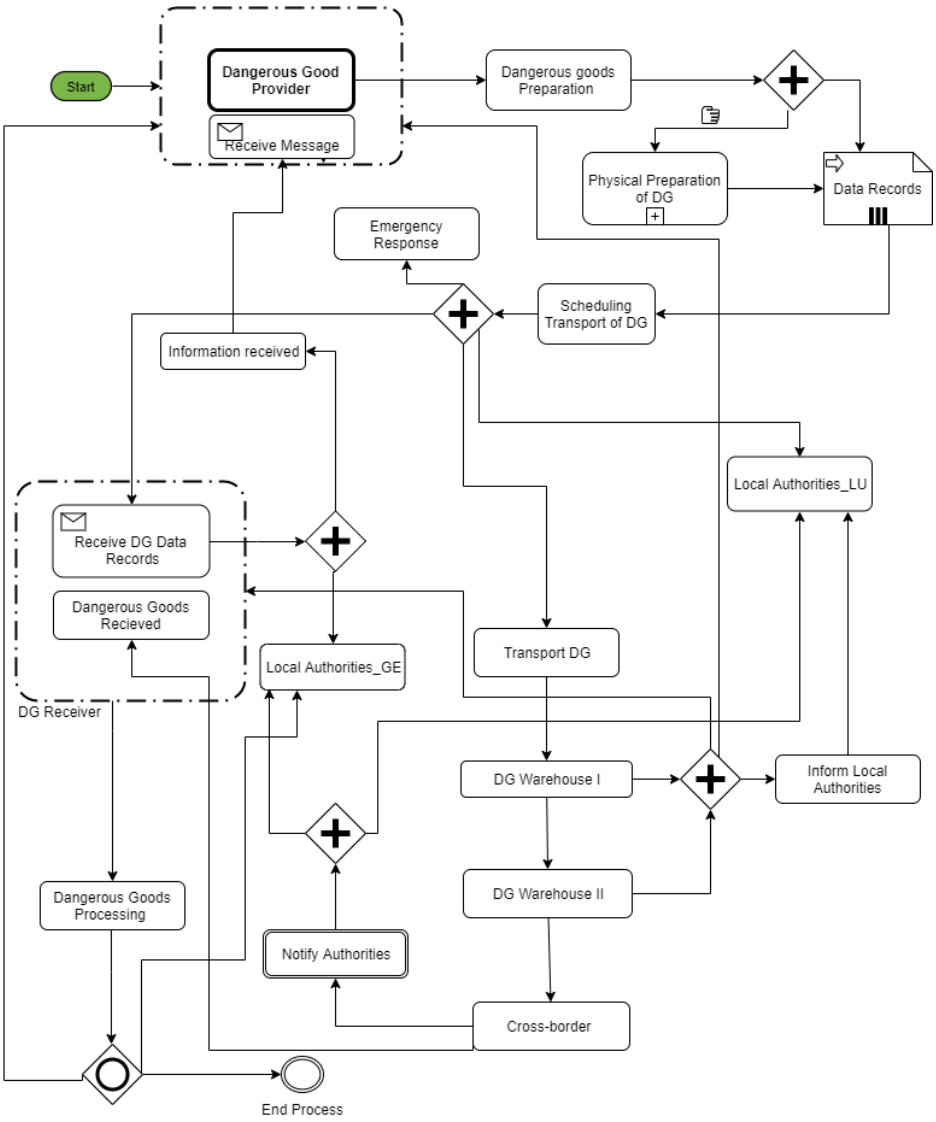

Figure 4: An end to end BPMN model for the process for TDG.

tion during mobility) and embark in the transport facilities (e.g., sensors and GPS trackers into the trucks, etc.). These IoT devices are not intended necessarily to have powerful processing capabilities

All these IoT devices are identified before deployment (using the CA authority of HF, which releases public key for IoT devices) and authenticated. These IoT devices are registered on the blockchain (L1) using their hardware identification. This registration allows storing the IoT devices *public key* on the blockchain, for their identification [24]. This allows to avoid the blockchain to receive information from an unauthorized IoT device and therefore securing it from potential attacks.

Regarding the communication protocol between IoT devices, we recommend using peer-to-peer communication. Indeed, indeed while this is optional, it might be chosen by the system designers to improve the performances of the system (e.g., extending communication range using P2P IoT communication protocol)[7].

- *L2: Blockchain Lightweight Node*

  The second layer is composed of IoT devices that have higher capabilities to processing data (transactions) that are captured by IoT devices (hosted at L1). Mainly these devices are the Raspberry Pi, which have the necessary storage, processing power capacity and operating system that allow them to perform authentication and signing (confirm) transactions. These IoT devices are known as blockchain *"lightweight node"*[8], which means that they don't contain the full blockchain stack. Their primary task is to sign transactions (confirmations) using the blockchain mechanism. When the

[7]There are several communication protocols for IoT devices such as ZigBee, WiFi, Bluetooth, etc.
[8]The definition of the "Full Node" and "Lightweight Node": https://www.mycryptopedia.com/full-node-lightweight-node/

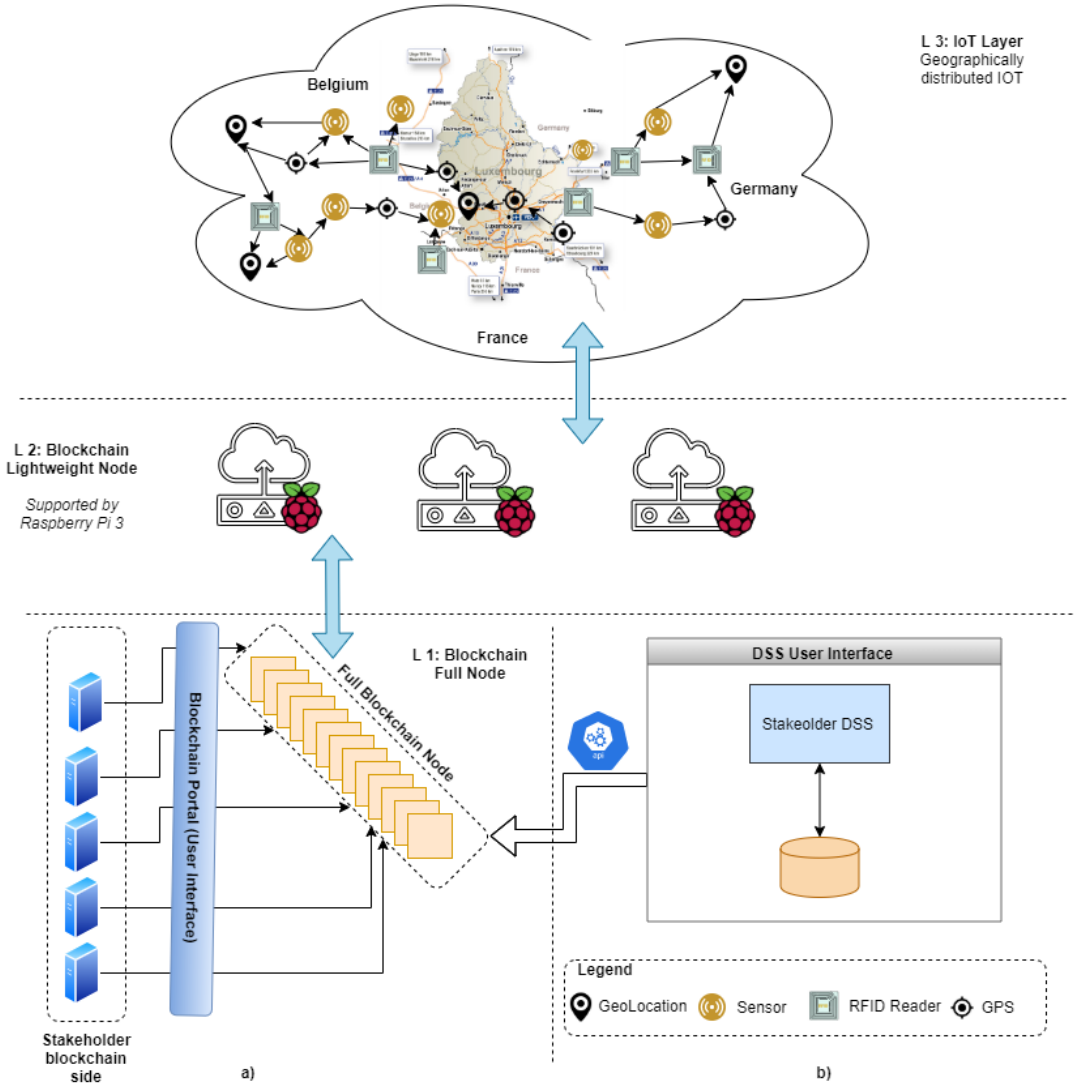

Figure 5: The conceptual architecture for a smart, secured and trusted process of TDG.

"lightweight node" receives a transaction, it first checks if that transaction is from a registered IoT device and further it signs the transaction. After signing (verifying) the transaction, the *"lightweight node"*, use the appropriate communication channel to send the transactions to the full blockchain node (L1).

The communication channel that we propose is a connection over a cellular network 2G/3G/4G provided by a mobile operator or over a wireless WAN (Wide Area Network) provided by a LPWAN (Low Power WAN) providers, e.g., SigFox, LoRA, etc., to properly transfer transaction data from L2 layer to L1 layer and vice versa. Since the communication channel could be subject to security issues in this segment of the network [59], we propose to always encrypt the transferred transactions.

- L1: *Stakeholder blockchain side*

  This layer belongs to the stakeholder's domain. It is composed of several blockchain nodes that might be deployed in different premises of the stakeholder creating a geographically distributed networked system. These nodes have the capabilities to add new blocks into the blockchain. These are a set of transactions received from the previous layer (L2) and/or transactions received from other stakeholders. The business logic required for TDG is implemented in this layer by main of a well defined *Smart Contract (SC)*. The SC that is intended to express the workflow of the process of TDG is deployed on this layer to fulfill the TDG business logic. Furthermore, all other components such as IoT devices (L3) and "lightweight nodes" (L2) are registered on this layer. When a block is added on the blockchain, the corresponding SC is executed in order to trigger the specified tasks in the business model in conformance with its logics.

  This layer serves also as user interface for the stakeholders. The ones involved in the process might use the

API provided by layer to insert immutable information (using the *blockchain portal*) and share them with other authorized stakeholders (as presented on the left side of the Figure 5, (L1 (a))), exchange information with other stakeholders and monitor the lifecycle of the TDG process [30].

The proposed approach permits also to existing business applications such as DSS, or other ERP systems, to connect to the blockchain (as full blockchain nodes) using specific API, as presented on the right side 5, (L1 (b)) [28].

This proposed approach aims to provide a new way of managing, storing and sharing information in the process of TDG. This allows stakeholders to connect their applications to the system while eliminating the need to use third-party or centralized systems (e.g., clouds or centralized databases), as presented in Figure 3. Using blockchain technology for storing and managing the information brings to the system the required level of confidentiality. As a matter of fact, only the certified parties are enabled to perform actions in the Supply Chain of DG. Furthermore, this system enables the authentication and authorization of any stakeholder accessing the system. All the users are authenticated and a full authorization control is performed on any of their actions. For example, a driver is only allowed to load DG if he is successfully authenticated by the host, e.g., "DG Provider", and at the same time the location of the driver should be one of the "DG Provider" premises. In case of violation, a notification alarm is sent to "authorities" and "DG Receiver" for non-compliance.

In such a system the information remains immutable, thanks to the blockchain properties. The nodes hosting the main ledger are fully decentralized, and the system remains sustainable since none of the end-users (stakeholders) is able to shut-down the whole system.

The information sensed by IoT devices provides real-time tractability information about the actual state of the TDG process. The user interface allows authorized stakeholders to monitor the process and securely store their data in the system. The ability of immutable record-keeping of blockchain enables auditing of processes and operations for TDG.

5. PROOF OF CONCEPT (POC) IMPLEMENTATION

This section presents some technical information about the implementation of the proposed solution. In this initial proof of concepts (PoC), we have implemented and integrated all parts of the proposed approach. In addition, we have used real IoT devices to simulate the end-to-end scenario for TDG.

Firstly, we present the specification of the smart contracts that are used in the PoC. Secondly, we present the sub-networks, i.e., channels for managing the confidentiality of the exchanges between stakeholders.

Thirdly, we present the technical pre-requisites for the development of the solution.

5.1 Smart Contracts (SC) specification

We have identified the need to specify and developed nine different SCs to fulfill the requirements of the presented use case, i.e., 4.2. These specification are available for downloading and testing at Github [37].

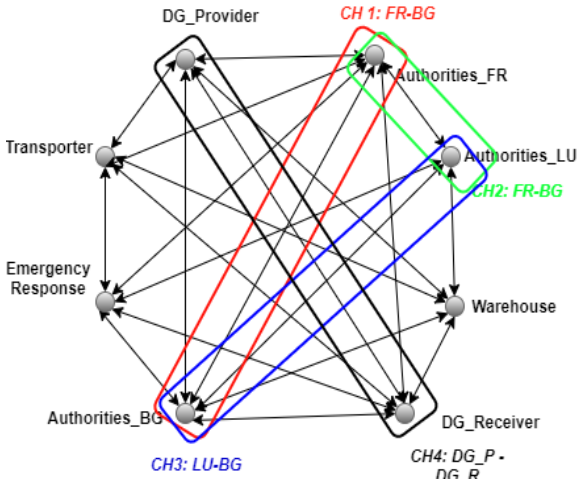

Figure 6: The structure of sub-networks (channels) in HF for TDG. Inspired from [30].

We have also implemented an end-to-end test script called *end2endtest.bash*, which contains the necessary information to run the example individually.

In the following, we will present and discuss the specification of the nine SC:

1. `SmartContract_DG`

   This SC determines the properties of the DG, which are prepared for transportation. The main attributes highlighted here are DG identification, type of DG, risk level (sensitive parameters, e.g., in high temperature, humidity, disturbance, or others), quantity etc. Moreover, this SC allows stakeholders to introduce a new DG that is subject to transport.

2. `SC_DG_Process_Initialization`

   This SC offers one of the main functionalities of our approach. It initializes the process of TDG. For each TDG, an *identified (ID) process* will be initialized. This SC also informs the involved stakeholders about the starting of the process. This process (ID) remains open, and all interactions, for example, the exchange of information with authorities or between stakeholders will be identified with the process (ID). There could be a situation where the TDG process can start while DG might be stored in a Warehouse (an intermediate stop) and remains there for a certain time period, e.g., several weeks before delivery. In this case, the process remains open until this DG is eventually delivered to the contractual destination, i.e., "DG Receiver premise", as presented in Figure 4. This SC maintains effectively the workflow of the process of TDG.

3. `SC_DG_Process_Status`

   The essential functionality of this SC is to allow stakeholders, e.g., "Authorities", to check the current status of the TDG. This SC permits only authorized stakeholders to monitor the process of TDG and therefore play a key role in the traceability of the TDG process lifecycle.

4. `SC_DG_Transport`

   This SC is responsible for authorizing the starting the process of transport of DG. It provides all the information about the transport modalities, such as the type of DG to transport, the itinerary information, and the truck-related information. This information is valuable for authorities that are responsible for monitoring the movement of DG, and identify transport transportation mean.

5. `SC_DG_Cross_Warehouse`

   Gives the necessary information about the warehouse facility. A piece of information is the location of the warehouse, current capacity to host DG to be stored, information on the arrival date/time of DG, availability to maintain the state of the DG with the required level of safety conditions (expressed by SmartContract_DG).

6. `SC_DG_Cross_Border`

   Presents a checking point, when the truck arrives at the border of a country, and it automatically informs stakeholders, i.e., "Authorities" of both countries and also the "DG Receiver".

7. `SC_DG_Process_Destination`

   When the DG is received by the "DG Receiver", this SC automatically informs other stakeholders, e.g., "Authorities" and the "DG provider" about it. Furthermore, it provides on DG delivery all available authentication information to the "DG Provider", the truck location, information about truck identification and DG package identification (e.g., by using RFID), the digital driver signature. This process is made possible with the help of information transmitted by various IoT devices deployed in the environment as well as other information that are available to the system.

8. `SC_Alert`

   This SC alerts stakeholders when an emergency situation arises. This SC is triggered:

   - when the risk parameters are matched, e.g., high temperature and an accident probability is high.
   - when the accident has happened (detected by a combination of information from sensors of temperature (humidity) and disturbance), the emergency alarm should be immediately sent to the responsible stakeholders, e.g., "Authorities" and shoul trigger "Emergency Responses".

   To highlight the contain of this particular SC, a simplified specification is presented in Listing 1.

```
S0:@parameters:
    stakeholderList,
    IoTDeviceList,
    SubstanceList,
    transportedSubstance,
    location,
    timestamp,
    riskLevel,
    disturbanceMeasure,
    disturbanceLevelWave,
    TempLevelSubstance,
    S1: check (if
        ReceivedTransaction in
        IoTDeviceList)
    S2: check (if
        transportedSubstance in
                SubstanceList) and
            ((TempLevelSubstance
            >=substanceRiskLevel)
                or
            disturbanceMeasure >=
            disturbanceLevelWave)
    S3: check (if stakeholder in
        stakeholderList)
    S4: function (sendMessage:
        Alert (location,timestamp)
    -> stakeholder))
```

Listing 1: SC alert

9. `SC_IoT`

   This SC models the interaction between IoT devices and the full blockchain node. It is used by other SC such as *SC_DG_Transport*, *SC_DG_Cross_Warehouse*, *SC_DG _Cross_Border* and *SC_DG_Process_Destination*.

5.2 Channels and Network Organization

As stated before, the concept of channel in HL enables privacy and confidentiality. In the context of TDG, stakeholder communication is sensitive and requires high-level security. To fulfill this requirement, we have composed a network that allows stakeholders to manage their communications and to exchange information thought their *private channels*.

The information exchanged by stakeholders, which appears as "transaction" on the blockchain, should not be accessible to the participant of the channel and not to any other one. The sketch presented in Figure 6, shows a possible organization of the network of stakeholders, where filled circles indicate stakeholders, thin arrows indicate communication, and colored layouts present private sub-networks or channels, e.g., *CH1: FR-BG*. HF allows stakeholders to configure the members of communication channel by adding the stakeholders to their network [26]. The network and peers (blockchain nodes) are distributed geographically and managed mainly on the premises of the stakeholders.

5.3 Technical components used for the PoC

To implement our approach, we have settled up a technical working environment composed of the three following software components:

1. *Full Blockchain Node Environment*
   As stated before, we have selected a consortium blockchain framework named "Hyperledger Fabric (HL)". Several technical dependencies for running this blockchain framework are required:

   - Hyperledger Fabric v1.4
   - Docker Container v18.09.7 [15]
   - Docker Composer v3.7
   - Node.Js v10.18.0
   - Server (nodes) characteristics:
     - RAM Memory: 10 GB
     - Processing Power: Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz

Furthermore, regarding **tools** for HL, we have used "Hurley" as a development environment, and "Convector" to manage the smart contracts [3].

2. *Lightweight Blockchain Nodes*

   For this layer, we have chosen embedded devices with enough available computing resources act as transaction validator, data aggregator, and data transmitter:

   - Raspberry Pi4[9]
     - Operating system: Raspbian
     - Communication protocol Bluetooth (or Zigbee)
     - Long Range Communication: 3G, SigFox

3. *IoT devices Nodes* We could use different types of IoT devices in our POC:

   - Wireless Sensors
     - Environmental data: - Temperature and Humidity: HTU21D
     - Disturbance data: HC-SR04
     - Location:GPS coordinates
   - Mobile phone/tablet (Android or iOS)
   - RFID Readers
     - Barcode Reader
     - RFID tag Reader

6. EXPERIMENTS AND RESULTS

To evaluate the proposed solution, we have defined different evaluation metrics. Firstly, we estimate the overall *blockchain weight (size)* in term of number of transactions received from IoT devices and exchanged between stakeholders. This metric is important because it impacts the overall weight of the blockchain. Secondly, we estimate the *processing time required for transaction* since it indicates the time performance of the system. Finally, we estimate the *size of data composing the transactions sent.*

Initially, an end-to-end scenario is specified and we measure the necessary time required to create all the objects (i.e. representing stakeholders) that are used for the TDG process. Figure 7 shows the number of transactions, and also the required time (expressed in seconds) for the creation of each object . This total time to create all objects is around 18.9s, with an average time for the creation of an object equal to 2,57s.

Blockchain weight (size):

The objective here is to measure the block weight for N *number of transactions.* this indicator is important to understand the scalability properties of the solution. Indeed, even if in this initial scenario, the number of stakeholder is small, this indicator gives a initial idea about the scalability and helps in its extension to a more complex and large one. Figure 8, shows the dynamic of the weights (sizes) of the exchanged blocks during time.

Processing time of transactions :

[9]The minimal requirement is Raspberry Pi3 B

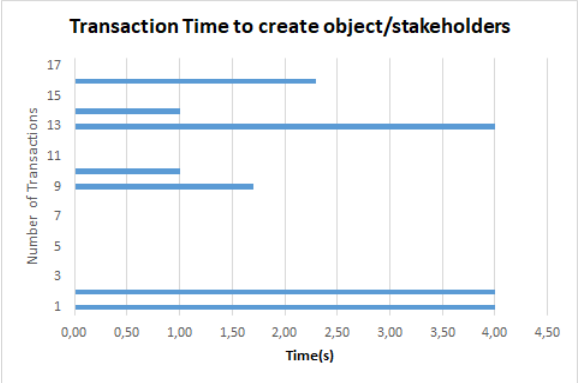

Figure 7: The required time (s) and number of transaction for object creation.

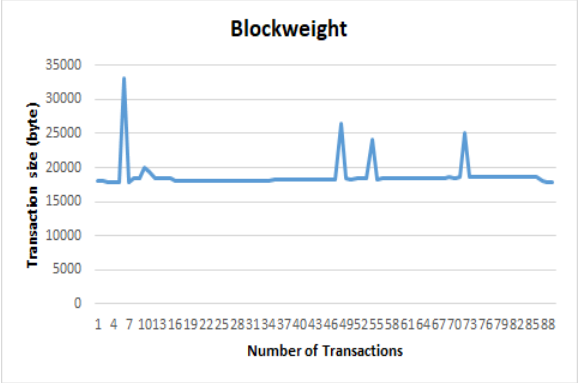

Figure 8: Monitoring of the block weight (size) for performance issues.

This measurement indicates the time required to process the transactions that are created during time. This time actually depends on the frequency of messages received from the IoT devices (e.g. *collect_temperature, transaction_humidity, transaction_location*) and the needed time to add these transactions as blocks in the blockchain. The addition of these two times represents the global latency of the system. The obtained results indicates that the average time needed to compose these transactions is 2.8s, with a standard deviation of $\sigma = 0.0081s$.

Size of data composing the transactions:

The average transaction size highlights another significant element in the evaluation of the performance of the proposed solution. Since data is coming from different sources of the global system (i.e. IoT devices, Stakeholders, ...), it may then have different sizes. This has an impact on the transactions sizes and therefore on the performances of the system. Figure 9 highlight the results obtained from our tests.

6.1 Our approach vs other existing research proposals

In this section, we aim to present a short comparison of our solution against other existing approaches aiming also to integrate blockchain and IoT technologies for TDG. We no-

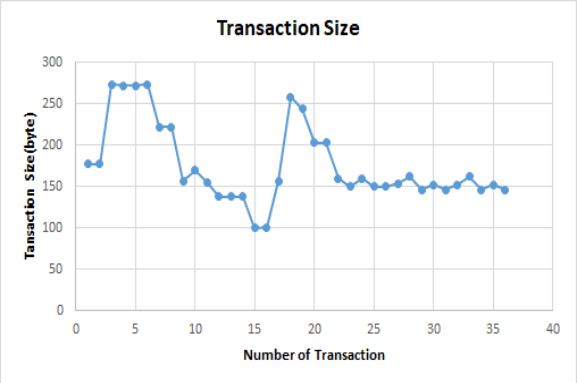

Figure 9: Monitoring of the transaction size for performance issues.

tice that most other approaches do not explicitly introduce the various stakeholders involved in the process. Indeed, in our approach, regulatory is a cornerstone of the solution. All stakeholders involved in the process and explicitly incorporated as virtual objects (digital twins) in the system and could only interact with it through these objects. This allow us to consider the end-to-end process as a unified process and SCs as means to enforce the business logic of the process. To the best of our knowledge, this has not been by any existing contribution. The proposed approaches fills this research gap 4 and bring in the following advantages:

a) Technical capabilities for immutable IoT data. Firstly, the technical features of our approach enable storing immutable information. That information is treated if, and only if it is retrieved from authenticated low complexity IoT devices that are already *"certified"* and registered in the deployed system. Secondly, we use other types of more powerful embedded devices, (i.e., Raspberry Pi), which beyond signing transactions, it also acts as a *data aggregator*, in case the connection with the application layer, i.e., blockchain is temporarily lost. We argue that this capability to *aggregating data* significantly improves the *reliability* of the system since generated data from IoT never vanishes. Third, in the application layer (L1), we use an appropriate blockchain framework, i.e., HF, which supports and satisfies the performance requirements for such use cases. The configurable architecture of HF enables efficient data transmission, and the scalability is secured.

b) Organizational aspect for the use case and compliance with the regulatory framework.

Primarily, we deploy a system that enables stakeholders to act in compliance with the regulatory framework.

The design principles used for the proposed use case determines that the data flow, monitoring aspects (traceability) of the movement of DG, are under the surveillance of the stakeholders. In such a scenario, information security, privacy, and confidentiality properties are highly required by stakeholders. This process should follow at any time the requirements of the stakeholders and always be in compliance with the regulatory framework of the countries where the DG is. To achieve this objective, we specified several SC to capture and execute the operations that are needed to make the process compliant with the stakeholder requirements and regulatory framework. For example, the case of notifying *stakeholders* when DG is crossing the border incorporates privacy and confidentially issues (according to stakeholder requirements and regulatory framework). In this situation, this information should be sent only to the relevant stakeholders, e.g., "Authorities" and authorized stakeholders.

7. CONCLUSION AND FUTURE WORKS

The transparency, reliability, and security of information, are among the main requirements for a sustainable Supply Chain for TDG. For responding to the highlighted concerns in the TDG as presented in section 1.3, we proposed a novel solution in order to collect information about the TDG process in the physical world and monitor its life-cycle in the digital world. We have used IoT and blockchain technologies in an integrated manner along with smart contracts (SC). The objective of the system is to allow to capture the semantic of the safe execution of the TDG process as well as all the required interactions between the different parties. All stakeholders involved in the process are represented in the system as a digital twins (objects) in order to allow them to interact with the system in a secure and authorized way. The consensus mechanism in blockchain technology supports the security aspect of the data stored in such a system while the distributed and decentralized nature of the blockchain avoids the single point of failure of existing centralized systems. Furthermore, the authentication of IoT devices and verification of the transaction by *lightweight nodes* contributes to transparency improvement. On the other hand, with the help of the SC, the process of TDG is traceable, auditable, and the authorized stakeholders can monitor the process at any time. We implemented a Proof of Concept prototype and executed a use case scenario close to a real situation. We evaluated using several metrics the performances of the system as well as its correctness. For future works, We are planing different extensions to this project, such as the multi-country deployment schema, which will incorporate several stakeholders from different countries that cooperate for the TDG from one country to another possibility crossing several third party countries such as in Europe.

8. ACKNOWLEDGMENTS

We acknowledge our colleagues Jonathan Lamont, for helping on developing the PoC, and Sébastien Faye and Foued Melakessou for supporting with IoT device implementation.

9. REFERENCES

[1] AWS IoT - Amazon Web Services. `https://aws.amazon.com/iot/`. (Accessed on 04/08/2020).

[2] Dangerous Goods Classification. `https://www.unece.org/fileadmin/DAM/trans/danger/publi/unrec/rev14/English/02E_Part2.pdf`. (Accessed on 04/01/2020).

[3] Getting Started - Covalent Documentation. `https://docs.covalentx.com/article/71-getting-started`. (Accessed on 12/30/2019).

[4] Hyperledger-Fabric Documentation. `https://buildmedia.readthedocs.org/media/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf`. (Accessed on 12/10/2019).

[5] IoT Use Cases for Enigma & Homomorphic Encryption. `https:`

//www.vdcresearch.com/News-events/iot-blog/iot-use-cases-for-enigma-homomorphic-encryption.html. (Accessed on 12/20/2019).

[6] On the Tangle, White Papers, Proofs, Airplanes, and Local Modifiers. https://blog.iota.org/on-the-tangle-white-papers-proofs-airplanes/-and-local-modifiers-44683aff8fea. (Accessed on 12/19/2019).

[7] M. Ammar, G. Russello, and B. Crispo. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38:8–27, 2018.

[8] K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the Internet of Things. *Ieee Access*, 4:2292–2303, 2016.

[9] A. Cocchia. Smart and digital city: A systematic literature review. In *Smart city*, pages 13–43. Springer, 2014.

[10] A. Conca, C. Ridella, and E. Sapori. A risk assessment for road transportation of dangerous goods: a routing solution. *Transportation Research Procedia*, 14:2890–2899, 2016.

[11] M. Conoscenti, A. Vetro, and J. C. De Martin. Blockchain for the Internet of Things: A systematic literature review. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pages 1–6. IEEE, 2016.

[12] COTIF. Regulation Concerning the International Carriage of Dangerous Goods by Rail. http://otif.org/fileadmin/new/3-Reference-Text/3B-RID/RID_2017_E.pdf. (Accessed on 12/07/2019).

[13] L. Da Xu, W. He, and S. Li. Internet of Things in industries: A survey. *IEEE Transactions on industrial informatics*, 10(4):2233–2243, 2014.

[14] L. Ding, Y. Chen, and J. Li. Monitoring dangerous goods in container yard using the Internet of Things. *Scientific Programming*, 2016, 2016.

[15] Docker. Enterprise Container Platform | Docker. https://www.docker.com/. (Accessed on 12/10/2019).

[16] A. Dorri, S. S. Kanhere, and R. Jurdak. Towards an optimized blockchain for IoT. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, pages 173–178. ACM, 2017.

[17] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, pages 618–623. IEEE, 2017.

[18] Eurostat. Road freight transport by type of goods - Statistics Explained. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Road_freight_transport_by_type_of_goods#Road_freight_transport_of_dangerous_goods. (Accessed on 08/04/2020).

[19] T. M. Fernández-Caramés and P. Fraga-Lamas. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, 6:32979–33001, 2018.

[20] W. C. Frank, J.-C. Thill, and R. Batta. Spatial decision support system for hazardous material truck routing. *Transportation Research Part C: Emerging Technologies*, 8(1-6):337–359, 2000.

[21] F. Golatowski, B. Butzin, T. Brockmann, T. Schulz, M. Kasparick, Y. Li, R. Rahmani, A. Haber, M. Sakalsız, and Ö. Aydemir. Challenges and Research Directions for Blockchains in the Internet of Things. In *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, pages 712–717. IEEE, 2019.

[22] C. Harbor. IOTA: The Distributed Ledger Technology Designed for the Internet of Things. Source: https://www.hackster.io/news/iota-the-distributed-ledger-technology-designed-for-the-internet-of-things-f6abaf0e45a4, 04, 2019, (Accessed on 04/25/2020).

[23] E. Hofmann and M. Rüsch. Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*, 89:23–34, 2017.

[24] S. Huh, S. Cho, and S. Kim. Managing IoT devices using blockchain platform. In *Advanced Communication Technology (ICACT), 2017 19th International Conference on*, pages 464–467. IEEE, 2017.

[25] Hyperledger. A Blockchain Platform for the Enterprise. https://hyperledger-fabric.readthedocs.io/en/release-1.4/. (Accessed on 12/10/2019).

[26] Hyperledger.org. Hyperledger: An Open Source Blockchain Technologies. https://www.hyperledger.org/. (Accessed on 12/10/2019).

[27] A. Imeri, N. Agoulmine, C. Feltus, and D. Khadraoui. Blockchain: Analysis of the New Technological Components as Opportunity to Solve the Trust Issues in Supply Chain Management. In *Intelligent Computing-Proceedings of the Computing Conference*, pages 474–493. Springer, 2019.

[28] A. Imeri, N. Agoulmine, and D. Khadraoui. A secure and smart environment for the transportation of dangerous goods by using Blockchain and IoT devices. pages 1–8, 2019.

[29] A. Imeri, A. Khadraoui, and D. Khadraoui. A Conceptual and Technical Approach for Transportation of Dangerous Goods in Compliance with Regulatory Framework. *Journal of Software*, 12(9):708–722, 2017.

[30] A. Imeri and D. Khadraoui. The security and traceability of shared information in the process of transportation of dangerous goods. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5. IEEE, 2018.

[31] A. Imeri, D. Khadraoui, and N. Agoulmine. Blockchain Technology for the Improvement of SCM and Logistics Services: A Survey. In *Industrial Engineering in the Big Data Era*, pages 349–361. Springer, 2019.

[32] A. Imeri, J. Lamont, N. Agoulmine, and D. Khadraoui. Model of Dynamic Smart Contract for permissioned Blockchains. In *Proceedings of the Practice of Enterprise Modelling 2019 Conference Forum, Luxembourg*, 2019.

[33] IOTA. The Next Generation of Distributed Ledger

Technology | IOTA. https://www.iota.org/. (Accessed on 12/19/2019).

[34] Y. Jiang, C. Wang, Y. Wang, and L. Gao. A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management. *Sensors*, 19(9):2042, 2019.

[35] M. A. Khan and K. Salah. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395–411, 2018.

[36] K. Košt'ál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak. Management and Monitoring of IoT Devices Using Blockchain. *Sensors*, 19(4):856, 2019.

[37] J. Lamont and A. Imeri. Blockchain and IoT in Dangerous Goods Transportation. https://github.com/Gr4pha/hyperledger-blockchain-and-iot. (Accessed on 08/04/2019).

[38] C. Liao, S. Bao, C. Cheng, and K. Chen. On design issues and architectural styles for blockchain-driven IoT services. In *Consumer Electronics-Taiwan (ICCE-TW), 2017 IEEE International Conference on*, pages 351–352. IEEE, 2017.

[39] J. Lin, Z. Shen, and C. Miao. Using blockchain technology to build trust in sharing LoRaWAN IoT. In *Proceedings of the 2nd International Conference on Crowd Science and Engineering*, pages 38–43. ACM, 2017.

[40] S. Lucero. IoT platforms: enabling the Internet of Things. https://www.esparkinfo.com/wp-content/uploads/2018/11/enabling-IOT.pdf, 2016.

[41] C. M. Medaglia and A. Serbanati. An overview of privacy and security issues in the Internet of Things. In *The Internet of Things*, pages 389–395. Springer, 2010.

[42] G. D. Molero, F. E. Santarremigia, P. Aragonés-Beltrán, and J.-P. Pastor-Ferrando. Total safety by design: Increased safety and operability of supply chain of inland terminals for containers with dangerous goods. *Safety science*, 100:168–182, 2017.

[43] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, White papers, 2008.

[44] T. Nam and T. A. Pardo. Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times*, pages 282–291. ACM, 2011.

[45] E. V. Ocalir-Akunal. Decision support systems in transport planning. *Procedia engineering*, 161:1119–1126, 2016.

[46] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito. Blockchain and IoT Integration: A Systematic Survey. *Sensors*, 18(8):2575, 2018.

[47] E. Parliament. Regulation (EC) No 1013/2006 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1013&from=EN, 2006. (Accessed on 12/07/2019).

[48] S. Popov. IOTA White papers: The Tangle. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf. (Accessed on 12/19/2019).

[49] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustišek. Towards decentralized IoT security enhancement: A blockchain approach. *Computers & Electrical Engineering*, 72:266–273, 2018.

[50] A. Raschendorfer, B. Mörzinger, E. Steinberger, P. Pelzmann, R. Oswald, M. Stadler, and F. Bleicher. On IOTA as a potential enabler for an M2M economy in manufacturing. *Procedia CIRP*, 79:379–384, 2019.

[51] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz. On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 2018.

[52] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher. Towards using blockchain technology for IoT data access protection. In *Ubiquitous Wireless Broadband (ICUWB), 2017 IEEE 17th International Conference on*, pages 1–5. IEEE, 2017.

[53] H. Sukhwani, N. Wang, K. S. Trivedi, and A. Rindos. Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network). In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pages 1–8. IEEE, 2018.

[54] P. Tasca and C. J. Tessone. Taxonomy of blockchain technologies. principles of identification and classification. *arXiv preprint arXiv:1708.04872*, 2017.

[55] Tedermint. Cosmos/Ethermint: Ethereum on Tendermint using Cosmos-SDK! https://github.com/cosmos/ethermint. (Accessed on 12/19/2019).

[56] V. Torretta, E. C. Rada, M. Schiavon, and P. Viotti. Decision support systems for assessing risks involved in transporting hazardous materials: A review. *Safety science*, 92:1–9, 2017.

[57] UNECE. European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR). https://www.unece.org/trans/danger/publi/adr/adr2017/17contentse0.html. (Accessed on 04/08/2020).

[58] N. Vayiokas. Risk Assessment of Transportation of Dangerous Goods.

[59] J. M. Voas. Networks of 'Things' | NIST. https://www.nist.gov/publications/networks-things, July 2016. (Accessed on 12/11/2019).

[60] N. Wang, X. Huang, and D. Wei. Route selection for dangerous goods based on D numbers. In *Control and Decision Conference (CCDC), 2016 Chinese*, pages 6651–6656. IEEE, 2016.

[61] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen. The blockchain as a software connector. In *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, pages 182–191. IEEE, 2016.

[62] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba. A taxonomy of blockchain-based systems for architecture design. In *Software Architecture (ICSA), 2017 IEEE International Conference on*, pages 243–252. IEEE, 2017.

[63] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5):1250–1258, 2017.

[64] H. Yi and F. Wei. Research on a Suitable Blockchain for IoT Platform. In *Recent Developments in Intelligent Computing, Communication and Devices*, pages 1063–1072. Springer, 2019.

[65] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4):352–375, 2018.

[66] K. G. Zografos and K. N. Androutsopoulos. A decision support system for integrated hazardous materials routing and emergency response decisions. *Transportation Research Part C: Emerging Technologies*, 16(6):684–703, 2008.

[67] G. Zyskind, O. Nathan, and A. Pentland. Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471*, 2015.