The Blockchain-Based Digital Certificate for the Transport of Dangerous Goods

Adnan Imeri, Christophe Feltus, Nazim Agoulmine, Djamel Khadraoui

The Blockchain-Based Digital Certificate for the Transport of Dangerous Goods

Adnan Imeri, Christophe Feltus, Nazim Agoulmine, and Djamel Khadraoui

1 Introduction

The transport of dangerous goods (TDG), also named hazardous goods (e.g., oils, gas, chemical products, radioactive substances, corrosive products, explosives, medical waste), consists in the carriage of goods presenting potential important risks to the people, to material, and/or to the environment, and which necessitates dedicated and specially reinforced security measures therefore. This transport of dangerous goods (TDG) represents an excessively important activity for the countries of the European Union and worldwide, as most member states increase in transport of dangerous goods in the recent years. The highest increase, in EU, was recorded in 2018 and concern Belgium (77.3%), Slovenia (46.7%), Croatia (42.3%), and Finland (36.7%).[1] According to global statistics [1], dangerous goods may constitute about fifty percent of the global transportation in the next years, should it be by road, railway, air, or seas. Compared to traditional transportation e.g., general supply chains, the TDG is a particular class of transportation that is subject to specific requirements among which the human and environmental safety.

[1] https://ec.europa.eu/eurostat/statistics-explained

A. Imeri (✉)
Luxembourg Institute of Science and Technology, Esch-sur-Alzette, Luxembourg

Université of Evry Val d'Essonne, Evry, France
e-mail: adnan.imeri@list.lu

C. Feltus · D. Khadraoui
Luxembourg Institute of Science and Technology, Esch-sur-Alzette, Luxembourg

N. Agoulmine
Université of Evry Val d'Essonne, Evry, France

It also incorporates rigorous information immutability and the traceability of the DG movement [2], as indicated in the "Agreement concerning the International Carriage of Dangerous Goods by Road" [3] applicable since 1 January 2021.

In this context, this chapter aims to propose a platform to support the verification of the identity, of the history of transportation, and of the location over time of the dangerous goods by means of blockchain-based digital certificate acting as a method for documented recorded identification. The principle of the blockchain is that a specific data is recorded as a series of "blocks" which is distributed over the network and is accessible by users possessing private keys that they use to identify themselves and electronically sign transactions. This "block" also contains (1) hash values that allow verifying the data and (2) a piece of the hash value from the previous block that guarantee traceability and integrity of the information. When users create more data, new blocks are successively added to this block chain and are recorded with ledger-based technology to track transactions but also to ensure accountability.

In parallel, a digital certificate is a credential which allows an organization to identify and share information in a secure way over Internet or other private network by means of a pair of public/private key. Using jointly **blockchain technology** and **digital certificate** in the paper aims to ensure transaction *transparency* thanks to an unalterable record distributed among many users, *easy access* thanks to the collaborative environment that makes it easier for all agents to rapidly access on the transportation information, less *paperwork* thanks to the electronic distribution of data, and especially, *strong users identification* thanks to the digital certificates' credentials. This signifies, by the way, greater gains in efficiency, more streamlined approach at the management level, more reactivity in the treatment of information, and less risks of treatment-based errors.

Besides proposing a blockchain-based digital certificate for the TDG, our approach also analyzes to what extent the blockchain may be specified to integrate and be compatible with the **Internet of Things** (IoT) technology and specifications. IoT for the TDG has been considered as an important technology to move toward the digital society and is capable of supporting intelligent applications such as container information forecasting, container gate-in and gate-out management, fire control, and environmental parameters monitoring [4]. Our platform is fully compatible with the IoT technology and allows leveraging the benefits generated so far.

1.1 Supply Chain Management

The extraordinarily growing globalization of production and the megabit of data generated by the manufacturing and transportation processes have forced industries to set up supply chain management sufficiently autonomous and efficient to support the integration of key business processes from the original suppliers through the end-users [5]. According to [6], nowadays the commonly accepted paradigms of supply chain management are no more appropriate for operating in *data-driven*

smart manufacturing and goods transportation, provided the cost and effectiveness impact engendered by the imposed unnecessary constraints on the system. For Li et al. [6], the origin of this problem lies with the lack of structural limitations of the current paradigms, that is., to deal with the massive volume of data emerging at the various stages of production and transportation. This statement is especially relevant for the sector of the TDG, as explained in Sub Section 1.2, provided the overload of information legally required by the governments (e.g., Directive 2008/68/CE, "TMD" decree, Regulation 84-810 and 2003-699, Article L. 5331-2).

1.2 Supply Chain for Dangerous Goods

In this section, we present a study concerning the supply chain of dangerous goods (DGs). Initially, we present the definition of DG, then details of the supply chain of DG highlighting the complexity in the TDG, including the main stakeholders involved in TDG.

Dangerous goods (DGs) are considered as any material or substance or a mixture of substances (gases, liquid, or solids), which exposes potential risks (identified as hazardous) for harming humans, animals, property, and the environment [3]. DGs are classified based on their physical and chemical effects ADR2021. ADR classifies DG in categories such as "Explosives," "Gases," "Flammable liquid," "Flammable solids," "Oxidizing substances and organic peroxides," "Toxic and infectious substances," "Radioactive material," "Corrosive substances," and "Miscellaneous dangerous substances and articles" [3, 7].

The supply chain of DG is complex and belongs to the regulated domains. The complexity originates from the involvement of many regulatory frameworks at the national and international levels. The regulatory framework governs TDG entirely [8]. Table 1 shows the main regulatory frameworks applied in the TDG. In the context of our study, we are mainly focused on road transport of DG as one of the most used transport modes in the supply chain of DG [13].

The TDG requires strict procedures for preparing transportation and its specificity, documentation, and DG treatment. The DG storage, treatment, and reuse or processing (for industrial purposes) refer to the management part of DG. Figure 1, presents the general supply chain for DG. For operation with the DG, various participants are involved, such are "Consignors," "Transporter," "Driver and vehicle crew," "Filler," "Loader," "Unloader," "Consignee," "Tank-operator/portable tank operator," and "DG Safety Advisor." Section 4 of ADR specifies roles (participants) and legal responsibilities for each involved party in TDG [3].

1.3 Research Method

At a methodological level, the research that we tackle concerns the improvement of the traceability in the field of the transport of dangerous goods. Accordingly,

Table 1 International regulatory framework and agreements for TDG, specific to the mode of transport

Mode of transport	Regulatory framework	International organization	Abbrev.
Road (Land)	European Agreement on the International Carriage of Dangerous Goods [3]	UNECE	ADR
Inland Waterway	European Agreement on the international carriage of Dangerous Goods by Inland Waterway Navigation [9]	UNECE	ADN
Rail	Regulation for the International carriage of Dangerous Goods by Rail [10]	OTIF	RID
Sea	International Maritime Dangerous Goods Code [11]	IOM/CCC	IMDG Code
Air	Dangerous Goods Regulations; Technical Instructions For The Safe Transport of Dangerous Goods by Air [12]	ICAO	DGR IACI IT

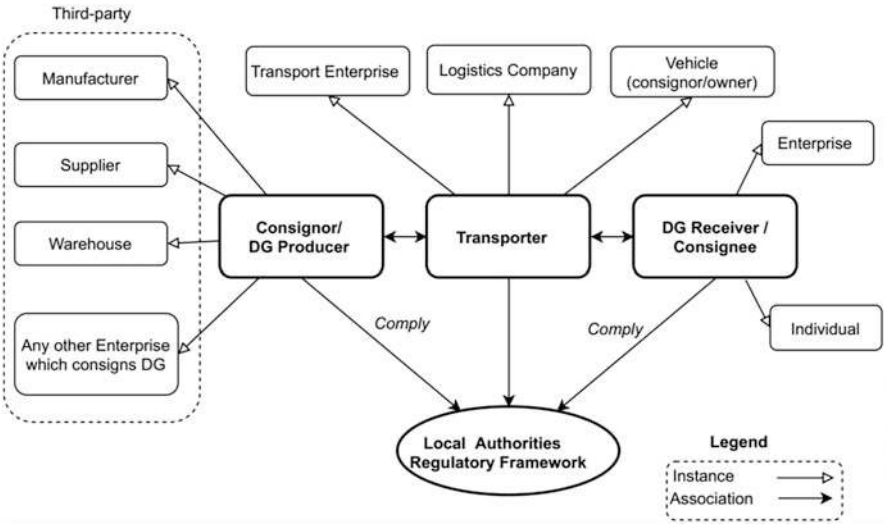

Fig. 1 The involved stakeholders and basic organization of the supply chain for TDG. Inspired from [3]

we have defined and conceptualized a blockchain-based solution that aims to enable following the DG life cycle from its origin (depart point) to destination (processing of DG). Through this research, we strengthen the stakeholders' trust in the TDG chain by raising up the transparency level through the information system which sustains this chain. Accordingly [14], explains that the **Design Science Research (DSR)** paradigm seeks to extend the boundaries of human and organization capability by creating new and innovative artefacts. Practically, provided that we aim to design a new artifact (the BC-based solution) to allow the

stakeholder to trust the DG transportation with IT enablers, we acknowledge that this research may plainly be considered in the scope of DSR [15]. As advocated by the DSR theory [14, 15], the method that we use to design this solution is an iterative approach consisting first of analyzing the problem under scope and in defining the requirement for a solution, second of defining and validating the relevant concepts, and third of designing the blockchain-based solution.

Given that our artifact is motivated by real problems and relies on the knowledge of the field, we need to involve practitioners and end-users all along with the artifact-building activities. Therefore, we have applied the design research method proposed by [16]: the Action Design Research method which objective is to strengthen the connections between the end-users (TDG companies) and the researchers by combining the building, intervention, and evaluation (BIE) activities. Given that the elaboration of our artifact strongly relates to the information system, we apply an **IT-Dominant BIE** Generic Schema (Fig. 2). When applied to our research, at step 1, we (researchers) have first performed a workshop to identify the problem of transparency and traceability of DG, in cooperation with the practitioner, that is, The Ministry of Transportation in Luxembourg. The output from this workshop significantly highlights the need to have a platform (solution) that allows "managing" the life cycle of DG in an end-to-end manner. In step 2, we have proposed a conceptual solution for information sharing and traceability related to TDG. The general conceptual solution has been validated by the scientific practitioners in [2, 17]. At step 3, we proposed a BC-based solution (beta version), and at step 4, the proposed solution was presented to the involved stakeholders and end-users and was accepted and supported as the main solution to highlight the transparency in TDG. The components of the solution were published in [7], which proposes blockchain and IoT integration. Finally, at step 5, we plan to extend the solution by integrating it on the main TDG BC-based platform. Finally, according to [18], the evaluation

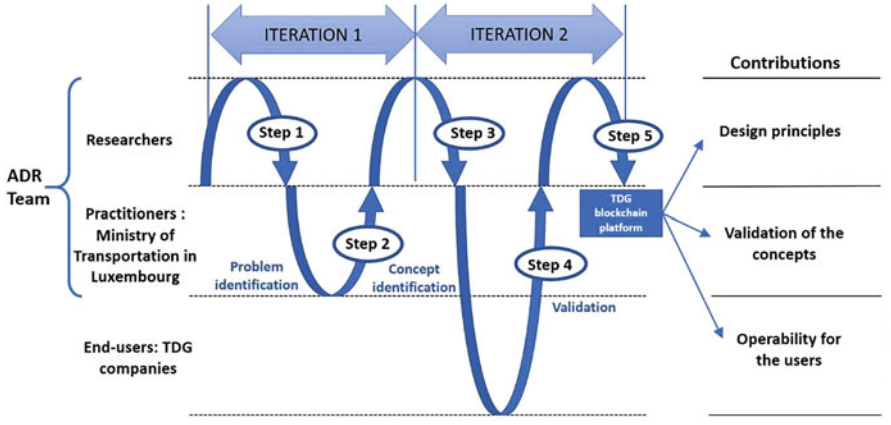

Fig. 2 IT-Dominant BIE (building, intervention, and evaluation) generic schema applied to blockchain platform for TDG design. (Adapted from [16])

of a designed artifact must use precise evaluation criteria. Provided that the goal of our research is to support end-users with an innovative TDG blockchain-based platform, the validation criteria is the operability of this platform, defined in ISO 25010 (SquaRE [19]), that is, the *ability* of the blockchain-based platform to be easily operated by a given user in a given environment. In our context, this given environment consists of the TDG infrastructure operated during the daily activities of the TDG companies. This ultimate validation should be achieved in future works.

The outline of this chapter is organized as follows. Section 2 shows the research motivation and general problem definition. Section 3 presents the main characteristics of blockchain technology. In Sect. 4, we show related works studies. Section 5 shows the conceptual approach for a digital certificate. The proof of concept (PoC) implementation is shown in Sect. 6. Finally, in Sect. 7, we conclude and present our future works.

2 Motivation and Problem Definition

DGs are sensitive and require strict supervision works in order to maintain safety and security. Entirely, the TDG process requires end-to-end transparency and to comply with the regulatory framework (as shown in Fig. 1). Authorities and the involved stakeholders require to know the life cycle of DG, starting from the preparation of DG for transport, the information during the transport, and the definitive treatment of DG. For being able to monitor the TDG, it requires adopting an approach that enhances transparency. This will be achieved with the help of technological means which ensure information immutability, availability, and security [20]. The existing systems, which are largely centralized databases [13], do not have enough technical capabilities to support data immutability and lack of availability since the centralized approach is prone to a single point of failure [7, 8, 13, 21]. Among the raised question is "How to ensure an end-to-end transparency in TDG?" "How to perform full traceability of DG in the process of transport and also in the lifetime of DG?"

Another significant issue in TDG is the dynamic changes of parameters of DG during transportation. Besides **classified substances as DG** several non-dangerous goods might turn into DG when certain environmental conditions are not fulfilled. DG reacts differently on such parameters and may cause damages or other risks such as fire, explosion, infection, and other potential risks. The raised question is, "How to ensure that the specific environmental parameters are kept under control during the transport process?" To respond to these questions, we propose a conceptual solution that responds to the specific problems related to DG. Thus, we examine the technical capabilities of blockchain and IoT for supporting our approach.

3 Background: Blockchain Technology and Its Main Characteristics

Blockchain is a distributed decentralized database that allows storing append-only transaction data. The blockchain network comprises several decentralized nodes that communicate with each other in a peer-to-peer mode. All the nodes included in the blockchain network contain the same ledger, and they rely on communication in distributed nodes, thus avoiding any central authority [22]. The blockchain nodes gather transactions into "blocks." The transactions are initially validated by performing cryptographic checks (public-private key cryptography). The process of adding a new block into blockchain is called "mining," and the nodes that perform this mining are called miners [23]. The miner[2] proposes a new block after performing specific computing power condition [24] or being delegated by other nodes to perform mining [25]. After proposing the new block, it is added to the main ledger chained with the previous block, thus achieving consensus over the transaction state by the majority of involved nodes according to the consensus protocol used, for example, Proof of Work and Proof of Stake [23]. The block of transactions that are stored into the blockchain is immutable, and cryptography tools ensure data integrity [26]. Among the main blockchain fundamental characteristics is that the block of data is linked together, so block N contains the hash address of the previous block N-1 [26, 27]. The tendency to change the information stored into blockchain is denied by consensus protocol which verifies the state of data [22].

The smart contract (SC) is an autonomous computer code encoded to react and support a specific problem [26]. It is deployed on the blockchain and executed based on its specifications to perform a specific task. SC implements a certain level of business logic and, in combination with blockchain technological capabilities, constitutes a powerful tool to solve information-related issues such as transparency, traceability, immutability, availability, and interoperability [17, 26].

4 Related Works Studies

In this section, we present some related works studies toward transparency and traceability in SCM with the help of blockchain and smart contracts.

The research from [28] shows the possible advancements of blockchain technology in operations and supply chain management. It includes enhancing product safety and security, reducing supply chain costs, improving supply chain sustainability, reducing third-party dependencies, and reducing illegal counterfeiting. The research highlights the need for further studying the blockchain technology opportunities for further adaption to supply chain operations. The research in [29]

[2] Different terms are associated with the miner, for example, full node, validator, and backer.

shows a traceability mechanism for the medicine supply chain. The approach intends to trace information from manufacturing to end consumer, which will be retrieved by scanning QR code of medical products. The authorized parties, which are authorized by the regulatory authorities of the medical supply chain, can retrieve this information. This solution, that is, "Medical supply chain" uses permissioned blockchain [30] and has a transaction data structure similar to Bitcoin [31], with a slight difference in encryption of QR code. The research from [32] explores a blockchain-based solution as a proposal to enforce sustainability in supply chain management in terms of worker protection and a safe work environment. The solution intends to respond to the consumer inquiries for social sustainability requested by consumers. It uses blockchain, IoT, and big data analytics to perform traceability from sellers and respond to consumers. The research from [33] shows an approach for digitizing and sharing the vehicles. It intends to solve the issues of vehicle odometer fraud by proposing a blockchain-based solution for storing, managing, and sharing vehicle life cycle information with several stakeholders. Similarly, in [34] a proof of concept is shown for the trading of cars in the "market of lemons[3]". It uses the principal blockchain technology features, and it organizes the research works based on design science research to provide a trustfree platform. In case of any possible error, the research includes the safeguard mechanism in transaction correction for trading in "market of lemons" [17]. The research from [35] presets a product life cycle (PLM) management. It intends to collect and manage information and knowledge to achieve competitiveness. The raised issues are sharing this information among the involved stakeholders, highlighting concerns in inseparability, openness, and decentralization since PLM is mainly implemented in a centralized way. To overcome the mentioned issues, this research proposes a blockchain-based solution integrated with IoT and M2M. In [36], the certificate of provenance for goods is proposed by using blockchain. The research in [37] presents an independent online shipment tracking framework, which intends to complement the current SCM enterprise-based solutions. The research is related to the transportation of goods from supplier to customer, known as the physical distribution phase. The current online shipment solution is considered restricted to all stakeholders, information is provided by a carrier, the sharing of information is done on a needed basis, and it remains a single source of information. The research from [38] presents *originChain,* a traceability system based on BC and smart contracts. This system intends to provide transparent, tamper-proof traceability data, data availability, and also it considers regulatory-compliance aspects by automatically checking them. It is mainly applied to companies that import products to China. It considers the traceability perspectives of the suppliers and retailers. The supplier's traceability perspective is to prove the product origin and quality and regulatory compliance, while the retailer's perspective is on product origin and quality. The *originChain* works as traceability providers, and the stakeholder that needs such a system applies for traceability services. The architecture of *originChain* indicates that the nodes are

[3] Market of Lemons: https://www.investopedia.com/terms/l/lemons-problem.asp

geographically distributed over three different premises and supported by private BC. Data storage aspects in the BC manage several data sources off-chain while storing the hash address of such data on-chain. However, this solution is limited to service providers, and its traceability services are provided following a "contract" signed between parties for the offered traceability services. The research from [39] treats the problem of determining the provenance for the goods in the supply chain. In an inter-organizational and complex supply chain, the physical provenance of goods, for example, pharmaceutic or authentic luxury goods, is not always possible because of technological limitations and the complexity of the supply chain. For solving such issues, this research highlights the potential of BC technology. In combination with IoT and using the ontologies that represent knowledge about provenance and traceability, provenance issues are answered. This research aims to develop an ontology-based BC approach for responding to provenance problems in the supply chain. Using the ontologies is for better data standards and formal specification for automated interfaces, which helps develop a better supply chain. In this context, the TOVE Ontology[4] for fundamental concepts of traceability is used to provide the provenance of goods in SC. Proof of concepts is developed, which uses a "traceable resource unit," an object to be traced from one part to another part of SC [40].

Beyond the current research, our approach presents a dynamic digital certificate for transparency and traceability improvements in the supply chain of DG. It considers dynamic environment parameters retrieved during transportation and warehousing of DG. In the context of our study, the concept of digital certification does not indicate any static issued statement, but indeed it signifies the end-to-end life cycle of specific DG, including all involved stakeholders, processes, and information. We present a concept of a digital certificate associated with a specific TDG process and dynamically maintain changes at the administrative, static (physical level), and dynamic level (environmental data retrieved from the DG surrounding environment). The proposed blockchain-based digital certificate continuously maintains the DG state and remains active until the end of the DG life cycle.

5 Blockchain-Based Digital Certificate for Transparency and Management of TDG

This section shows the conceptual approach for a digital certificate for improving the transparency in transport of DG.

[4] http://www.eil.utoronto.ca/theory/enterprise-modelling/tove/

5.1 *Conceptual Approach for Blockchain-Based Digital Certificate*

In a single DG lifecycle, the process of transport and management[5] of DG imposes at last three operation phases. The first phase is the "preparation for TDG," the second phase is the "process of transport of DG," and the last phase is the "treatment of DG" which certainly finishes the life cycle of a DG. With the concept of "digital certificate," we intend to maintain traceable information for any DG operational phase. Figure 3 shows the concept of formulation of digital certificate.

At the first phase, that is, "process of transport of DG," the specification and set of information about "authorization" to transport DG are required. Further, the identification of the involved stakeholders and DG physical characteristics need to be provided. That immediately establishes the core of the *digital certificate* which indicates that a specific set of parameters is established (stored) in distributed ledger with the help of SC. In the subsequent phases of the process of TDG, the "same" digital certificate (specific to DG) is continuously "up-dated" (addind a new parameter to the ledger). Following in the second phase, that is, "process of transport of DG" the information about the transport process is continuously captured and immutably stored in the blockchain. The eventual update on DG characteristics, for example, quantities or physical parameters, is evidenced and reported immediately to the responsible stakeholders. Finally, the third stage, that is, "treatment of DG" gathers all the details about the final treatment of DG, which also indicates the end of the DG life cycle.

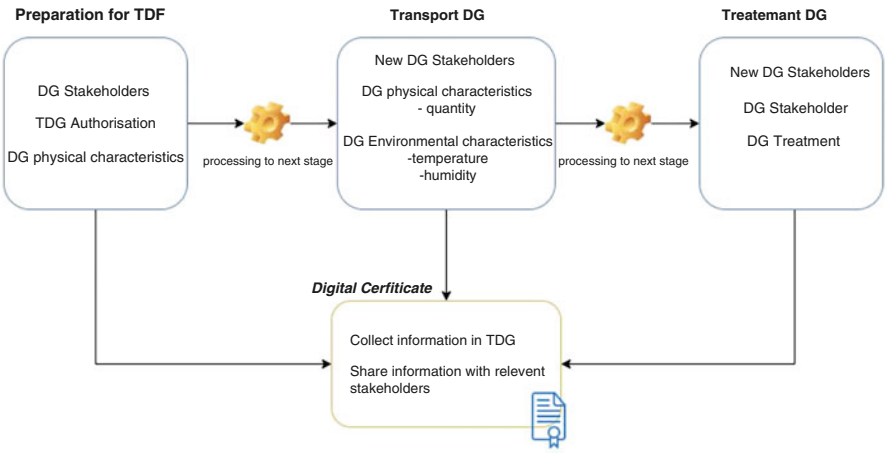

Fig. 3 The concept of the digital certificate from a different process perspective

[5] The term "management" describes storing, maintaining, and processing the DG.

5.2 Digital Certificate as for the DG

This section presents the conceptual design of the digital certificate.

The TDG stakeholders, particularly the competent authorities, require surveillance of DG movement across the geographic area under their jurisdiction in and cross-border context. The stakeholders and even the end customers require information for the physical flow of goods from the departure point to the destination point. To have access to a such information, the establishment of a traceability mechanism is required. Traceability is the possibility to track and trace the history, administration, or location of the DG located in the warehouse or during transportation [2]. Tracking and tracing the information of the active and passive processes in the TDG enhances monitoring and auditing aspects. The active traceability makes it possible to know the exact location of the DG that is in transit. The passive traceability enables the inquiry of any possible information regarding the completed process in TDG.

To manage the traceability aspects, we present the concept of *digital certificate.* The *digital certificate* is established at an early TDG planning phase, before transport starts, by gathering the necessary information, as shown in Sect. 3. The *digital certificate* remains valid during and after the transport process. It contains significant information articles for the TDG. Instances of such information includes "ID_DG_Process," "ID_DG_Provider," "ID_DG_Receiver," "ID_DG_Transporter (Sub_Contractors_ID)," "ID_DG_Good," "loading, quantity at departure (or arrival)," "risk level (sensitivity)," "Truck _ID," "Container_ID," "ID_IoT_ Devices," and "Timestamp."

Additionally, we introduce the article "ID_IoT_Devices" representing the set of all IoT devices that are part of our TDG control system. The IoT device allows for capturing digital information from physical objects (truck, containers), provides real-time information for the geographic location of DG, and measures the DG state inside the truck. In [7], we presented an extensive study on the integration of blockchain and IoT. Furthermore, the "Container_ID" identifies any container (or other types of the load of DG), while "Truck_ID" presents the identification of the truck that transports the DG. In a single transport process, there might be several trucks involved. The "timestamp" identifies the date and time of any activity involving the DG. The aforementioned information articles remain available and are updated during the process flow. New values are captured and appended in the *digital certificate* articles based on "local information push" and "real-time" information flow. At any time, the authorized stakeholders may retrieve the *digital certificate* with all the information during an end-to-end process. The information retrieval is further shown in the Merkle-tree style (BC data structure). At a high-level view, the *digital certificate* concept presents a virtual *sub-ledger* formed from the global ledger. It presents an interactive component that allows new information articles to be added based on the need for that information. We propose using SC to gather and store this information as a segregated sub-ledger, maintaining the transaction history for an end-to-end process.

Figure 4 illustrates the concepts of a *digital certificate* in an end-to-end transport. As shown here, the certificate is established with significant information articles

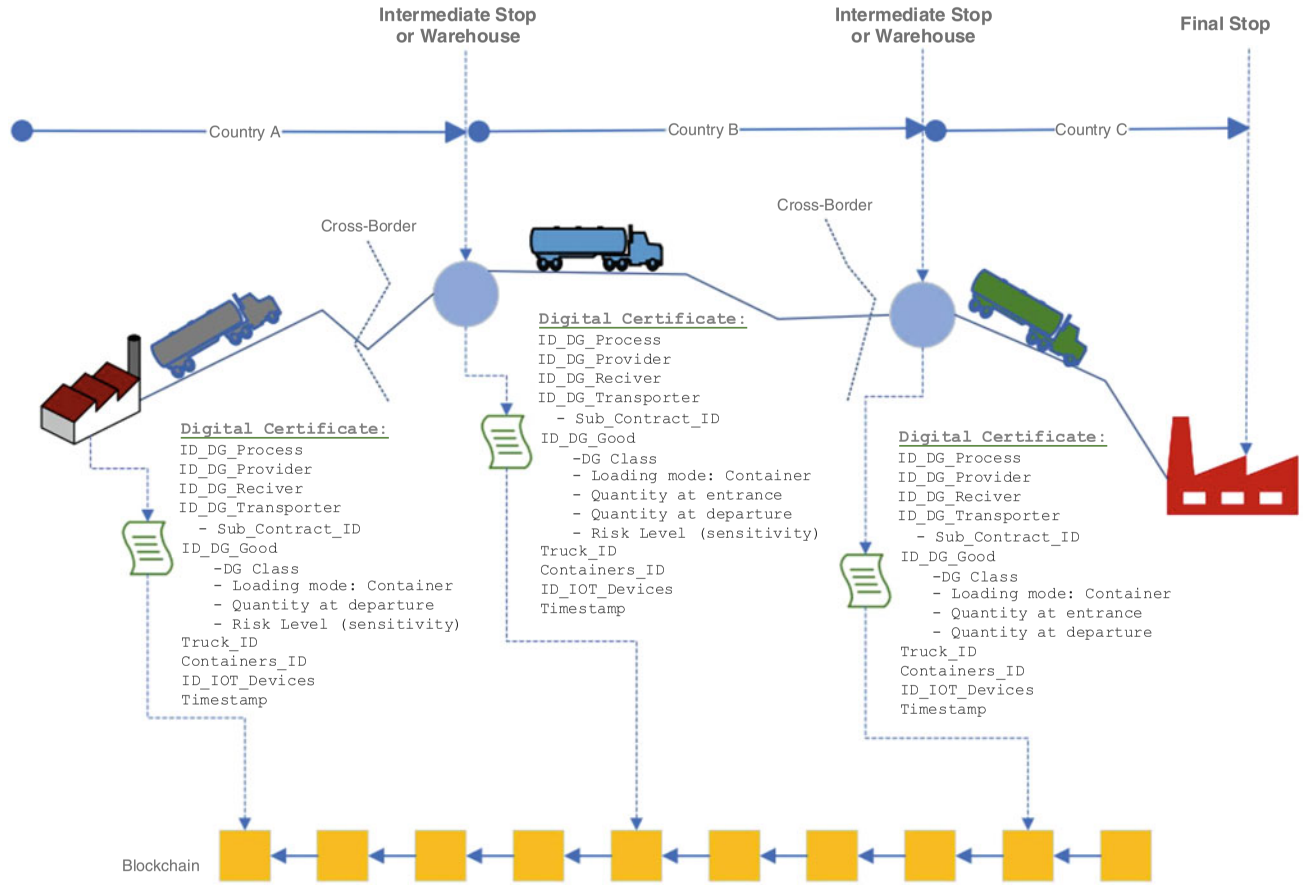

Fig. 4 The concept of digital certificate for digital traceability and management of DG

at the departing point in the transport process. It gathers previous information known from the certification of the stakeholder process and authorization and combines additional detailed information for the transport process. There might be intermediate stops[6] during the transport process in different countries (e.g., from country A to country B). At any entry on the intermediate stop, the *digital certificate* is updated with the last (on the push and real-time) information. The intermediate stop might play the role of warehousing the DG, meaning that the transport will not continue immediately, and the DG received remains stored there for a certain time. The *digital certificate* remains open for this process, identified by articles "ID DG Process." After a certain time, the same DG may be moved to another warehouse or directly to the destination point. It uses the same *digital certificate* to continue the process and update it accordingly.

We formally present some parameters, that is, quantity that we consider continuously in the *digital certificate* with the help of SC.

Consider we have the set of DG noted D.

$$(\forall d \in D)\,(\exists\, quantity\,(d) = \epsilon) \xrightarrow{transportation} (\forall d \in D)\left(\exists\, quantity\,(d) = \left(\epsilon' \vee \epsilon\right) \wedge \left(\epsilon \neq \epsilon'\right)\right) \tag{1}$$

In the Eq. (1), the ϵ signifies DG quantity (ϵ' - different quantity). After transporting and warehousing DG, the quantity may differ from its initial measure. This signifies that either the DG is separate in other quantities or used partially (if the warehouse is the destination point). The *digital certificate* calculates these quantities and keeps the ledger updated. Even in the situation in which the separated part is transported to other stakeholders (may be located in other countries), which might be repeated several times (by subcontracting other certified transporters), it still keeps that information until the end of the life cycle of the DG. That highlights aspects of monitoring and control for DG, even if they are separated into smaller quantities. The final step on the digital certificate counts k-parts as the sum of entire quantity of DG ($\epsilon = \epsilon_1, \epsilon_2, \ldots, \epsilon_k$, thus $\epsilon = \sum_i^k \epsilon_i$) from its departure until its treatment. Formally and empirically, that is the first indication that the DG is treated according to the regulatory framework and not misused (thrown in open land or sea).

The digital representation of DG and its characteristics through *digital certificate* enhance the management aspect in TDG. We refer to the ability to manage some characteristics of DG digitally as *digital management*. The *digital management* aspects provide stakeholders with extensive information for the current capacity, type, and related storage information for the DG in the warehouse. Based on that information, they might decide if they possibly host additional quantities of the DG or not. Furthermore, the digital information for the DG distributed in several warehouses allows stakeholders to have the most relevant information about their DG capacities circulation under their ownership. In the context of *digital*

[6] Contrary to the warehouse where DG is stored for a longer time, the intermediate stop is used for driver exchange or rest, and in terms of time, it takes several minutes until to H hours.

management, the information is received digitally. Unlike paper-based approaches, we measure the temperature (or humidity) of the arriving DG and write it on paper. In the paper-based approach, after a certain time, there is not only the disadvantage of one-time temperature measures on arrival, but also there is no mechanism to prove that the temperature was as it is written on the paper. Moreover, there is no way to return on that particular day (or hour) and verify the process flow with empirical data. The *digital management* provides digital information in the end-to-end process. Monitoring the state of DG is during the entire end-to-end process enhances quality control aspects and improves the management aspects of the process, and in addition, it can be verified at any time. Awareness of the current location of the DG and its condition is managed through the TDG control system. This tracking and tracing feature allows quick response in case of emergencies identified autonomously by the IoT devices or by manual alerting (by information push). In both cases, the system provides information to the involved authorities and the emergency response teams.

6 Proof of Concept (PoC): Smart Contract for Digital Certificate

This section aims to show details of the initial proof of concept (PoC) implementation for blockchain-based *digital certificate.*

To evaluate our approach, we used Hyperledger Fabric (HF) Go Lang SDK [41] for implementing the PoC. Our approach proposes a collaborative architecture that allows different stakeholders to join the network and share information based on their operations in TDG. This architecture enables future prospective stakeholders to join the network continuously. To achieve that, we deploy HF-based architecture, which further allows us to develop TDG system components. In this solution, we assume that all the involved stakeholders are allowed to access all information. Thus, we share all this information in a single channel, named *"Global Channel TDG."* Figure 5 shows the architectural organization of the proposed solution. The network is composed at last of four blockchain nodes (knows as *peers* in HF jargon), that is, "DG Receiver," "DG Transporter," "DG Provider," and "Authorities." These nodes use the *"Global Channel TDG"* as a communication channel to exchange information for TDG.

To draw attention to the business logic of the *digital certificate*, we developed SC called *SC_Digital_Certificate.* It is installed (deployed) in the *"Global Channel TDG,"* operates actively on the shared channel, and collects information according to the TDG process stage. Collecting and sharing a particular set of information, the *SC_Digital_Certificate* formalizes a mini-ledger for each DG, thus composing the *digital certificate.* Listing 1.1 presents a small code partition of the *SC_Digital_Certificate,* while the complete code is shown in [42].

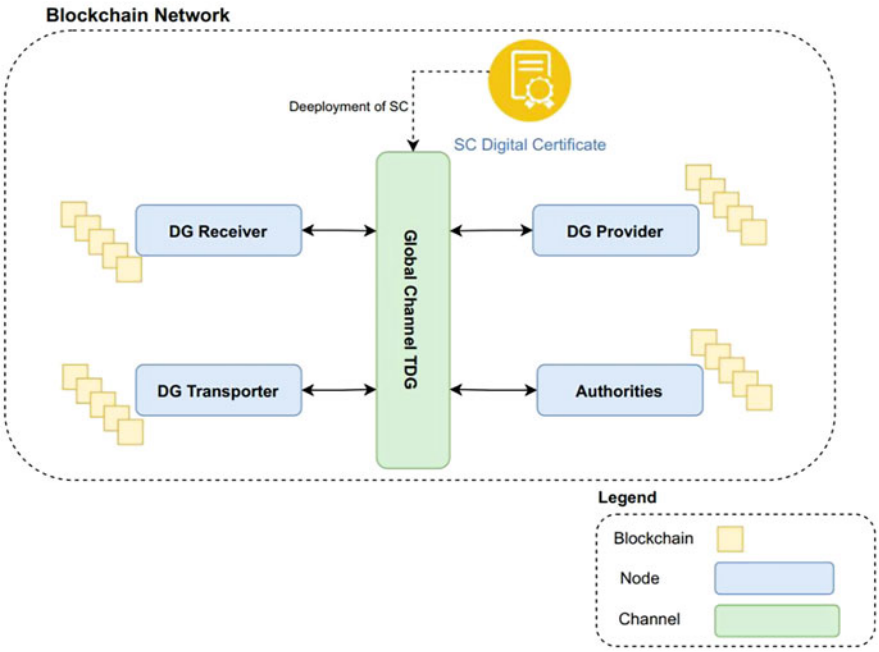

Fig. 5 The network of BC-based stakeholders in TDG

For accessing and testing the digital certificate SC, we have specified an API[7] which enables us to interact with the *digital certificate.* This interaction allows us to retrieve the information that is listed in the *digital certificate.* Listing 1.2 shows the information retrieved from the *digital certificate* in JSON format. The components "id_Certificate":ID_0006101 identifies uniquely the *digital certificate* for curtain DG (or process, identified "id_DG_Process":ID_DG_0011658. In an end-to-end process, the information received is continuously added in the *digital certificate* parameters, thus forming a completed ledger of transaction related to a specific DG associated with a specific process, that is, "id_DG_Process":ID_DG_0011658. The information stored in the digital certificate also serves as a referential point for the other SCs, which are complementarily implemented to support the TDG system. For example, by receiving the information from IoT devices, in case of the temperature, for example, "id IoT Temp Data": +33.11 °C passes the risk level "risk-Level":T + 31 °C, then another SC is triggered to notify the relevant stakeholders for a possibly disastrous situation. Similarly, it maintains trace on the quantity of DG in the departure point, that is, "quantity_At_Departure":6.5 liters/ton, then it checks the quantity at "quantity_At_Entrance" in the warehouse

[7] Application programming interface for GO: https://github.com/hyperledger/fabric-contract-api-go

of at the destination point. That helps to audit the process and being aware of how the DG are distributed among several stakeholders for treatment or are treated at a single destination point.

```
type Certificate struct {
ID_Certificate string `json :"id_Certificate"`
ID_DG_Process string `json :"id_DG_Process"`
ID_DG_Provider string `json :"id_DG_Provider"`
ID_DG_Receiver string `json :"id_DG_Receiver"`
ID_DG_Transporter string `json :"id_DG_Transporter"`
Sub_Contract_ID string `json :"sub_Contract_ID"`
ID_DG_Good string `json :"id_DG_Good"`
DG_Class string `json :"dg_Class"`
 Loading_Mode string `json :"loading_Mode"`
 Quantity_At_Entrance string `json :"quantity_At_Entrance"`
 Quantity_At_Departure string `json :"quantity_At_Departure"`
 Risk_Level string `json :"risk_Level"`
 Truck_ID string `json :"truck_ID"`
 Container_ID string `json :"container_ID"`
 ID_IoT_Devices string `json :"id_IoT_Devices"`
 ID_IoT_Devices_Data string `json :"id_IoT_Devices"`
 Timestamp string `json :"timestamp"`
 }
 /*...more lines of code ... */
 func (s *SC_CERTIFICATE) CreateCertificate(ctx contractapi.
  TransactionContextInterface, certificate string) (string,
 error){

 var dg_process_certificate Certificate

 /*...more lines of code ... */

 if process_certificate != nil {
 fmt.Printf("the certificate already exist with ID %s",
 dg_process_certificate.ID_Certificate)
 return "The certificate already exists", err
 }
 /*...more lines of code ...*/

 func (s *SC_CERTIFICATE) UpdateCertificate(ctx contractapi.
TransactionContextInterface ,certificate_updated string) error {

 /*... more lines of code ... */
```

Listing 1.1 The short representation of code for SC Digital Certificate

```
{"id_Certificate":"ID_0006101",
"id_DG_Process":"ID_DG_0011658",
"id_DG_Provider":"Esch Hospital",
"id_DG_Receiver":"EcoGroup Swiss",
"id_DG_Transporter":"AGI Transport Group",
"sub_Contract_ID":"--",
"id_DG_Good":"DG611768",
"dg_Class":"6.1",
"loading_Mode":"container",
```

```
10    "quantity_At_Departure":"6.5 liters/ton",
11    "quantity_At_Entrance":"6.5 liters/ton",
12    "risk_Level":"T+31C",
13    "truck_ID":"TR006987",
14    "container_ID":"CO698774",
15    "id_IoT_Temp":"TempIoT:DHT11DG",
16    "id_IoT_Temp_Data":"+20.17C",
17    "id_IoT_Location":"EM-506RE"
18    "id_IoT_Location_Data":"49.497509, 5.982500"
19    "timestamp":"14/05/2021 17:01:12"}
```

Listing 1.2 The representation of the digital certificate in JSON format

7 Conclusion and Future Works

Transparency and traceability are critical properties in numerous supply chains. Similarly, in TDG, transparency is highly required from the involved stakeholders, particularly from the authorities as the responsible party to govern this process. In this work, we present the concept of the digital certificate, which enables storing and maintain information for an end-to-end TDG. The digital certificate proposes an active and dynamic mini-ledger that allows continuous monitoring of the DG state. In TDG, there are specific parameters (temperature, humidity) that need to be kept under control to avoid adverse situations. We propose a blockchain-based digital certificate to maintain the TDG process and actively update its state according to the information received from IoT devices or stakeholders. The proposed digital certificate is dynamic, and it is associated with a specific DG, thus enabling the digital management of DG. The dynamicity remains on selection, sharing, and triggering other events with the help of different SC. At the TDG process run-time, collecting this information in real-time enables monitoring the TDG process by responsible stakeholders. The digital certificate enables TDG process audit, thus at any time, the relevant (authorized) stakeholders in TDG can request specific information to verify the correctness of the process.

In the actual pandemic of COVID-19 [43], safe transportation of vaccine is crucial. The issue with the COVID-19 vaccine transportation is the maintenance of low-rate temperature degree, which may expose several risks if the temperature is not maintained in the range of "normality." In such a situation, to improve transparency, it must have real-time information that remains immutable during the end-to-end process. Thus, the digital certificate would add value to improving transparency since the received real-time information remains immutable.

We consider the proposed approach a contribution to the transparency in supply chain by storing almost dynamically information on the blockchain. In future works, we intend to extend the operation scale of our approach by extending the number of involved stakeholders and providing large-scale IoT devices.

References

1. Lukasik, Z., Kúsmińska-Fija'lkowska, A., & Kozyra, J. (2017). Transport of dangerous goods by road from a European aspect. *Zeszyty Naukowe. Transport/Politechnika Slaska*.
2. Imeri, A., & Khadraoui, D. (2018). 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),* 1–5. IEEE.
3. U. N. E. C. for Europe (UNECE). (2020, Nov 19). Agreement concerning the international carriage of dangerous goods by road (ADR 2021). In *European Agreement Concerning the International Carriage of Dangerous Goods by Road (ADR)*.
4. Ding, L., Chen, Y., & Li, J. (2016). Monitoring dangerous goods in container yard using the internet of things. *Scientific Programming*, 1–25.
5. Mentzer, J. T., et al. (2001). Defining supply chain management. *Journal of Business Logistics, 22*(2), 1–25.
6. Li, Q., & Liu, A. (2019). Big data driven supply chain management. *Procedia CIRP, 81*, 1089–1094.
7. Imcri, A., Agoulminc, N., & Khadraoui, D. (2020). Blockchain and IoT integrated approach for a trusted and secured process to manage the transportation of dangerous goods. *Revista de Sistemas e Computaç ão-RSC, 10*(1), 26–41.
8. Imeri, A., Khadraoui, A., & Khadraoui, D. (2017). A conceptual and technical approach for transportation of dangerous goods in compliance with regulatory framework. *JSW, 12*(9), 708–721.
9. European agreement concerning the international carriage of dangerous goods by inland waterways: (ADN) including the annexed regulations, applicable as from 1 January 2017. volume 1: OCLC: 992936978.
10. RID. Intergovernmental organisation for international carriage by rail (RID). (2019, Jan). https://otif.org/en/?pageid=1105. Accessed on 02/15/2020.
11. OTIF. International martime organization (imdg) code. (2019, Jan). https://www.iata.org/en/publications/dgr/. Accessed on 02/15/2020.
12. IATA. (2017, Jan). Dangerous goods regulations. https://www.iata.org/en/publications/dgr/. Accessed on 02/15/2020.
13. Torretta, V., Rada, E. C., Schiavon, M., & Viotti, P. (2017). Decision support systems for assessing risks involved in transporting hazardous materials: A review. *Safety Science, 92*, 1–9.
14. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 75–105.
15. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77.
16. Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. *MIS quarterly,* 37–56.
17. Imeri, A., Agoulmine, N., Feltus, C., & Khadraoui, D. (2019). 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* (pp. 474–493). Springer.
18. March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251–266.
19. de Noimalizacio'n, O. I. (2011). ISO-IEC 25010: 2011 systems and software engineering systems and software quality requirements and evaluation (SQuaRE)-system and software quality models. *ISO*.
20. Feltus, C., Khadraoui, D., De Remont, B., & Rifaut, A. (2007). Business governance based policy regulation for security incident response. *Crisis*, *7*.
21. Imeri, A., Agoulmine, N., & Khadraoui, D. (2019). A secure and smart environment for the transportation of dangerous goods by using blockchain and IOT devices. In *7th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2019),* 1–8.

22. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375.
23. Antonopoulos, A. M. (2014). *Mastering bitcoin: Unlocking digital cryptocurrencies*. O'Reilly Media, Inc.
24. Nguyen, G.-T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information Processing Systems, 14*(1), 101–128.
25. Bouraga, S. (2021). A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Systems with Applications, 168*, 114384.
26. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE international conference on software architecture (ICSA),* 243–252. IEEE.
27. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering, 59*(3), 183–187.
28. Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: Implications for operations and supply chain management. *Supply Chain Management: An International Journal*, 469–483. https://eprints.lancs.ac.uk/id/eprint/131605/
29. Kumar, R. & Tripathi, R. (2019). Traceability of counterfeit medicine supply chain through blockchain. In *2019 11th International Conference on Communication Systems & Networks (COMSNETS),* 568–570. IEEE.
30. Helliar, C. V., Crawford, L., Rocca, L., Teodori, C., & Veneziani, M. (2020). Permissionless and permissioned blockchain diffusion. *International Journal of Information Management, 54*, 102136.
31. Nakamoto, S. (2019). Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot.
32. Venkatesh, V., Kang, K., Wang, B., Zhong, R. Y., & Zhang, A. (2020). System architecture for blockchain based transparency of supply chain social sustainability. *Robotics and Computer-Integrated Manufacturing, 63*, 101896.
33. Brousmiche, K. L., Heno, T., Poulain, C., Dalmieres, A., & Hamida, E. B. (2018). Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned. In *2018 9th IFIP international conference on new technologies, mobility and security (NTMS)*, 1–5. IEEE.
34. Notheisen, B., Cholewa, J. B., & Shanmugam, A. P. (2017). Trading real-world assets on blockchain. *Business & Information Systems Engineering, 59*(6), 425–440.
35. Liu, X., Wang, W., Guo, H., Barenji, A. V., Li, Z., & Huang, G. Q. (2020). Industrial blockchain based framework for product lifecycle management in industry 4.0. *Robotics and Computer-Integrated Manufacturing, 63*, 101897.
36. Martin, M. First ever European certificate of origin through blockchain — business west. https://www.businesswest.co.uk/blog/first-ever-european-certificate-origin-through-blockchain, 06 2018. Accessed on 05/08/2021.
37. Wu, H., Li, Z., King, B., Ben Miled, Z., Wassick, J., & Tazelaar, J. (2017). A distributed ledger for supply chain physical distribution visibility. *Information, 8*(4), 137.
38. Lu, Q., & Xu, X. (2017). Adaptable blockchain-based systems: A case study for product traceability. *IEEE Software, 34*(6), 21–27.
39. Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management, 25*(1), 18–27.
40. Imeri, A., Khadraoui, D., & Agoulmine, N. (2019). Blockchain technology for the improvement of SCM and logistics services: A survey. In *Industrial engineering in the big data era* (pp. 349–361). Springer.
41. Fabric, H. Introduction — hyperledger-fabricdocs main documentation. https://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html. Accessed on 05/09/2021.
42. Imeri, A. Smart contract codes. https://git.list.lu/adnan_imeri/thesisaimeri/-/blob/master/SmartContractCodes/SC_Digital_Certificate_DG. Accessed on 05/14/2021.
43. County-Level COVID-19 Vaccination coverage and social vulnerability — united states, December 14, 2020–March 1, 2021. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7993557/. Accessed on 05/15/2021.