IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received November 4, 2019, accepted December 6, 2019, date of publication December 18, 2019, date of current version December 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960542

A Survey on Using Blockchain in Trade Supply Chain Solutions

HUSSAM JUMA[1,2], KHALED SHAALAN[1], AND IBRAHIM KAMEL[3]

[1]Dubai Customs, Dubai, United Arab Emirates
[2]Faculty of Engineering and Information Technology, The British University in Dubai, Dubai, United Arab Emirates
[3]Department of Electrical Engineering, Sharjah University, Sharjah, United Arab Emirates

Corresponding author: Hussam Juma (hussam.mohammed@dubaicustoms.gov.ae)

This work was supported by the Dubai Customs.

ABSTRACT Blockchain has emerged as a promising technology to ensure trust between parties. By using this technology, we can establish a secure communication paradigm, where data integrity and immutability can be guaranteed. These inherited features underline blockchain as a suitable technology to optimise the adopted processing model in several domains, such as health, trade supply chain and food safety. In this paper, we present a detailed overview of the use of blockchain technology in (international) trade supply chains. Furthermore, the discussed proposals have been classified based on the target application scenarios. Our goal is to clarify the benefits of applying this technology to the trading domain and highlight the challenges that are associated with applying this technology to optimise the trading domain. Accordingly, we underline several issues that occur during the designing of the blockchain solution to optimise the (international) trade supply chain.

INDEX TERMS Blockchain technology, distributed ledger, Dubai customs, trade supply chain, world customs organization.

I. INTRODUCTION

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

The complexity of the trading process increases significantly in the international trading scenario. International trade involves many parties, mainly including the trading community (importers and exporters), customs agency, shipping agent, port operators, freight forwarders, and customs brokers. The freight forwarders arrange shipments for customers. The shipping agents usually deal with the transportation of cargo. A customs broker usually is responsible for the preparation of the shipment declaration information, which will be submitted to the customs agency. During the trade, each of the involved entities performs its task based on the documents that are provided by other entities in the trade supply chain. For instance, the customs process the declaration application submitted by the broker, and then send its result, the clearance, to the next entity in the supply chain.

In the international trade supply chain, the employed information sharing mechanism is also a dominant factor in determining the overall efficiency of the supply chain. In this trading domain, several entities require access to

The associate editor coordinating the review of this manuscript and approving it for publication was Jenny Mahoney.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

the documents from the different participants in the supply chain in a timely manner. A key document's dependent entity in this supply chain is the customs authority, which plays an important regulatory role. Customs authority acts as the gate that protects society and the economy. The protection task is established by monitoring the flow of goods entering the country to detect counterfeit products and smuggling activities. To fulfil this task, customs authority relies on the information provided by several participants in the international trade supply chain. This information is used in the shipment clearance process to examine the shipment under consideration and to determine if a physical examination is required [1].

The issue of ensuring the integrity of the exchanged information can be addressed by providing a traceable secure system that allows the trade participants to gain access to the data (document) in a timely manner. In this system, once a document is submitted, participants gain access to this document based on their role in the trade model. Additionally, the system must be able the provide the users with the ability to trace the status of the shipment through the entire trade supply chain model. Towards this end, several proposals [2]–[8] have investigated the use of blockchain technology to optimise the (international) trade supply chain. Blockchain technology has revolutionised the manner in which trust can be established between entities. Thus, the participants of the trade supply chain can share their information without any privacy concern. Blockchain is Distributed Ledger Technology (DLT) in which records (data) are stored in block format, where these blocks are linked (chained) using cryptography [9], [10]. Blockchain technology can ensure the traceability and integrity of the shared data between the participating entities. These inherited features highlight the potential of optimising the trade supply chain through the use of blockchain technology.

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

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

The rest of this paper is divided as follows. In section II, we present background information about blockchain technology and the rule of the customs administration in the international trade supply chain. Section III describes the methodological approach applied in this work. In section IV, we present our categorisation of the blockchain-based solutions for the trading domain, which is followed by a detailed discussion of these proposals, and our findings. This paper is concluded in section V.

II. BACKGROUND

In this section, we start by giving a brief description of blockchain technology. Then, we describe the impact of blockchain technology on simplifying the international trade supply chain, and the related customs administration processes.

A. BLOCKCHAINS

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

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

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

Blockchain solutions can be categorised into two main types: public blockchains and private blockchains.

1) PUBLIC BLOCKCHAINS

Public blockchains (e.g., Ethereum [11]) are typically described as a permissionless blockchain, whereas anyone has permission to write new transaction (record) to the blockchain. Having the ability to interact with the blockchain in permissionless fashion introduce significant

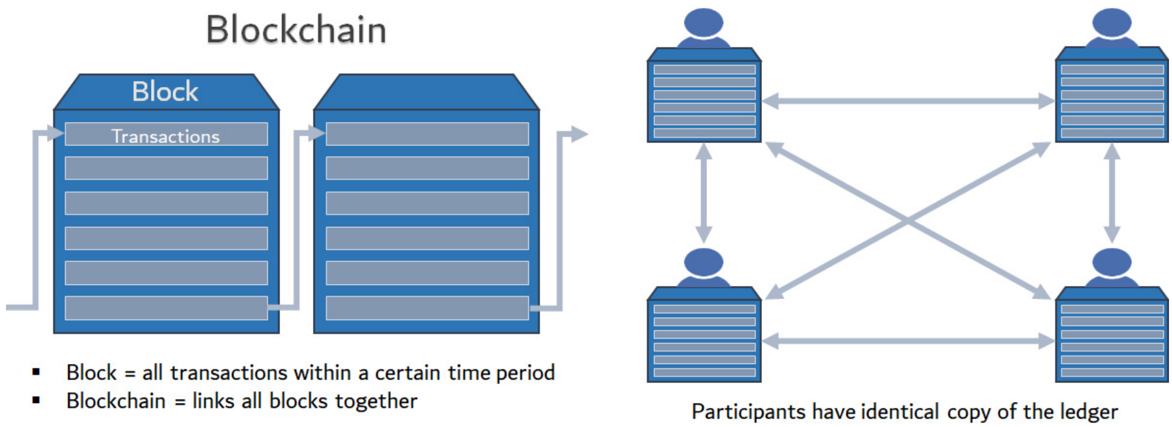

FIGURE 1. Blockchain and ledger architecture.

pressure on the consensus mechanism. Therefore, strong consensus mechanism such as Proof-of-Work (PoW) and Proof-of-Stack (PoS) [12] are required to ensure the privacy and integrity of the data. Additionally, to establish some trust between the participants, all participants in this type of blockchain, must have the same authority (privileges). This decentralisation of the authority privileges is crucial since in such environment no participant(s) should be able to control the blockchain.

2) PRIVATE BLOCKCHAINS

In a private blockchain (e.g., Hyperledger Fabric [13]), only a subset of the entities (participants) have permission to write new records to the blockchain, and such a blockchain type usually is described as a permissioned blockchain. The identities of the participants in a private blockchain are known to each other, where we expect to have a single participant with administrative privileges. In this type of blockchain, the administrative participants register the other participants and determine their blockchain access permission. The presence of the administrative entity results in categorising a private blockchain as centralised in terms of authority privilege since the entity with the administrative right can control the blockchain.

Additionally, having administrative participant(s) reduces the security pressure, as a rule, to be followed by each participant on the blockchain is pre-determined and the administrative participants monitor the flow of information in the blockchain. Therefore, a simplified consensus mechanism such as Proof-of-Authority (PoA) [12] can be implemented here. A consortium blockchain is similar to a private blockchain; however, in this blockchain, a consensus mechanism is performed by a pre-determined approved set of participants.

3) SCALABILITY

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

In this section, we presented the general categorisations, which usually are used to describe any blockchain solution. However, these categorisations do not represent absolute values. In other words, being a permissioned or permissionless blockchain is not an 0-1 value. For instance, if we describe a blockchain solution as a permissioned blockchain, this means that the overall solution architecture has a permissioned behaviour. In this solution, small components might have permissionless behaviours, but they do not influence the overall behaviour.

B. INTERNATIONAL TRADE AND BLOCKCHAIN

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

1) IMPORTATION

Figure 2 presents the steps of the importation scenario by sea; other methods of transportation (air and land) follow relatively the same steps. In this trading domain, a large number of documents are exchanged between the trade supply chain entities. The figure shows the identity of the participants for this international trade supply chain. Once the importer and

FIGURE 2. The international trade supply chain (sea transportation).

the exporter have agreed on the payment method, the exporter provides the importer with the following documents:

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

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

2) CUSTOMS CLEARANCE AND BLOCKCHAIN

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

Such an objective can be achieved by establishing blockchain-based information-sharing mechanism between the trade supply chain participants. In such a domain, a private blockchain network can be used to connect the (international) trade supply chain participants [14]–[17]. Thus, the involved participants (stakeholders) for any shipment can have direct access to the exchanged document. In such a network, using smart contracts, we can automate the process of validating and authenticating the trade documents. In addition, by connecting all of the involved participants to the network, we can simplify the auditing process, since the correctness of the documents has already been established.

III. RESEARCH METHODOLOGY

To address the research questions proposed in this work, we have conducted a detailed review and discussion about the use of blockchain technology in trade. Our review adopts the methodological approach proposed by Tranfield *et al.* [18], which mainly consists of three main steps: planning, execution, and reporting. In the planning step, we determine the search keywords and the protocol for execution. In addition, we determine the databases to execute our search. In the execution step, we follow the planned protocol to obtain the desired articles and information. In the reporting step, we address the presented question in this work, by discussing all factors that influence the question's solutions. Next, we describe the planning and execution steps, where the reporting step is described in the next section.

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

A. PLANNING

The search criteria are designed to help in addressing the research questions presented in this work. Accordingly, the main terms that are used in the research questions have also been used in the search criteria. These terms are ''trade supply chain'', ''blockchain'', ''customs'', ''trade monitoring'', ''counterfeit trade'' and ''trade facilitation''. In any of the performed search, the format of the search words can be represented as follows <blockchain and ANY>, where blockchain as a term must be included in addition to any other term(s). In this paper, we have included peer-reviewed papers and working papers. The latter type of papers is normally generated from industrial corporations. In terms of peer-reviewed papers, we have focused our search on the following databases: IEEE, ACM, scientist Direct, Scopus, Springer, and Taylor and Francis. Working papers are included in our work only if they address customs administration processes or originated from major industrial companies such as IBM [19] or Deloitte [14].

B. EXECUTION

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

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

Additionally, for each application scenario, we limited the number of papers discussed to five. However, for papers dealing with customs administration-related processes, no limit was applied. This limitation was imposed to reduce the probability of discussing papers that share more or less the same main concept. In addition, proposals that addressed customs administration-related processes were the only set of proposals that required a full discussion of the objective of the work. Other proposals are presented to fill the gap in terms of blockchain and the trade supply chain. At the end of this selection process, we were focusing mainly on 34 papers.

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

IV. BLOCKCHAIN AND TRADE SUPPLY CHAIN (REPORTING)

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

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

In this direction, towards addressing the first research question (RQ1), which is related to the impact of the blockchain technology on the trade supply chain, we start the presented discussion by categorising the discussed proposals (34 papers) as follows (Figure 3 summarises this classification):

- **Electronic trading solutions**: these solutions normally provide online trading platforms. The characteristics of these platforms underline a public blockchain as a suitable deployment environment since all participants will have the same level of authority.
- **Validation solutions**: These solutions are typically deployed on a private blockchain. In general, they are designed to address highly regulated trading processes. For instance, solutions that are proposed to prevent

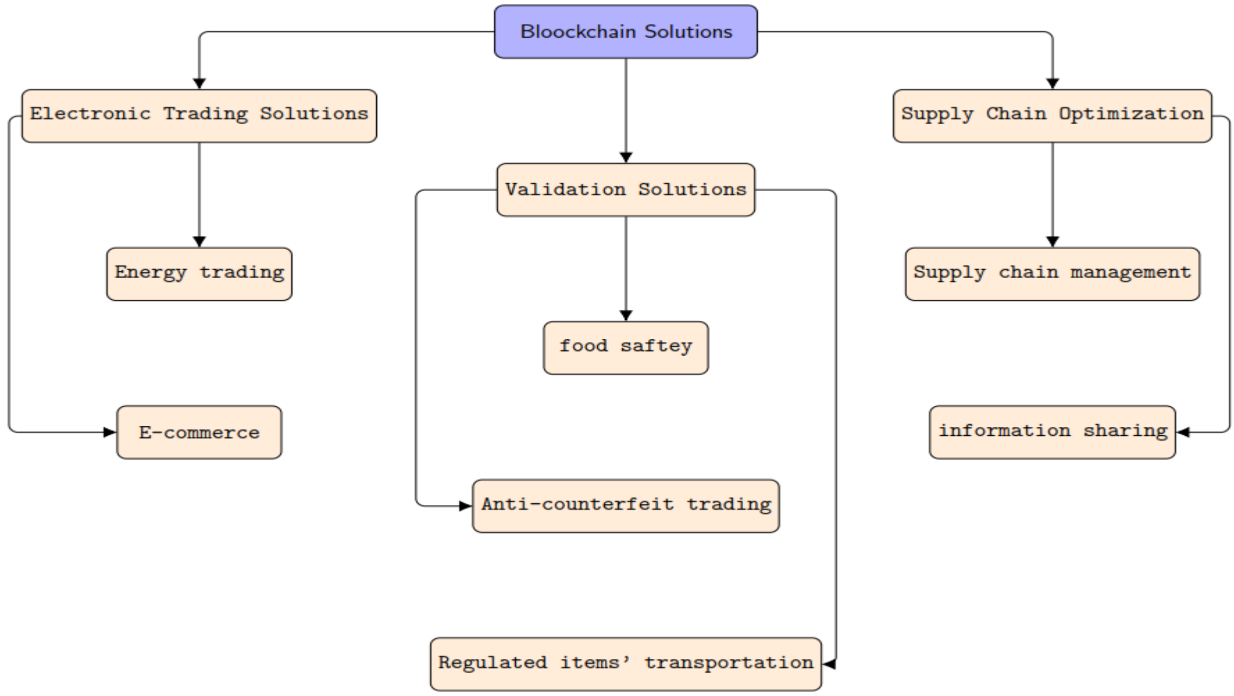

FIGURE 3. Classification for blockchain solution in the trading domain.

fake goods trading are normally deployed in a private blockchain, since the participants in such a blockchain are expected to be part of the supply chain, where each participant has predetermined permission.

- **Supply chain management solutions:** These solutions are designed to optimise the overall supply chain management. As for this category, we also discuss proposals that aim to optimise a single functionality in the trade supply chain. In general, we expect such solutions to be deployed on a private blockchain since public customers are not expected to interact with such processes. However, in situations where the target processes are designed to address customer requirements of the general public, a public blockchain could be a suitable deployment environment.

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

- Blockchain type (public / private / consortium).
- Authority distribution (centralised / decentralised).
- Accessibility (permissioned / permissionless).
- Scalability (number of transactions).

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

A. ELECTRONIC TRADING SOLUTIONS

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

1) ENERGY TRADING

Several proposals have investigated the use of blockchain for energy trading in Industrial Internet of Things (IIoT) [20]–[23]. Typically, in IIoT, energy trading is performed using one of the following strategies: (1) Microgrids, (2) Energy harvesting networks, and (3) Vehicle-to-grid networks. In microgrids, groups of smart buildings with renewable energy tools construct a grid and trade electricity among the group members in a P2P manner. In energy harvesting networks, nodes with renewable energy sources also charge each other in P2P manner. In vehicle-to-grids networks, vehicles represent mobile electricity storage devices, which can charge other vehicles or the grid itself. In such trading environments, trust and privacy are major issues, and, in this direction, Li et al. [20] proposed blockchain-based secure energy trading system for IIoT. This system mainly consists of five parties: (1) energy nodes, (2) energy aggregators, (3) transaction server, (4) wallets, and (5) smart meters. The energy nodes form the network (e.g., smart buildings and electric vehicles in the above examples). Energy aggregators work as brokers to facilitate the trade between the seller nodes and the buyer nodes. The transaction server is used to record the buying request and send them to the nearest aggregator node. Each energy node has a wallet, which stores the number of energy coins that this node owns. In each node, the smart meter is used to calculate the amount of the traded electricity.

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

To address the problem of determining the trading price, Mengelkamp *et al.* [22] proposed a conceptual auction-based approach that targets energy trading between smart buildings. To ensure the privacy and integrity of the trades' transactions, the authors employed the blockchain technology to ensure the traceability and privacy of the transactions. To address the trading scenario, the authors employed a bidding mechanism to determine the trading price. Accordingly, this work presented an analytical study to investigate market behaviour. Liu et al. [24] focused on the problem of minimising the fluctuation levels in the grid. Accordingly, they proposed a blockchain-based algorithmic approach to improve the overall charging and discharging strategies. To test their approach, the authors deployed their solution on a public blockchain (Ethereum), where the results showed that the proposed solution could minimise the power fluctuation level.

Similar to any other trading platform, data integrity (security) and privacy are major challenges in energy trading. Thus, several proposals have also investigated the optimisation of the security mechanisms in this trading domain [25], [26]. In situations where an identification process is applied to identify the energy nodes before commencing the trade, the actual trading process will be done in a relatively semi-private manner, which reduces the security challenge because all parties are known as a priori. Additionally, in such trading domain, employing a fairness mechanism by exploring the traceability feature of the blockchain technology is expected to improve the stability of the system.

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

2) E-COMMERCE

Similar to energy trading, e-commerce trade involves typically three parties: the seller, the buyer, and the trading platform. In this type of trade, the platform aims to ensure that the trading agreements' conditions are satisfied, where the agreements' validation process in e-commerce trading is more advanced than the validation process in energy trading platforms. This is because the energy trading platform deals with one type of commodity (electricity), whereas in e-commerce platforms, any good can be traded. E-commerce trading can be categorised mainly into the following [27]: (1) Business-to-Consumer (B2C), (2) Consumer-to-Consumer (C2C), (3) Business-to-Business (B2B), and (4) Business-to-Government (B2G). Compared to B2C and C2C, the number of trades on a daily basis is expected to be relatively smaller in B2G and B2B. In addition, in B2G and B2B, the identity of the traders are expected to be confirmed before commencing the trades. This is established, as in these trading scenarios, the seller company (business) typically provides the company (or government department) that acts as a buyer with credential information (user-name and password) to its platform.

In contrast, in B2C and C2C, there is no actual precise mechanism to identify the traders, and, typically, any public user should be able to access the trading platform. Therefore, in B2C and C2C, scalability and privacy is a fundamental challenge. In B2B and B2G trading domains, the focus is typically on optimising the trading process to improve the trading experience. Usually, blockchain-based e-commerce solutions consist of three types of participants: verifier, participant, and supervisor [28]. A verifier is responsible for ensuring the correctness of the transactions before they are written on the blockchain. A participant represents the sellers and buyers. A supervisor is a trusted third-party node that ensures that the trade conditions are satisfied.

Pittl et al. [29] presented a trading platform termed as Bazaar-Blockchain, which is an improved version of Bazaar-Extension [30]. This trading platform can be recognised as an e-commerce platform designed for cloud environments, and it allows the customer and the cloud service provider to negotiate the price and the terms of deals. Generally, the status of an offer between the customer and the cloud service provider can be advisory, solicited, accepted, or rejected [31].

Offers that are flagged as advisory require further negotiation, and solicited offers are fully specified. Acceptable offers become binding after both parties sign their agreements. Using blockchain technology, Bazaar-Blockchain is implemented as an extension of the CloudSim simulator. Bazaar-Blockchain aims to increase the scalability and the data integrity of the negotiation process. However, in such a market, any proposed approach should address the scalability requirement, as demand and supply can vary significantly over time.

To address the privacy concerns in e-commerce trading, Min et al. [32] proposed the Peer Blockchain Protocol (PBP). This protocol uses several types of blocks to ensure overall system security. First, the transaction is written on peer micro-blocks. Once validated, these peer-blocks are aggregated to construct peer key-block. In any interval of time, the number of the generated peer key-blocks is significantly lower than the number of generated peer micro-blocks. The objective of this division is to reduce the bandwidth requirement, as the peer key-block contains the hash values for the peer micro-blocks. Additionally, peer key-blocks are validated before they are aggregated to construct global blocks. Having three types of blocks that follow different types of validation strategies is expected to improve security. Due to the inherited characteristics from the blockchain technology, traceability and security concerns in the e-commerce trading platform can be easily addressed. However, in e-commerce trading system, two main issues of user identification and scalability must be addressed. In such a system, the user identification process must ensure and validate the identity of the user to ensure that all the transaction is lawful. In blockchain technology, this can be performed by using a third-party validator node. Regarding the scalability, the blockchain solutions must not include any expensive computational process, which is essential, as the expected volume of online trades is large. This volume of trade suggests that the consensuses mechanism that is employed must adopt a "light" strategy to establish an upper bound for the expected running time. A multi-level architecture has also been adopted by Xie *et al.* [33] to establish a trusted blockchain-based e-commerce framework. In this framework, based on the type of performed validation, blocks are categorised into three different types: undecided, valid, and invalid. The main intention of this division is to support the storage of a massive number of transactions.

In the e-commerce trading domain, the impact of using blockchain technology depends on the challenges and the requirements for each trading category. In B2B and B2G, the identity of the traders is known and confirmed, and this reduces the pressure on the applied consensus mechanism. In such trading categories, blockchain technology can be used to optimise the trade supply chain by monitoring the trading process. In B2C and C2C, the identity of the users is not expected to be always confirmed. Accordingly, traders are expected to have the same level of authority (privileges); thus, it is expected that such trading solutions to be implemented using a permissionless decentralised public blockchain. In addition, by using permissionless blockchain, the design must focus on the scalability and data privacy issues to reduce the pressure on the consensus mechanism. The scalability concerns highlight the importance of employing efficient, lightweight mechanisms to address privacy and data integrity issues.

B. VALIDATION SOLUTIONS

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

1) ANTI-COUNTERFEIT TRADING

Trading counterfeit goods have a significant negative, damaging impact on society and the economy. For instance, trading fake medicines not only has a dangerous outcome on people's health and, thus, on their life but also costs the economy millions of dollars [34], [35]. Thus, establishing an efficient mechanism for anti-counterfeit has always been a priority for the public and private sectors. To effectively address this problem, the information-sharing platform between the trade supply chain participants should guarantee the immutability, integrity, and privacy of the information. In this direction, blockchain technology has emerged as a promising technology to address this problem.

Toyoda et al. [36] proposed a blockchain-based product ownership management system, where its primary objective is to use the traceability feature in the blockchain to avoid trading of counterfeit products. This is established by providing customers with the ability to trace the product from the manufacturing stage through the entire supply chain until it reaches them. This system comprises of two chains: (1) RFID-enabled supply chain and (2) post supply chain. The RFID-enabled supply chain connects the retailer to the manufacturer through the distributor, and the post-supply chain connects the retailer to the customer via the shops (or online sales).

In the RFID-enabled supply chain, which uses the Electronic Product Code (EPC), the manufacturer enrols its unique prefix in order to identify its ownership of the products in any future transactions. Then, the manufacturer registers the EPC of each product that he owns. Once the shipment reaches the distributor, the distributor uses the product's EPC for validating the product's genuineness, following which, these products can be shipped to any shop (small retailer) while keeping their ownership and EPC information in the information flow. Once a customer chooses a specific product, the EPC of the product can be used to identify the manufacturer to the customer in order to establish the genuineness of the product. In addition, the blockchain is used to identify the seller as the owner of the product. Using the EPC with the ability to trace the ownership, we can correctly decide whether a specific product is genuine. However, as the author mentioned, this system requires an administrative node (server) that validates and performs the registration of the manufacturer and the products' EPCs. In the supply chain presented here, none of the entities (participants) in the supply chain enjoys the total trust of all other entities or participants. Thus, a public blockchain (Ethereum) is used as a suitable environment to validate the proposed system performance. Using a public blockchain environment challenges the scalability of the presented system since strong group consensus is required to be performed. In addition, in the case of multi-ownership, all manufacturers who produce the same product must be a part of the blockchain. This creates additional pressure on the manufacturers in terms of creating the required infrastructure.

Similarly, Alzahrani *et al.* [37] also investigated the problem of the trade of counterfeit goods. In this research, the authors proposed a blockchain-based solution that utilises the benefits of Near Field Communication (NFC) in detecting and avoiding counterfeit goods. The main aim of this paper is to authenticate transactions using two types of authentication mechanisms, namely, the local authentication and global authentication. The local authentication is used to ensure that the tag and the information about the products have not been altered at any stage during the trade-process. In the global authentication, the main idea is that the validator nodes trace the entire series of transactions of each shipment to make sure that the current transaction is correct and as expected. In this work, in order to validate the current block, the consensus protocol selects a subset of the nodes as validators, and by reducing the number of validators, it aims to reduce the energy consumption of the system. These two authentication mechanisms work together to validate the trade. Using simulation experiments, the authors validated the performance of the presented approach in terms of consensus latency and detection rate. To address the problem of trading counterfeit products in the food supply chain, Baralla *et al.* [38] presented an authentication blockchain-based framework that can be used by the public to authenticate that the goods are made in, for instance, Sardinia. Other industrial initiatives to use blockchain for anti-counterfeit in food and e-commerce trades are presented in [39]–[42].

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

2) FOOD SAFETY

To ensure the quality of the distributed food, several measures are typically applied across the food supply chain. These steps work to monitor the surrounding environment of the goods at all stages of the supply chain. In addition, these measures typically involve several laboratory tests performed at pre-determined points in the supply chain. To increase the confidence of the employed food safety measures, techniques to ensure the uploaded information integrity and data immutability must be applied. In this direction, several proposals [43]–[47] have integrated these food safety methods with blockchain technology to optimise these methods.

Tian [43] presented a blockchain-based system to address the problem of food safety in the supply chain, which provides a reliable real-time traceability of the food supply chain by combining the benefits of the blockchain, the Internet of Things (IoT), and Hazard Analysis and Critical Control Points (HACCP) methods. In this system, blockchain is used to address the traceability requirement, and IoT is used to capture the required information about the shipment environment (for instance, temperature and light). The HACCP approach is a well-known method that is used to avoid hazards in the food supply chain. This method consists of several tests that must be performed at different points during the passage of the food along the supply chain. The overall objective of this system is to increase the efficiency of the HACCP through the use of the blockchain and IoT technologies.

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

The problem of food safety has also been investigated by Malik *et al.* [44]. To address this problem, the authors proposed permissioned consortium blockchain-based framework. By using the consortium mechanism, the authors aimed to increase the trust of the customers by avoiding having a single node with high authority. This framework deals with four types of members: (1) non-participating, (2) participating, (3) governance board, and (4) validators. Non-participating members (such as customers) can only query the blockchain. Participating members are the food supply chain entities, and they are the source of transactions. The governance board members consist of several government agencies, and they are responsible for determining the read and/or write access rules for the participating members.

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

Cui and Idota [45] presented a case study analysis, where Dentsu's blockchain-based system was used in Japan for the sale of organic vegetables. In this experiment, each vegetable was equipped with a chip that carried the required information about the status of the vegetable. The recorded information was used to generate information for vegetable batches. This information was uploaded to the blockchain. During the production life-cycle, the results of the performed laboratory tests on the vegetables were uploaded to the blockchain. In addition, IoT devices were used to monitor the storage and distribution environment, and the information recorded by these devices was periodically uploaded to the blockchain. In this study, an e-commerce trading platform was used to facilitate trades, where the actual trading was also stored in the blockchain. Customers were provided with an application to inquire about the historical data of the vegetables. In this paper, the authors did not provide enough information about the implementation details. However, giving the inquiring capability to customers suggests that the entire solution must be implemented on a public blockchain.

Similarly, Kamath [47] described the blockchain system solution proposed by Walmart Inc. to trace the production of food. Tracing the production of mangoes from trees to shelf is one of the pilot studies performed by Walmart. In this study, blockchain technology combined with IoT devices was used to provide the customers with the ability to trace the production and transportation of the traded mangoes.

Along the same lines, Hua *et al.* [48] proposed a blockchain-based conceptual framework for the agriculture domain. This framework discussed the benefits of blockchain technology and how it can be applied in agriculture to increase the trust level between the customers and the distributors. This framework consists of three types of activates: (1) registration, (2) verification, and (3) tracing. The administrative node performs the registration of the participating entities. Smart Contracts handles the verification of the uploaded data. Tracing is usually performed by the end-user to trace the historical information of the goods. This paper achieves its objective of highlighting the advantages of adopting the blockchain technology in the agriculture domain. However, the paper did not address the technical requirements to implement the proposed framework. In [49], a similar conceptual framework has been presented for the rice supply chain. Thiruchelvam *et al.* [50] presented a quantitative analysis approach to clarify the importance of employing a blockchain-based technological solution for the coffee supply chain in Burundi. A case study that explores the benefits of employing a blockchain solution in the agriculture domain is also presented by Vara *et al.* [51].

Westerkamp *et al.* [52] proposed a blockchain solution to trace the origin of the raw material used in the production of goods. This system uses recipe-based architecture, where raw materials are represented as tokens, and during the manufacturing process, the token of the final product is constructed based on the input tokens (consumed materials). Such traceability mechanism highlights the presented system as a suitable approach to add the food safety problem. By using this strategy, the authors aimed to trace the final product and the raw materials. In this system, smart contracts handle mainly three types of tasks: (1) tokenisation, (2) recipes, and (3) certified goods. Regarding tokenisation, a single, smart contract is responsible for creating and maintaining the token for each type of goods. Other types of smart contracts (recipes) handle the transformation of the raw material to the final product, where the token for this product is determined. During the manufacture of products, certain materials could be used to replace others, and the certified goods contract is responsible for identifying the equality relationship. In the evaluation section of this paper, one of the highlighted factors is the benefit of relying on events to transform information in terms of cost compared to storing all of the information in a smart contract.

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

3) REGULATED ITEMS' TRANSPORTATION

In this category, we focus on proposals that mainly use blockchain technology to fulfil the trade and transportation agreements, which are typically implemented as smart contracts. Furthermore, trading restricted items such as pharmaceutical goods are highly regulated [53]. Bocek *et al.* [54] proposed a tractability system termed Modum.io for pharmaceutical supply chain, which combines the benefits of IoT and blockchain. In this system, sensors (IoT) are used to monitor the temperature of each parcel during the shipment, and this is used to ensure the satisfaction of the government regulations. The architecture of this system consists of the back-end, front-end, and IoT sensor devices. The back-end consists of the blockchain (Ethereum network) and a server node, where this server is responsible for monitoring the blockchain and the deployment of the smart contracts.

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

To initiate the monitoring process, the sensor node has to be placed within the Bluetooth communication range of the Android phone. Then, the user has to associate the tracking number of the package with the MAC address of the selected sensors. Once this association is established, the tracking number of the package and the associated MAC address for the sensors are stored in the back-end server. Then, the client initiates the temperature monitoring process, where the sensors that are placed inside the packages start the periodical temperature recording process. After receiving the shipment, the client uses the tracking number of the package to request the MAC address of sensors from the server. The client then connects to the sensor to download the temperature readings. To test the performance of the presented system, the authors have run a pilot project lasting nearly one month with a pharmaceutical company, where 52 shipments have been successfully tracked using the proposed system.

Tseng *et al.* [55] proposed a blockchain-based conceptual model for the drug supply chain, where they discussed the benefits of employing this technology to monitor the shipment and distribution of the drugs. Imeri and Khadraoui [56] applied a relatively similar concept to address the problem of transporting dangerous goods. They presented a conceptual framework that aims to provide the required traceability information for the participating entities. These entities are the goods provider, transport operator, regulatory authority, customers, and emergency institutions. In this framework, smart contracts are used to define the path of the shipment and to notify certain entities whenever a specific event occurs. Additionally, the authors claimed that all participating entities are equal, and no administrative node is required. However, the process to achieve this equality assumption must be clearly stated.

A real-world blockchain traceability system termed OriginChain is presented in [57], [58]. OriginChain aims to automate the process of ensuring that the shipment satisfies the regulations and rules. This system deals with three types of users: (1) service user, (2) traceability provider, and (3) blockchain administrator. Examples of service users are retailer, consumer, and supplier. Traceability provider represents a company that provides several types of traceability services such as product examination, loading monitoring, lab tests, and yard examination. Blockchain administrator generates and deploys smart contracts that capture the traceability requirements. In this system, the process starts with the supplier submitting a registration application to the traceability provider, which validates the application and registers the supplier company. Then, to start the traceability service for a specific trade, the supplier must provide all the paperwork such as invoices, trade agreements, and contracts. Once the traceability provider validates these documents, the supplier and traceability provider have to sign a legal agreement that specifies the services that must be used (lab tests, yard inspection, etc.). The service starts once the supplier calls the factory contract from the web application. This contract creates service, registry, and data contracts. Service contract shows the traceability services that must be employed, and the legal information of the agreement is captured in the registry contract. Data contract deals with data storing and accessing. Information is stored either on-chain or off-chain. Information required for traceability is stored on-chain, and raw information (certificate files) is stored off-chain. OriginChain is implemented using the Ethereum blockchain.

Similar to any other crucial natural resource, sand trading follows government regulations, which ensure that the local trading budget is not exceeded and any illegal mining activities are detected. In this direction, Pour *et al.* [59] presented a framework to regulate sand trading. The framework presented by the authors authenticate all of the mining activities and use the available information to analyse if a new mining request should be approved based on the available budget.

Mao *et al.* [60] presented a blockchain-based trading system for the food supply domain. Accordingly, they presented a dynamic programming algorithmic approach that aims to establish a match between sellers and buyers that optimise their trading returns.

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

C. SUPPLY CHAIN OPTIMISATION

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

1) SUPPLY CHAIN MANAGEMENT

Wu *et al.* [61] presented multi-ledger tracking framework to simplify the process of supply chain management. This framework consists of several private sub-ledgers and a single centralised public ledger. Each sub-ledger represents a single shipment, and they can be accessed privately by the trading partners. The centralised public ledger represents the global tracking information that can be seen by public users. This framework consists of the following components: (1) index server, (2) peer, (3) administrative node, and (4) external monitoring nodes. The index server has the addresses of all nodes that are parts of the network. Peers represent the participating entities (for example, customs authority and shipping agents). The administrative node keeps track of all activities in the network. External monitoring nodes are third-party monitoring nodes that validate and track the status of this shipment. Furthermore, these nodes post their validation results on the blockchain. All of these components submit the shipment-related transactions to either the private sub-ledgers or the public ledger.

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

Chen *et al.* [62] also proposed a conceptual framework that aims to improve supply chain management by using a blockchain-based solution. In this framework, the authors proposed a system architecture that consists of several layers: (1) IoT sensors layer, (2) data layer, (3) contract layer, and (4) business layer. The idea of dividing the system architecture into four layers is to group the functionality components according to the services that they provide. In the sensor layer, the authors proposed employing technologies that can be used to track the goods (for example, GPS and RFID). The data layer has the blockchain and the ledger, and smart contracts are executed inside this layer to ensure the quality of the data. The contract layer has the responsibility of executing some of the functionalities that can support the decisions made by the business layer, which includes the main business activities.

Similarly, Meng and Qian [63] proposed a conceptual framework termed DeliveChain, which can be used to gather the required information to analyse the expected delivery performance for a given company. DeliveChain is designed to capture the status of the production and delivery in the supply chain, and this information is used to support the business decision. DeliveChain consists of five layers: (1) data input layer, (2) transaction layer, (3) smart contract layer, (4) ledger layer, and (5) business intelligence layer. The data input layer determines the acceptable data input methods by the system (GPS, staff, IoT). In the transaction layer, the data gathered by the data input layer is represented in specific pre-determined formats based on the type of the input source. The logic of the business is mainly implemented in the smart contract layer. In this layer, critical data and events are tracked to ensure the reliability of the system.

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

Blockchain is an ideal tool to ensure the integrity and security of the data. In these two frameworks [62], [63], the authors assigned unspecified computational tasks to the smart contracts. However, the computational capability of smart contracts is limited, and this should be taken into consideration during the designing of smart contracts.

To optimise trading in agriculture domain, Kaigun et al. [64]proposed blockchain solution, which employs double chain architecture. This solution is designed to establish a secure, trustworthy trading system, where enterprises aim to increase their share of the market wealth (rent-seeking). The two chains that form the architecture are termed as the user information chain and transaction chain. Information related to users' agriculture businesses or enterprises are stored in the user information chain, and all of the details of the transactions are stored in the transaction chain. Using two chains increases the privacy of the proposed solution. For instance, any member of the system can check the businesses' resource details on the user information chain without knowing the enterprises' details. The actual transactions are stored in the transaction chain using the Merkle Tree structure. To address rent-seeking, the system uses smart contracts that aim to establish the minimum total equity value among the traders.

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

2) INFORMATION SHARING

In the international trading domain, customs authorities' rule of protecting society by detecting smuggling and fake products is a challenging task. To fulfil this task, customs requires detailed information from businesses to monitor the flow of goods. Naturally, businesses are unwilling to share information, where the reason behind this is to avoid liability and protect confidant private information related to businesses strategies. To address this problem, Engelenburg *et al.* [7] proposed software architecture for business-to-government information sharing. They addressed these issues by proposing the designing of an information-sharing system that can be acceptable to businesses. In this direction, they highlighted the importance of maintaining the data confidentiality to avoid liability caused by sharing information as the main requirements for the businesses. These requirements are established in the proposed architecture through the use of blockchain technology. Besides the blockchain technology features of data immutability and data integrity, this architecture itself employs a context-based information sharing strategy. Using this strategy, a participating member can determine the logic of accessing certain information provided by his/her company. Therefore, if any other member would like to access this data, a request will be sent to the decision component, where it will be evaluated based on the owner's sharing strategy. In permissioned blockchain, we can pre-determine the information accessible by each member. Therefore, this architecture can be categorised as an extra level of privacy.

Additionally, to improve the process of international trade, Vos et al. [65] presented DEFEND, a secure and privacy-preserving decentralised system for freight declaration. DEFEND is a blockchain-based solution that aims to simplify and support the collaboration between the economic operators and the customs agencies. The author assumes that the participating entities in this system are: (1) the economic operators, (2) customs agencies, (3) containers, and (4) packages. A container contains several packages, and a unique identification number identifies each container. Additionally, in this system, the economic operators trust the customs agencies, whereas the customs agencies do not trust the economic operators or each other. By supporting traceability, this system aims to ensure that the customs agency is fully aware of the status of all packages inside the containers.

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

Adopting blockchain technology is expected to have a significant impact on optimising the information-sharing component in the international trade supply chain. Using such a secure platform, the participants must be able to identify and authenticate the source of information. Additionally, using blockchain-based information-sharing mechanism, participants can control the type of information that they are willing to share with other participants, and this significantly helps them in protecting their business strategies.

D. FINDINGS AND DISCUSSION

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

1) TYPE OF BLOCKCHAIN (PUBLIC/PRIVATE/CONSORTIUM) (RQ2)

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

In local trade, where the objective is to establish and regulate the trading market, it is more likely to use a public blockchain, as any user should be able to access the trading platforms without any restriction. Blockchain solutions for only the supportive processes can be deployed on a private blockchain, as the public customers are not part of these processes. A private blockchain can also be suitable for the local trading environment when the targeted market is restricted in nature and pre-authorisation is required. For instance, trading restricted items that require special permeate is more likely to occur in private blockchain. A consortium blockchain is suitable when one of the traders (or both) are several personals. For instance, when a government department is part of the trade, it is expected that several pre-determined employees have to agree on the trading conditions. Additionally, these points also apply to international trade. For instance, solutions that propose using blockchain to increase the customer visibility of the trade flow is expected to use public blockchain (e.g., [44], [47]). However, if the solution is proposed to implement critical business processes such as issuing banks letter of credit [66] (back-end processes), we expect that the deployment will occur on a private blockchain. In international trade, consortium blockchain is expected to be used when several participants have to validate the trade transaction.

From the customs perspective, the trading activities are performed between a pre-determined set of participants

TABLE 1. Summary of the investigated proposals.

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

among whom a level of trust already exists. Thus, to ensure the practicability of the proposed system, and, as, in most scenarios, the data is not accessible to the public customers, the system is more likely to be deployed in private blockchain. Consortium blockchain can be used for application scenarios that require the validation of several government entities. For instance, if permits authorities such as health administration and department of defence are integrated with the application architecture, it is more likely to use consortium blockchain to make sure that restricted items obtain the appropriate permits. Public blockchain can be used to host general descriptive information for public users. Compared to the public blockchain, using private blockchain (and consortium blockchain) reduces the pressure on the employed security mechanism because the network participants are pre-determined. Thus, using this type of blockchain in the design of the system has the advantage of simpler security requirements. In addition, in such a trading solution, certain participants (customs authority) are expected to play an administrative role to regulate the trade. Having such an administrative node that monitors the participants' activities helps in securing the trading process.

2) APPLICATION DOMAIN INTEGRATED TECHNOLOGY (RQ2)

In situations where the application scenario requires combining the benefits of blockchain technology with other technologies such as IoT, the solution architecture becomes vital in determining the overall performance. In this solution, we expect most of the processing to occur outside the blockchain, as the computational power of smart contract is limited [67]. Hosting the computational functionalities outside the blockchain and the interaction with these functionalities should be carefully planned at the designing stage to ensure the reliability of the final solution.

In customs domain, implementing the main processes that are related to the task of examining the shipment under consideration and issuing the clearance requires integration with several existing technologies. Currently, at Dubai Customs, the process of importation and exportation uses several machine learning-based technologies to validate the documents, the calculated duties, and trace the containers. These technologies require high computation and storage capabilities, and implementing them using smart contracts is not applicable. Thus, the blockchain-based processing model must take into consideration the issues that may arise because of this integration.

3) VALIDATION (RQ2)

To validate the performance of the proposed blockchain architectures, the discussed proposals have used several types of validation mechanisms such as simulation, Proof of Concept (POC), and the numerical experiments. The validation mechanism depends on the main idea of the proposal. For instance, proposals that investigate simplifying certain processes (e.g., [7], [65]) are more likely to establish a PoC using a real implementation. In this case, the selected deployment environment depends on the required accessibility strategy. For instance, the Ethereum environment is generally used for public permissionless application scenarios, and IBM Hyperledger Fabric is typically used for private permissioned application scenarios. Simulation is typically used when the objective is to validate the behaviour of certain network-related components (e.g., [39], [55]). In such a scenario, quantifying the behaviour of these components requires relatively a considerable number of transactions over a long period of time, and, therefore, simulating their behaviour is the most efficient validation method. Proposals that present conceptual frameworks normally support their claims through logical arguments without any evaluation methods. Some of these conceptual framework proposals sound efficient; however, without proper experimentation, their expected performance will always be unclear. Other experiment methodology, such as quantitative analysis can be used to validate the acceptance level of the proposed approach [50].

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

4) SCALABILITY AND NUMBER OF TRANSACTIONS (RQ2)

Both public and private blockchains prioritise security over performance. In terms of the number of transactions, public blockchains, such as Ethereum, currently support around 15 transactions per second [68], [69], whereas private blockchains, such as Hyperledger Fabric, support around 3,500 transactions per second [19], [69]. Thus, in terms of scalability, blockchain solutions that are built based on Hyperledger Fabric are expected to scale-up more efficiently compared to Ethereum-based blockchain solutions. However, private and public systems are both slow compared to Visa, that supports 25,000 transactions per second [69], [70].

This difference between Ethereum and Hyperledger Fabric in terms of scalability is related to the architecture that supports each of them. The Ethereum blockchain is a permissionless solution, where all nodes are identical and perform the same tasks. In Hyperledger Fabric, on the other hand, the nodes are not equal, and tasks are distributed among the nodes, which can be mainly categorised into peers, ordering, and client nodes. Peer nodes are mainly responsible for performing the consensus mechanism. Ordering nodes make sure that all nodes that have a copy of the ledger store information in the same order. Client nodes host the end-user application and communication with the rest of the blockchain.

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

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

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

5) ACCESSIBILITY AND AUTHORITY DISTRIBUTION (RQ2)

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

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

6) CUSTOMS ADMINISTRATION AND BLOCKCHAIN (RQ3)

Overall, from customs administrative perspective, several factors influence the efficiency of automating the international trade supply chain through the use of blockchain technology. These factors can be mainly participants and their rules as well as integration with existing technologies. In international trade, the trade supply chain consists typically of a relatively high number of participants. The number of participants and their activities plays a major role in determining the overall practicality of the system. In this direction, the cost and benefits of joining the blockchain network are not the same for all participants [69]. Therefore, we cannot assume the willingness of all participants in the international trade supply chain to be part of our blockchain. Accordingly, we expect that the registration of some of the manufacturers, freight forwarders, or even shipping agents as active participants in the blockchain may be barred. For this purpose, the system design should allow for ''skipping'' the expected input from such a non-priority participant(s). For example, if the freight forwarder for a given trade is not part of the blockchain, the shipping agent, on receiving the goods from the freight forwarder, can resume the process of interacting with the blockchain. The identity of the non-priority participants depends on the targeted process. For instance, in the importation scenario, the priority of the participants is associated with the importance of the documents that they provide for the shipment clearance process.

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

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

V. CONCLUSION

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

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

As part of the international trade supply chain, customs administrations play an essential role in protecting the local society and economy. Accordingly, from a customs authority perspective, the data integrity and traceability features of the blockchain technology have a significant impact on simplifying the goal of protecting the society and economy. Accordingly, joining blockchain-based information-exchanged mechanism is expected to optimise the processing model of customs authority to facilitate international trade further.

ACKNOWLEDGMENT

The authors would like to thank everyone from the Service Innovation department for their fruitful discussion and inputs.

REFERENCES

[1] *WCO SAFE Framework of Standards*, World Customs Org., Brussels, Belgium, Jun. 2018.
[2] D. W. E. Allen, C. Berg, S. Davidson, M. Novak, and J. Potts, ''International policy coordination for blockchain supply chains,'' *Asia–Pacific Policy Stud.*, vol. 6, no. 3, pp. 367–380, 2019.
[3] C. A. McDaniel and H. C. Norberg. (2019). *Can Blockchain Technology Facilitate International Trade*. [Online]. Available: https://ssrn.com/abstract=3377708
[4] M. G. Belu, ''Application of blockchain in international trade: An overview,'' *Romanian Econ. J.*, vol. 22, no. 71, pp. 2–16, 2019.
[5] Y. Chang, E. Iakovou, and W. Shi, ''Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities,'' *Int. J. Prod. Res.*, pp. 1–18, 2019.
[6] C. Xu, K. Wang, G. Xu, P. Li, S. Guo, and J. Luo, ''Making big data open in collaborative edges: A blockchain-based framework with reduced resource requirements,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[7] S. Van Engelenburg, M. Janssen, and B. Klievink, ''Design of a software architecture supporting business-to-government information sharing to improve public safety and security: Combining business rules, Events and blockchain technology,'' *J. Intell. Inf. Syst.*, vol. 52, pp. 1–24, Jul. 2017.
[8] M. Rauchs, A. Blandin, K. Bear, and S. Mckeon. (2019). *2nd Global Enterprise blockchain benchmarking Study*. [Online]. Available: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-enterprise-blockchain-benchmarking-study
[9] *Blockchain E-Book*, C. Technol., London, U.K., 2018.
[10] B. T. A. Bta, ''Developing on hyperledger fabric 1. 1,'' Blockchain Training Alliance, Temecula, CA, USA, Tech. Rep., 2018.
[11] G. Wood, ''Ethereum: A secure decentralized generalized distributed ledger,'' Ethereum & Ethcore, London, U.K., Tech. Rep., 2018.
[12] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, ''Blockchain challenges and opportunities: A survey,'' *Int. J. Web Grid Serv.*, vol. 14, no. 4, p. 352, 2018.
[13] C. Cachin, ''Architecture of the hyperledger blockchain fabric,'' in *Workshop Distrib. Cryptocurrencies Consensus Ledgers*, vol. 49, no. 1, pp. 65–70, 2016.
[14] *Global Blockchain Survey-Blockchain Gets Down to Business*, Deloitte Insights, New York, NY, USA, 2019.
[15] C. Loklindt, M. Moeller, and A. Kinra, ''How blockchain could be adopted for exchanging documentation in the shipping industry,'' in *Proc. Lect. Notes Logistics*, Mar. 2011, pp. 194–198.
[16] *How Blockchain and Smart Contracts Can Improve Customs Control*, 2018. [Online]. Available: https://medium.com/smartz-blog/how-blockchain-and-smart-contracts-can-improve-customs-control-1501ca00068f
[17] L. Macedo, ''Blockchain for trade facilitation: Ethereum, eWTP, COs and regulatory issues,'' *World Cust. J.*, vol. 12, no. 2, pp. 87–94, 2018.
[18] D. Tranfield, D. Denyer, and P. Smart, ''Towards a methodology for developing evidence-informed management knowledge by means of systematic review,'' *Brit. J. Manage.*, vol. 14, pp. 207–222, Sep. 2003.
[19] E. Androulaki, ''Hyperledger fabric Hyperledger fabric: A distributed operating system for permissioned blockchains,'' in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.
[20] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, ''Consortium blockchain for secure energy trading in industrial Internet of Things,'' *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[21] E. S. Kang, S. J. Pee, J. G. Song, and J. W. Jang, ''A blockchain-based energy trading platform for smart homes in a microgrid,'' in *Proc. 3rd Int. Conf. Comput. Commun. Syst. (ICCCS)*, Apr. 2018, pp. 291–296.
[22] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, ''A blockchain-based smart grid: Towards sustainable local energy markets,'' *Comput. Sci. Res. Develop.*, vol. 33, no. 102, pp. 207–214, 2017.
[23] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, ''A secure charging scheme for electric vehicles with smart communities in energy blockchain,'' *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.
[24] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, ''Adaptive blockchain-based electric vehicle participation scheme in smart grid platform,'' *IEEE Access*, vol. 6, pp. 25657–25665, 2018.
[25] N. Z. Aitzhan and D. Svetinovic, ''Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,'' *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.
[26] A. Laszka, S. Eisele, A. Dubey, G. Karsai, and K. Kvaternik, ''TRANSAX: A blockchain-based decentralized forward-trading energy exchanged for transactive microgrids,'' in *Proc. IEEE Conf. Parallel Distrib. Syst.*, Dec. 2018, pp. 1–10.
[27] A. Gupta, ''E-commerce : Role of E-commerce in today's business,'' *Int. J. Comput. Corp. Res.*, vol. 4, no. 1, pp. 1–8, 2014.
[28] B. Li and Y. Wang, ''RZKPB: A privacy-preserving blockchain-based fair transaction method for sharing economy,'' in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Aug. 2018, pp. 1164–1169.
[29] B. Pittl, W. Mach, and E. Schikuta, ''Bazaar-blockchain: A blockchain for bazaar-based cloud markets,'' *Proc. IEEE Int. Conf. Serv. Comput. (SCC)*, Jul. 2018, pp. 89–96.
[30] B. Pittl, W. Mach, and E. Schikuta, ''An implementation of the WS-agreement negotiation standard in cloudsim,'' in *Proc. IEEE Int. Enterprise Distrib. Object Comput. Workshop (EDOCW)*, Sep. 2016, pp. 356–359.
[31] P. C. K. Hung, H. Li, and J.-J. Jeng, ''WS-Negotiation: An overview of research issues,'' in *Proc. 37th Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2004, pp. 1–10.
[32] X. Min, Q. Li, L. Liu, and L. Cui, ''A permissioned blockchain framework for supporting instant transaction and dynamic block size,'' in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 90–96.
[33] W. Xie, ''ETTF: A trusted trading framework using blockchain in E-commerce,'' in *Proc. IEEE 22nd Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2018, pp. 707–712.
[34] A. T. Mori, E. Meena, and E. A. Kaale, ''Economic cost of substandard and falsified human medicines and cosmetics with banned ingredients in Tanzania from 2005 to 2015: A retrospective review of data from the regulatory authority,'' *Brit. Med. J. Open*, vol. 8, no. 6, pp. 1–7, 2018.
[35] E. A. Blackstone, J. P. Fuhr, and S. Pociask, ''The health and economic effects of counterfeit drugs,'' *Amer. Health Drug Benefits*, vol. 7, no. 4, pp. 216–224, 2014.
[36] K. Toyod, P. T. Mathiopoulo, I. Sasase, and T. Ohtsuk, ''A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain,'' *IEEE Access*, vol. 5, pp. 17465–17477, 2017.
[37] N. Alzahrani and N. Bulusu, ''Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain,'' in *Proc. 1st Workshop Cryptocurrencies Blockchains for Distrib. Syst.*, Jun. 2018, pp. 30–35.
[38] G. Baralla, S. Ibba, M. Marchesi, R. Tonelli, and S. Missineo, ''A blockchain based system to ensure transparency and reliability in food supply chain,'' in *Proc. Euro-Par Workshops*, vol. 8374, 2014, pp. 224–235.
[39] E. Xiao. (Oct. 2017). *Alibaba, JD Tackle China's Fake Goods Problem With Blockchain*. [Online]. Available: https://www.techinasia.com/alibaba-jd-ecommerce-giants-fight-fake-goods-blockchain.
[40] PRESS-RELEASS. (2018). *Seal Network to build blockchain anti-counterfeiting network with the European Commission.—Blockchain powered product authentication*. [Online]. Available: https://seal.network/press-releases/seal-network-to-build-blockchain-anti-counterfeiting-network-with-the-european-commission.html
[41] (2018). *UCOT*. [Online]. Available: https://www.ucot.world/
[42] J. J. Roberts. (2017). *The Diamond Industry is Obsessed With the Blockchain*. [Online]. Available: http://fortune.com/2017/09/12/diamond-blockchain-%0Aeverledger/

[43] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manage.*, 2017, pp. 1–6.
[44] S. Malik, S. S. Kanhere, and R. Jurdak, "Product chain: Scalable blockchain framework to support provenance in supply chains," in *Proc. IEEE 17th Int. Symp. Netw. Comput. Appl.*, Nov. 2018, pp. 1–10.
[45] Y. Cui and H. Idota, "Improving supply chain resilience with establishing a decentralized information sharing mechanism," in *Proc. 5th Multidiscip. Int. Soc. Netw. Conf. (MISNC)*, vol. 18, 2018, pp. 1–7.
[46] T. Hepp, P. Wortner, A. Schönhals, and B. Gipp, "Securing physical assets on the blockchain: Linking a novel object identification concept with distributed ledgers," in *Proc. 1st CryBlock*, 2018, pp. 60–65.
[47] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with IBM," *Blockchain Res. Inst.*, vol. 1, no. 1, pp. 1–29, 2017.
[48] J. Hua, X. Wang, M. Kang, H. Wang, and F.-Y. Wang, "Blockchain based provenance for agricultural products: A distributed platform with duplicated and shared bookkeeping," in *Proc. IEEE Intell. Vehicles Symp.*, Jun. 2018, pp. 97–101.
[49] M. V. Kumar and N. C. S. N. Iyengar, "A framework for blockchain technology in rice supply chain management plantation," *Future Gener. Commun. Netw.*, vol. 146, pp. 125–130, Mar. 2017.
[50] V. Thiruchelvam, A. S. Mughisha, M. Shahpasand, and M. Bamiah, "Blockchain-based technology in the coffee supply chain trade: Case of Burundi coffee," *J. Telecommun. Electron. Comput. Eng.*, vol. 10, nos. 2–3, pp. 121–125, 2018.
[51] R. Casado-Vara, J. Prieto, F. De La Prieta, and J. M. Corchado, "How blockchain improves the supply chain: Case study alimentary supply chain," *Procedia Comput. Sci.*, vol. 134, pp. 393–398, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187705091831158X?via%3Dihub
[52] M. Westerkamp, F. Victor, and A. Küpper, "Blockchain-based supply chain traceability: Token recipes model manufacturing processes," in *Proc. IEEE Int. Conf. Blockchain*, Jul./Aug. 2018, pp. 1–8.
[53] N. Kumar and A. Jha, "Pharmaceutical 'good transportation practices (GTP)'—An innovative concept In' GXP' acronym," *Amer. J. Pharm. Heal. Res.*, vol. 4, no. 1, pp. 1–10, 2016.
[54] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—A use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 772–777.
[55] J. H. Tseng, Y. C. Liao, B. Chong, and S. W. Liao, "Governance on the drug supply chain via gcoin blockchain," *Int. J. Environ. Res. Public Health*, vol. 15, no. 6, pp. 1–8, 2018.
[56] A. Imeri and D. Khadraoui, "The security and traceability of shared information in the process of transportation of dangerous goods," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, 2018, pp. 1–5.
[57] X. Xu, Q. Lu, Y. Liu, L. Zhu, H. Yao, and A. V. Vasilakos, "Designing blockchain-based applications a case study for imported product traceability," *Future Gener. Comput. Syst.*, vol. 92, pp. 399–406, Mar. 2019.
[58] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Softw.*, vol. 34, no. 6, pp. 21–27, Nov./Dec. 2017.
[59] F. Pour, U. Tatar, and A. Gheorghe, "Agent-based model of sand supply governance employing blockchain technology," in *Proc. Annu. Simulation Symp.*, 2018, pp. 14:1–14:11.
[60] D. Mao, Z. Hao, F. Wang, and H. Li, "Novel automatic food trading system using consortium blockchain," *Arab. J. Sci. Eng.*, vol. 44, no. 4, pp. 1–17, 2018.
[61] H. Wu, Z. Li, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, "A distributed ledger for supply chain physical distribution visibility," *Information*, vol. 8, no. 4, pp. 1–18, 2017.
[62] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, and J. Zhang, "A blockchain-based supply chain quality management framework," in *Proc. 14th IEEE Int. Conf. E-Bus. Eng. (ICEBE)*, Nov. 207, pp. 172–176.
[63] M. H. Meng and Y. Qian, "A blockchain aided metric for predictive delivery performance in supply chain management," in *Proc. IEEE Int. Conf. Service Oper. Logistics, Inform. (SOLI)*, Jul./Aug. 2018, pp. 285–290.
[64] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. Van Nieuwenhuyse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology," *Future Gener. Comput. Syst.*, vol. 86, pp. 641–649, Sep. 2018.
[65] D. Vos, "DEFenD: A secure and privacy-preserving decentralized system for freight declaration," in *Proc. 1st ERCIM Blockchain Workshop*, 2018, pp. 1–8.
[66] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innov.*, vol. 2, no. 1, pp. 1–12, 2016.
[67] M. Muzammal, Q. Qu, and B. Nasrulin, "Renovating blockchain with distributed databases: An open source system," *Future Gener. Comput. Syst.*, vol. 90, pp. 105–117, Jul. 2019.
[68] *Etherscan*. Accessed: Jun. 27, 2019. [Online]. Available: https://etherscan.io/
[69] G. Perboli, M. Stefano, and R. Mariangela, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018.
[70] Blocksplain. (2018). *Blockchain Speeds & the Scalability Debate*. [Online]. Available: https://blocksplain.com/2018/02/28/transaction-speeds/

HUSSAM JUMA received the bachelor's degree in computer science from Applied Science University, Jordan, and the master's degree in computer science from Sharjah University, UAE. He is currently pursuing the Ph.D. degree in computer science with The British University in Dubai (BUiD), United Arab Emirates (UAE). He is also the Director of Service Innovation and Enterprise Architecture Department, Dubai Customs. He has extensive experience in business, technology and worked on variety of enterprise IT environments and research projects. His main research interests are enterprise architecture, innovation management, knowledge management, blockchain, smart cities, and the Internet of Things (IoT).

KHALED SHAALAN is currently a tenured Full Professor of computer science and information with the Faculty of Computers and Information, Cairo University, Egypt, an internationally recognized university worldwide. He is also a Full Professor with BUiD. He is also an Honorary Fellow with the School of Informatics, University of Edinburgh. His main area of interests include computational linguists and educational technology. He is an authority in the field of Arabic Natural Language Processing and commands a great respect among the research community in the Arab world. He has many research publications in highly reputed journals.

IBRAHIM KAMEL received the B.Sc. degree in computer engineering from the University of Alexandria, Egypt, in 1984, and the Ph.D. degree in computer science from the University of Maryland, College Park, USA, in 1994. He was the Chair of the Department of Electrical and Computer Engineering, University of Sharjah, United Arab Emirates, where he is currently a Full Professor. He also served as the Director of the Institute of Leadership in Higher Education. He served as an Adjunct Professor with Concordia University, Canada, from 2007 to 2017. Before that, he was the Lead Scientist with the Panasonic Research Laboratory, Princeton, NJ, USA, where he was managing several research projects, information security, multimedia information retrieval, and smart appliances. He taught also at Polytechnic University, Brooklyn, and Rutgers University, New Jersey, USA.