Computers & Industrial Engineering 135 (2019) 582–592

Contents lists available at ScienceDirect

Computers & Industrial Engineering

journal homepage: www.elsevier.com/locate/caie

The power of a blockchain-based supply chain

Rita Azzi[a,*], Rima Kilany Chamoun[a], Maria Sokhn[b]

[a] Saint Joseph University of Beirut, Faculty of Engineering, ESIB, Beirut, Lebanon
[b] University of Applied Sciences Western Switzerland, HEG Arc HES-SO, Neuchâtel, Switzerland

ARTICLE INFO

Keywords:
Blockchain
Supply chain management
Traceability systems
Decentralized systems

ABSTRACT

A supply chain is a system of organizations, people, activities, information and resources involved in moving a product or service from supplier to customer. It is designed to maintain the quality of sensitive goods during the whole shipment. Centralized supply chain management systems expose the supply chain to corruption, fraud, and tampering. Blockchain has emerged as a new distributed information technology; it represents a new approach in supply chain area, where visibility and transparency of product flows are the principal challenges. This paper describes how the blockchain can be integrated into the supply chain architecture to create a reliable, transparent, authentic and secure system. To reach this goal, we studied the benefits of introducing the blockchain to the supply chain and the challenges encountered in a blockchain-based supply chain management ecosystem. We combined theoretical and real-world application studies to build our theory about the requirements for an efficient blockchain-based supply chain.

1. Introduction

The manufacturing of goods is becoming complex due to the increased number of intermediaries between the producer and the final consumer. Globalization and market expansion pushed companies to expand their products portfolios and life cycle, to meet new markets requirements. Hence, there's little knowledge of the product origins, processing or shipping journey (Van Kralingen, 2016). The challenge becomes not only quantitative but also qualitative. The main challenge of the supply chain remains in the traceability and data management system. The management of Information system in most sectors notably in healthcare, financial, food, and education is centralized. Transactions, decision-making, and storage system are controlled by third-party intermediaries. However, a centralized management system could represent a threat to data integrity, availability, and resiliency, leaving the system subject to corruption fraud and tampering (Abeyratne & Monfared, 2016). A trusted ecosystem needs to be created between the suppliers and their customers. This is achieved by a policy that focuses on the transparency of the chain to ensure product traceability, where accurate data collection and secure data storage are required.

Blockchain has been introduced in supply chain areas to make the chain more transparent, authentic and trustworthy (Laaper, Fitzgerald, Quasney, Yeh, & Basir, 2017). The purpose of this work is to study how integrating the blockchain into the supply chain can create a more reliable and authentic ecosystem.

Blockchain provides an untampered/ unalterable record of transactions. All product and shipping details are collected through different technologies and validated before becoming a permanent record on the blockchain (Ramamurthy, 2016; Zyskind, Nathan, & Pentland, 2015). To achieve our main objective, we provide first a literature review of the actual supply chain challenges before introducing the blockchain as a solution. The literature points out to new blockchain-based supply chain challenges. Hence studying blockchain integration into supply chain consists of evaluating blockchain-base supply chain efficiency and sufficiency. Next, we present the method adopted in this paper. Then we describe Ambrosus and Modum platforms, two real cases, introduced to add value to our evaluation and build our theory. Finally, we conclude with our recommendation to build a blockchain-based supply chain.

List of Acronyms: API, Application programming interface; BLE, Bluetooth Low Energy; CCD, Charge-coupled device; ERP, Enterprise resource planning; EVM, Ethereum virtual machine; FDA, Food & drug administration; GDP, Good distribution practice; GPRS, General Packet Radio Service; GPS, Global Positioning System; HTTP, HyperText Transfer Protocol; IoT, Internet of things; IPFS, InterPlanetary File System; JSON, JavaScript Object Notation; M2M, Machine to machine; NFC, Near-field communication; NMBA, N-Methylnitrosobutyric acid; PBFT, Practical Byzantine Fault Tolerance; QR code, Quick Response Code; REST, Representational State Transfer; RFID, Radio-frequency identification; 3G, Third generation; URL, Uniform Resource Locator

[*] Corresponding author.

E-mail addresses: rita.azzi@net.usj.edu.lb (R. Azzi), rima.kilany@usj.edu.lb (R.K. Chamoun), maria.sokhn@he-arc.ch (M. Sokhn).

https://doi.org/10.1016/j.cie.2019.06.042
Received 29 August 2018; Received in revised form 6 May 2019; Accepted 17 June 2019
Available online 18 June 2019

2. Literature review

2.1. Background

A supply chain ecosystem describes the processes that involve designing, engineering, manufacturing, and distributing products or services from suppliers to end-consumers (Muckstadt, Murray, Rappold, & Collins, 2001). Because these processes affect the goods, information and financial flows, some regulations are set to protect the consumers' right (Viswanadham & Samvedi, 2013). The eight basic consumer's rights recognized by the United Nations involve the right to safety, the right to be informed, the right to redress and the right to a healthy environment (Your rights as a consumer).

In the United States, the Food and Drug Administration (FDA) maintains consumers' right by promoting and protecting public health, through goods control and supervision. It works on applying predefined regulation and by protecting and promoting the development of human and veterinary drugs, biological products, medical devices and radiation-emitting products, human and animal food, and cosmetics (Food & Drug Administration, 2018). Many incidents have occurred in the past years, ultimately putting to question the supply chain reliability and its product data accuracy. In March 2018, 210 persons in the USA got an E. coli infection. Three months later, the public health and regulatory officials traced the origin of this infection to romaine lettuce which had been contaminated through the water back in the Yuma growing region (E. coli O157:H7 Infections Linked to Romaine Lettuce, 2018). In January 2008, Baxter Healthcare Corporation recalled various lots of heparin, an anticoagulant medication, after associating the product with adverse events, including deaths (Guerrini et al., 2008). More than three months later, U.S. FDA was able to establish a link between a contaminant found in heparin, a highly sulfated chondroitin sulfate, and the serious adverse events seen in patients given heparin. They traced back the contaminant to 12 different Chinese companies, and they found heparin batches shipped to 11 countries (Information on Heparin, 2018).

The Table below (see Table 1) provides information gathered from latest Food and Drug product recalls published on the FDA websites (Recalls, Market Withdrawals, Safety Alerts, 2019).

Based on the collected information, we highlight the multiple breaches encountered daily on a supply chain (Abeyratne & Monfared, 2016; Kshetri, 2018). Not only is people's health affected, but businesses also undergo damage. The company with a recalled product will suffer a reputation loss due to negative publicity and will see it sales reduced dramatically (Kshetri, 2018). During the investigation period, all related product will be affected, and some businesses shut down until the origin of this supply chain breach is detected (Kshetri, 2018). Between the market expansion, the growth in suppliers' relationships, and the rising consumer demand, the supply chain complexity has increased and revealed the need to meet new challenges. The key objectives of the supply chain, including cost, quality, speed, dependability, risk reduction, sustainability, and flexibility, are not fully achieved (Kshetri, 2018).

Transparency and traceability need to be enhanced in manufacturing supply chains (Abeyratne & Monfared, 2016; Caro, Ali, Vecchio, & Giaffreda, 2018; Laaper et al., 2017; Tian, 2016, 2017). The main supply chain risk lies in the product journey. We need more knowledge about the product, its origin, processing and shipping journey (Abeyratne & Monfared, 2016). Consumers are unable to verify the integrity of the acquired product; they have to trust the certification logo printed on products. Verifying this certification integrity requires strenuous auditing. Transparency must be enabled not only to regain the consumer's trust but to help the producer get a better perspective of the supply chain breaches and understand how management product decisions and environmental circumstances can affect a product. Achieving transparency requires accurate data collection and secure data storage, a difficult task currently entrusted to third parties through

Table 1
Food and drugs supply chain breaches reported by the U.S. FDA (Recalls et al., 2019).

	Date	Brand	Product description	Reason/problem
Food supply chain breach	03/08/2019	Fullei Fresh	Organic bean sprouts	Listeria monocytogenes
	02/25/2019	Marketside	Green beans and butternut squash	Potential Literia monocytogenes contamination
	02/25/2019	Bachman	Twist pretzels	Undeclared milk
	02/22/2019	Nova salted biscuit	Nova salted biscuit	Undeclared milk
Drugs supply chain breach	03/05/2019	Life-line tm	Additive for human drinking water	Potentially contaminated with Pseudomonas aeruginosa
	03/04/2019	Apotex Corp.	Drospirenone and ethinyl estradiol tablets, USP	May contain defective blisters
	03/01/2019	Sunstone organics	White Vein Kratom and Maeng Da Kratom	Potential for Salmonella
	03/01/2019	Torrent pharma	Losartan potassium tablets USP and Losartan Potassium/hydrochlorothiazide tablets USP	Contains N-Methylnitrosobutyric acid (NMBA)

centralized information depositories (Abeyratne & Monfared, 2016).

As revealed by Stoshi Nakamoto (Nakamoto, 2008); blockchain technology emerged in 2008 to serve as the shared ledger of the cryptocurrency Bitcoin. Unlike traditional currencies, Bitcoin eliminated the need for intermediaries and provided an efficient way to record transactions' information (Gupta, 2018). Blockchain brought to financial services: security, immutability, transparency and the ability to excise the middleman (Underwood, 2016). Used to record any transaction and to track the movement of any asset, blockchain revolutionized the traditional business network. Many sectors, notably in healthcare, insurance, government, supply chain management, and Internet of things, are likely to be transformed by the blockchain (Kshetri, 2018).

2.2. What is a blockchain?

A blockchain is a distributed ledger that records and shares all transactions that occur within the blockchain network. The blockchain network consists of multiple nodes that maintain a set of shared state and perform transactions modifying the states (Anh, 2017). Transactions must be validated by the majority of network nodes, before being ordered and packaged into a timestamped block. This mining process depends on the consensus mechanism adopted by the blockchain network (Christidis & Devetsikiotis, 2016). Before adding the new suggested block to the chain, all networks' nodes verify that the block contains valid transactions and references the correct previous block via a cryptographic pointer.

The blockchain network can be categorized either as permission-less or as permissioned network. A permission-less blockchain, is an open distributed ledger where any node can join the network and where any two peers can conduct transactions without any authentication from the central agency (Sankar, Sindhu, & Sethumadhavan, 2017). A permissioned blockchain is a controlled distributed ledger, where the decision making, and the validation process are kept to one organization (Sankar et al., 2017). A Certificate Authority determines who can join the network. All nodes are authenticated, and their identity is known to other nodes (Anh, 2017).

Fig. 1 below shows the blockchain data structure. The first block is known as the genesis block. A block consists of a header and a body. The block body contains the list of transactions (Di Pierro, 2017). The number of transactions within a block is related to the block and transaction's size. The block header contains various fields, mainly the block version indicating the set of rules which should be followed for validation (Zheng, Xie, Dai, & Wang, 2016), a hash of the previous block header, a timestamp, the Merkle tree root hash that represents the hash value of all the transactions in the block (Zheng et al., 2016). The nonce and target are block header fields, used for the Proof-of-Work protocol. It's a computational process, known as mining, where miners are the nodes that calculate the block header hash. A block is accepted by all nodes if a miner finds a nonce such as: hash (block header) < difficulty target. The nonce is a 32-bit field that is incremented until the equation is solved (Zheng et al., 2016).

Apart from being a distributed shared ledger, blockchain is also defined by three key concepts: consensus, smart contract and cryptography (Gupta, 2018; Anh, 2017).

1. A consensus is an agreement that helps a decentralized network to authenticate and validate a value or a transaction. It ensures that all network nodes share the same data and prevents malicious actors from manipulating the data (LFS171x). A consensus mechanism is defined by the following parameters: integrity, authentication, nonrepudiation, byzantine fault tolerance, decentralized governance, quorum structure and performance (Seibold & Samman, 2016). The type of consensus protocol depends on the blockchain type. For example, Bitcoin, a public ledger, uses Proof-of-Work, a computational expensive mining protocol to work around the Sybil attack, where a minority can control the whole network. In a permissioned blockchain, one organization determines the consensus process. A node needs to be certified to join the consensus process (Zheng et al., 2016). In that case, Proof-of-Work is unnecessary and is an expensive way to reach consensus because all participants are authenticated.
2. Smart contracts are self-executing scripts stored on the blockchain. When performing a transaction, smart contracts are invoked to execute the term of a contract/procedure on every node in the network (Christidis & Devetsikiotis, 2016). Hence, every node in a blockchain network must agree on the inputs, outputs and states affected by the smart contract (Anh, 2017). Satisfying common contractual conditions, such as payment terms or confidentiality, minimizes the need for trusted intermediaries (Bocek & Stiller, 2018).
3. Cryptographic techniques are used to ensure integrity, authenticity, immutability and nonrepudiation of the blockchain ledgers since even an authenticated node can act maliciously (Christidis & Devetsikiotis, 2016). The state root hash and the hash pointers are combined to secure and track all the historical changes made to the global state (Anh, 2017). The purpose of the root hash of the hash tree is to detect data tampering and to validate the transaction efficiently (Ramamurthy). To verify any transaction, we need to check the hash tree path related to the requested transaction. Any modification in a specific transaction will be instantly detected (Anh, 2017). The purpose of the block header hash is to verify the integrity of the block and of the transactions, and to form the chain link by embedding the previous block hash in the current block header. Transactions' block cannot be modified or deleted, once appended to the blockchain. Any modification in a specific block will invalidate all subsequent blocks (Anh, 2017). The asymmetric cryptography is used to provide integrity, authentication and nonrepudiation into the blockchain network. A user's node must sign the transaction before broadcasting it to the network (Christidis & Devetsikiotis, 2016; Anh, 2017; Zheng et al., 2016). Each user generates a key pair. The private key is used to encrypt the hash value derived from the transactions, and the public one is used by a peer node to verify the transaction's authenticity. Note that in a permissioned blockchain, an access control layer is added. For example, in Hyperledger, arbitrary policies are implemented to control users' access to the blockchain, thus adding more security to the network (Anh, 2017).

2.3. How blockchain improves the supply chain management

As already mentioned, there is a need to enhance the transparency and the traceability in the manufacturing supply chain. It is achieved by a policy that focuses on the transparency of the chain, where accurate data collection and secure data storage are required.

A good traceability system aims to minimize the production and distribution of unsafe or bad quality products by improving the labeling and tracking systems. The track and trace systems have evolved from paperwork to Internet of things (IoT) hardware and sensors (Abad et al., 2009; Aung & Chang, 2014; Badia-Melis, Mishra, & Ruiz-García, 2015; Van Kralingen, 2016; Zou, Chen, Uysal, & Zheng, 2014). The principal components of a tracking system are the tag, the tracer, and the sensor. A tag is a label set on the top of a product or a package that identifies the product. Passive Radio-frequency identification (RFID) and Quick Response Code (QR code) are examples of tagging systems. A tracer is a substance introduced into a product or its natural feature, used to provide information about the course or the process that involved a product, thus certifying its quality. A sensor is a device that detects environmental changes such as light, heat, motion, moisture, pressure, etc. The detected events are then sent to other electronic devices over the network for processing.

However, tracking devices are sometimes compromised and subject to cloning (Toyoda, Mathiopoulos, Ohtsuki, & Sasase, 2017). An

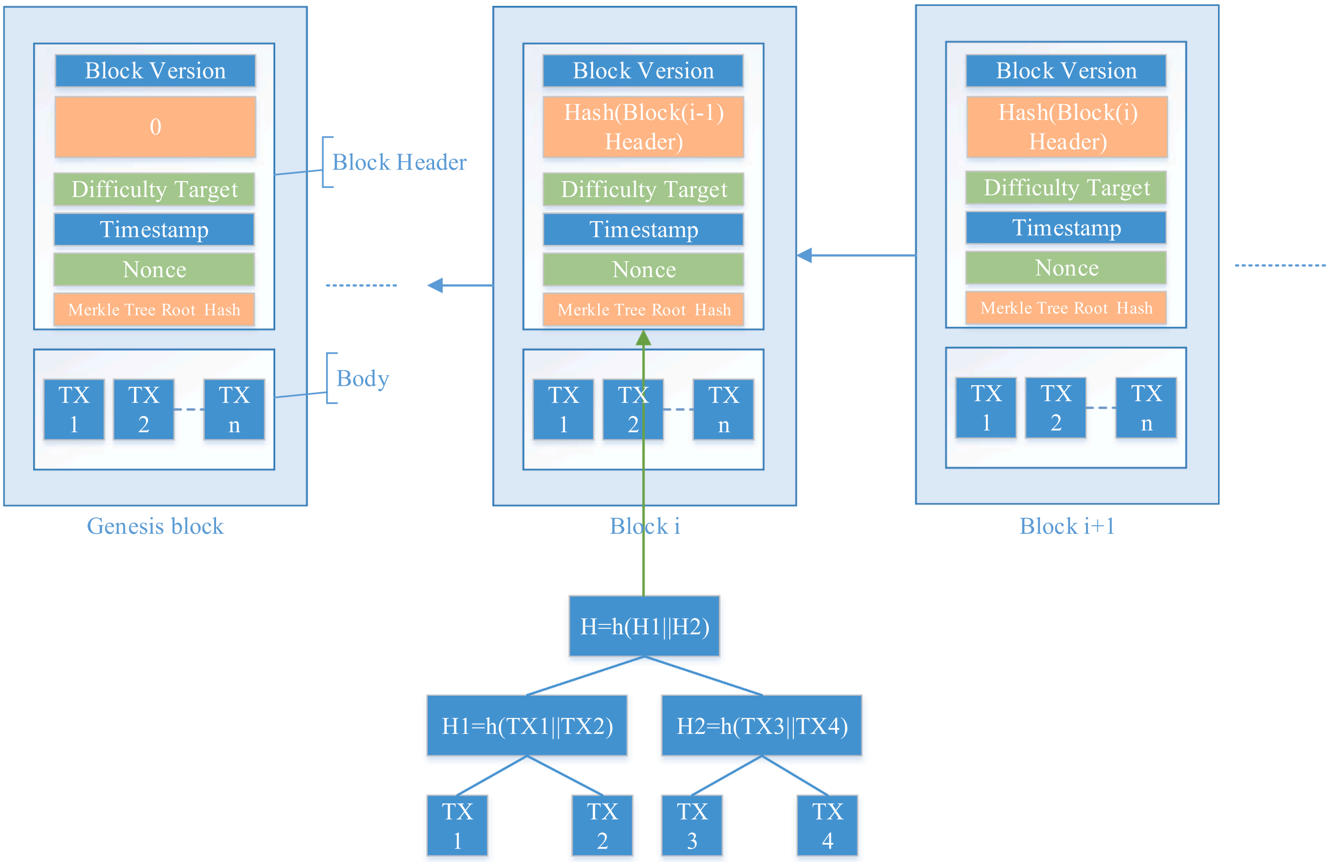

Fig. 1. Blockchain structure.

attacker can clone an RFID tag attached to a genuine product. Cloned tags on counterfeit products can mislead the consumers and endanger the consumers' safety in a medical or food industry (Huang et al., 2017). For producers, cloned tags can damage the company's reputation and cause severe economic losses in the logistics industries. Resolving clone attacks issue is achieved either through a prevention strategy based on developing either clone attack detection technique or a tag distribution schemes in order to prevent an attacker from copying the tags' content (Toyoda et al., 2017). According to Toyoda et al. none of these proposed track and trace methods can guarantee that the product, with an attached tag, is genuine once it is placed in retails stores for sale; this is because these methods leverage the tag's secret information (Toyoda et al., 2017). A blockchain-based product ownership management system was proposed, to transfer and prove the uniqueness of an RFID tag-attached products for the post supply chain. Counterfeits may be detected when the seller cannot prove the possession of the claimed product.

In supply chain area, storage and logistics management is considered a real challenge. Petri Helo et al. discuss in their paper the limit of centralized enterprise resource planning (ERP) technology in managing the supply chain and introduce a cloud-based solution (Helo, Suorsa, Hao, & Anussornnitisarn, 2014). In fact, ERP is a transaction management system that processes collected information and stores data in a single database. But ERP could not adapt to supply chain evolution and requirements especially in terms of transparency, flexibility, data accessibility and advanced decision making. A cloud-based NetMES system has been proposed to solve this issue (Helo et al., 2014). The cloud technology is used as a platform to exchange, store and monitor information where a centralized virtual database replaces a centralized physical database. It has added a real-time interaction to the whole proposed system; however, the security and privacy of stored data remain an issue. (Helo et al., 2014; Kshetri, 2017).

Besides, in a centralized system, a single entity controls data. If this entity fails or shuts down abruptly, the whole system will crash and stop processing transactions (Tian, 2017). The system is subject to fraud and malicious attack. It's not the case with the distributed ledger where a hacker cannot take advantage of a vulnerable point; if one node fails, the remaining nodes will not be affected. Note that a centralized system allows any user to modify a transaction in the ledger because there is no restriction on the operations (Nair & Sebastian, 2017). In case the data administrator is bribed, the whole system could be subject to tampering and falsifying information (Tian, 2017).

In China, the agri-food loss ratio is up to 30% yearly mainly due to their centralized logistic system (Tian, 2016). To reduce the losses during the logistics process and enhance food safety, Feng Tian proposed a decentralized traceability system based on RFID and blockchain. According to Feng Tian, enhancing the quality of the traceability system by integrating the RFID with other technologies such as WSN, Global Positioning System (GPS), etc. is not sufficient (Tian, 2016). These technologies cannot guarantee the integrity of the collected and shared data with all supply chain members. Integrated to improve the tracking system, blockchain strengthens trust, food safety assurance and information credibility. The RFID executes the tracing and monitoring to guarantee food quality and safety. All relevant information is then uploaded on the blockchain to create a reliable, transparent and secure decentralized platform, where all supply chain actors can interact (Tian, 2016). In case of an accident, emergency measures could be immediately taken to prevent the risk of hazard spreading. The proposed system has two disadvantages, first, the high cost of the RFID tag, which pushes some companies to narrow the application scope of the RFID, second, the immaturity of blockchain technology linked to the storage and synchronization issues (Tian, 2016).

According to Zheng Z. et al, blockchain is not always sufficient for storing data (Zheng et al., 2016). With the increasing number of transactions, the blockchain has become heavy. Hence scalability becomes challenging. For example, in a Bitcoin network, the block size is limited to 1 MB, and a block is added every 10 min (Zheng et al., 2016). Transaction's rate is limited to seven transactions per second, which is not enough for the trading system. Increasing the block size will reduce the network efficiency.

To overcome the blockchain scalability issue, Feng Tian, propose to integrate BigchainDB into the supply chain ecosystem. As proposed by McConaghy et al., BigchainDB combines the key benefits of distributed Databases – high throughput, low latency and high capacity- with the key benefits of blockchain – decentralization, immutability, creation and movement of digital assets (Tian, 2017).

Based on the above studies some questions have emerged:

- What are the benefits of introducing the blockchain to the supply chain?
- Can we trust the information shared in a supply chain traceability system?
- What are the challenges we need to address when integrating the blockchain in a supply chain?

3. Methodology and case study

To evaluate blockchain-based supply chain efficiency and sufficiency to create a reliable, transparent, authentic and secure system, we have adopted the theory built based on case studies as a research strategy. Working on real cases will highlight the challenges and characteristics to be taken into consideration in order to build an efficient blockchain-based supply chain. To confirm the theoretical study, knowledge of the practical and real-world application of the blockchain in a supply chain ecosystem is needed. By theoretical study, we imply study not deployed on a large scale. According to Eisenhardt k., case studies emphasize the rich, real-world context in which the phenomena occur (Eisenhard, 1989).

Several startups have already identified the blockchain as a new paradigm that aims to enhance supply chain management. We summarize, in Table 2, the main goal of the most prominent supply chain implementations and compare them according to the blockchain type and tracking system used. By introducing blockchain into their supply chain, these startups aimed to track, record and verify goods as well as protect them from fraud and tampering.

As shown in the Literature review, integrating the blockchain into the supply chain ecosystem brought significant new challenges notably on the blockchain level. To build a blockchain-based supply chain management, we need to take into consideration not only the blockchain technology but also the reliability of collected data.

To study how startups, integrate the blockchain into their supply chain ecosystem, we need to understand first their tracking system and the blockchain's role in their platforms' architecture. The efficiency and sufficiency of their blockchain-based supply chain will be developed in the discussion part. We selected Ambrosus and Modum as real cases to study since we could obtain sufficient information and they are related to the food and pharmaceutical supply chain: our main interest. By combining the theoretical findings with those drawn from real cases, we are able to address the emergent questions listed above.

4. Description of the selected cases

Ambrosus and Modum two Swiss Startups, have developed a system that merges IoT, blockchain technology and real-time sensors to trace and transmit products' information during the whole manufacturing process.

They aim to optimize supply chain visibility and quality assurance. Modum specializes in the pharmaceutical supply chain to ensure the safe delivery of pharmaceutical drugs in compliance with the GDP requirements. Ambrosus specializes in food and pharmaceutical supply chain to ensure the quality and safety of product consumption. For each case, we will describe the tracking system and the blockchain integration into these startups' system.

4.1. Case 1: Ambrosus

4.1.1. Tracking system

The Ambrosus network uses tags, tracers and sensors to track products throughout their life cycles. Their goal is to associate the product with the packaging and the transportation car, in a way that, if compromised, a notification is sent to the blockchain (Sensing system and integrity of supply chain data, 2017). Tracking components are customized according to the product type and based on the clients' needs. To track a fish from hook to fork, different tracking components are deployed (Sensing system and integrity of supply chain data, 2017). A smart gel tag is applied at the surface of the fish to assure product authenticity because the gel will react to fraudulent manipulation. A container sealed with a sensor contains all the collected fish. The sensor will assure the integrity of the product since it will detect any opened container. Another sensor is added to check the temperature and the GPS movement during the shipment. A Charge-coupled device (CCD) camera can be introduced to record all occurred activity until product shipment. All these sensors are bonded together and then bonded to the QR code. A QR code is a matrix barcode that contains information related to the product to which it is attached. All data obtained from the product, related to the QR code rectification and collected by the sensors aggregate to the QR code (Kirejczyk, Kędracki, Rukhavets, & Trifa, 2017).

In the Ambrosus network, all tracking devices are authenticated by a public-private key cryptography. The sensors and the QR code sign the collected data before sending it to the edge gateway using RFID technology (Kirejczyk et al., 2017). The gateway is a device composed of a microcontroller. It selects the received data before sending it to the blockchain through General Packet Radio Service (GPRS) technology (Kirejczyk et al., 2017). Note that the edge gateway needs to operate for months; thus, it must be powered by batteries or power harvesting (Sensing system and integrity of supply chain data, 2017). Once the received data is verified, it is saved on the blockchain. An Amber token is introduced to the ecosystem, and each amber will remain bonded to the product until a defined expiration date, such as a purchase (Sensing system and integrity of supply chain data, 2017). A customer can download all the required data concerning his purchased product from the web application which is built on top of the application programming interface (API). The API is linked to Ambrosus's data storage infrastructure; hence data becomes reachable to anyone who needs to verify the authenticity of his product.

4.1.2. Blockchain integration

In the Ambrosus Network, Ethereum blockchain is introduced to verify products' quality based on predefined requirements and to verify the tracking devices' identity. Supply chain automated governance and data management is mainly related to the deployment of two smart contracts: the requirement smart contract and the measurement smart contract.

The requirement smart contract defines the quality standards a specific item needs to maintain during the whole shipment till the delivery. The measurement smart contract stores:

- the collected attributes for a given batch at a specific point along the supply chain (Kirejczyk et al., 2017)
- the defined list of Ambrosus-certified measurement devices (Kirejczyk et al., 2017)
- the root hash of the Merkle tree

The list of statements defined in the requirement smart contract will be compared to the content of the measurement smart contract.

Table 2
Blockchain-base supply chain start-ups.

	Main goal	Blockchain type	Tracking system
Ambrosus (Kirejczyk et al., 2017)	Ensuring the origin, quality, compliance and proper handling of food and pharmaceutical tracked product	Public: Ethereum blockchain Private (for testing): Ambrosus Blockchain	Tag: QR code Tracer Sensor: Biosensor
Ascribe (McConaghy & Holtzman, 2015)	Web-based solution, to track, record and verify ownership, in the digital art market. All the digital contents are securely shared with artist and clients	Public: Bitcoin Blockchain	SPOOL protocol: Used for timestamping evidence of ownership transactions
Blockverify (Blockchain Based Anti-Counterfeit Solution)	Identify counterfeit goods, stolen merchandise and fraudulent transactions by introducing blockchain into the supply chain. Used for luxury and pharmaceutical items	Public: Bitcoin Blockchain	Block verify tag
Chronicled (Registry, 2016)	Protect goods from fraud and tampering	Public: Ethereum blockchain Future work: implement their own private blockchain	IoT devices: such as temperature logger, tamper proof smart tag
OwlChain (OwlChain, 2017)	Build a trusted ecosystem between the producer and the customer, by using public and transparent information Mainly adopted in the food industry	Private: AMIS blockchain based on the Ethereum technology	Tag
Provenance (Blockchain: the solution for transparency in prodcut supply chains, 2015)	Tracing back and verifying the origins, attributes and ownership of a specific product	Public: Ethereum Blockchain	Tags: QR code, Near-field communication (NFC) tags, Laser-engraved barcodes, 3D scanning
Modum (Modum white paper Data Integrity for supply chain operations powered by Blockchain Technology, 2017)	Track and trace pharmaceutical products in a secure way that meets all the requirements imposed by good distribution practice (GDP)	Public: Ethereum Blockchain	IoT sensor devices, and QR code
Everledger (Welcome to the digital vault of the future, Everledger, April 2015, 2015)	Tracking and protecting valuable assets (such as: diamond) from fraud, trafficking and theft	Public: Ethereum Blockchain Private: Hyperledger Blockchain	Thumbprint
Verisart (VERISART, 2015)	Certifying, documenting, verifying and tracking artwork ownership	Public: Bitcoin Blockchain	Image identification algorithm
TrustChain (Initiative, 2018)	Tracking and authenticating Jewelry such as diamonds	Public: IBM Blockchain based on the Hyperledger Fabric	Recording in the blockchain ledger: high-resolution photos of each diamond at every touchpoint along its journey, certificate of authenticity and product details

Meeting all the requirements ensure that the shipped product remains safe and in good quality (Kirejczyk et al., 2017). Measurement and requirement smart contracts are stored and are publicly available on the Ethereum blockchain.

However, Ethereum blockchain has a limited capacity in handling large quantity of data. Putting sensors' collected data on the blockchain will degrade its performance because the blockchain can handle a limited number of transactions per second (Sensing system and integrity of supply chain data, 2017). Thus, Ambrosus introduces Inter-Planetary File System (IPFS), a distributed storage, alongside the blockchain, to store all sensors' data (Kirejczyk et al., 2017).

In the Ambrosus layered architecture, the Ethereum blockchain and the distributed storage are located at the lowest level (first layer) as shown in Fig. 2. They represent the core of the Ambrosus system (Sensing system and integrity of supply chain data, 2017). Parity is the programming language used to build smart contracts running on Ethereum blockchain, and because running transactions on the Ethereum blockchain became expensive, an Ambrosus blockchain was adopted as the main transactional network. The Ambrosus blockchain is written in solidity and built upon the Ethereum blockchain.

The second layer consists of the Ambrosus protocol. The main three components of the Ambrosus protocol are: the measurement repository, the requirement smart contract and the amber token (Kirejczyk et al., 2017). All smart contracts associated with the Ambrosus protocol will run on the Ambrosus blockchain which will be copied to the Ethereum main network for further validation (Kirejczyk et al., 2017).

Above the Ambrosus protocol layer, we have the API, also known as the JavaScript layer. It allows developer to create and run Ambrosus contracts and objects in the Ambrosus platform without any blockchain programming knowledge (Kirejczyk et al., 2017). Developer can use JavaScript or html to connect their own hardware to the Ambrosus network.

4.2. Case 2: Modum

4.2.1. Tracking system

In the Modum network, monitoring begins in the web/mobile app, where setup, review and reporting happen. A quality manager creates a shipment profile with monitoring criteria and program notification to alert the team to any problem. The deviation can be visualized on the dashboard. The logistic teams activate the logger, also known as SensorTag, using an NFC plate, and connect it with the shipment ID. A smart contract is created to each shipment.

The SensorTag is used to measure the environmental conditions that

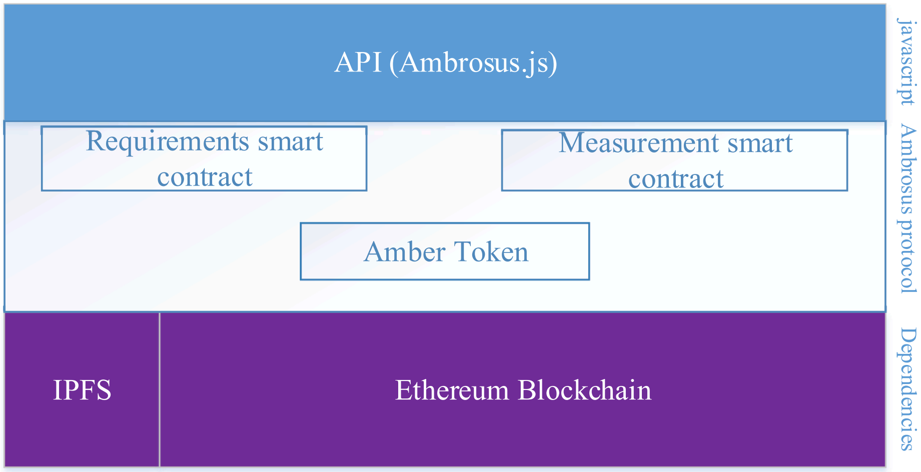

Fig. 2. Ambrosus system.

the shipment is subject to, store collected data in its internal memory and send data to the mobile application (Bocek, Rodrigues, Strasser, & Stiller, 2017).

Barcodes are used to identify the items handled in the Modum ecosystem. A sensor tag is associated with a unique MAC-Address through a QR code, and a packet is associated with a unique track-and-trace number through a distinct QR code. The camera of the Android device associates a logger with a shipment by capturing the QR code of both the sensor and the packet. The track-and-trace number/MAC-address association is sent to the server or is saved on the sensor internal memory if the server is not available (Bocek et al., 2017). The logger starts recording the temperature using the setting from the shipment profile. The temperature is recorded every 10 min in the sensor's internal memory. The server stores the track-and-trace number/MAC-address association, broadcasts the smart contract and stores the smart contract ID on the sensor device. When the client receives the packet, he will scan the track-and-trace number and request the temperature measurements downloaded from the sensor via the Bluetooth Low Energy (BLE). The data is sent to the smart contract to verify the compliance and a report is sent back to the client's mobile application (Bocek et al., 2017). There is no need to open the package to perform the checks (Modum white paper Data Integrity for supply chain operations powered by Blockchain Technology, 2017).

4.2.2. *Blockchain integration*

In the Modum Network, Ethereum blockchain is introduced to verify products' temperature compliance with GDP regulations. After the data verification process, smart contract stores, on the blockchain, the measurement hash and the uniform resource locator (URL) that points to the actual measurement data stored in the PostgreSQL (Bocek et al., 2017). Raw temperature data and user credentials are stored in PostgreSQL because collected data is too large or too sensitive to be stored on the blockchain.

The blockchain is in the back end of the Modum system, next to the server and database as shown in Fig. 3. The role of the server is to create, call and modify smart contract. This is done through an Ethereum node hosted by the server. HyperText Transfer Protocol (HTTP) server communicates with the Ethereum node over JavaScript Object Notation (JSON). Written in solidity, smart contracts run in an Ethereum virtual machine (EVM) to ensure that the shipment complies with the temperature required by the GDP. For each medical product type, hence for each shipment, a smart contract is configured (Bocek et al., 2017). A shipment-specific smart contract contains the temperature logger ID, the shipment ID and the alarm criteria. If the temperature data collected by the sensor does not meet the GDP regulation, the sender and receiver are notified to deal with the issue (Modum white paper Data Integrity for supply chain operations powered by Blockchain Technology, 2017).

The communication between the front end and the blockchain is done through HTTP server over Representational State Transfer (REST) API, using JSON to encode and decode requests and responses (Bocek et al., 2017).

5. Discussion

Different tracking components are deployed in Ambrosus and Modum systems, ranging from sensors to tags and tracers. The selection of the appropriate tracking device relies mostly on the product. For example, some products such as meat, fish, or vaccine must be maintained at a specific temperature and humidity conditions, requiring environmental monitoring sensors (Bocek et al., 2017; Sensing system and integrity of supply chain data, 2017). Alcoholic beverage industries must ensure product authenticity through products' lifecycle, and this process requires the usage of unique tags. Applied to corks these unique tags change color if the cork is removed or a needle is inserted to extract or tamper the liquid.

Chemicals and biological sensors are implemented to enable freshness investigation of food products and to assess food or medicine adulteration, authenticity and toxicity (Mustafa & Andreescu, 2018). Biosensor, an analytical sensor, is introduced to inform the interested supply chain parties about the biological content of a given product. Detecting the presence of allergens in food products such as milk, soybeans, eggs, peanuts, etc., is now a real concern since the prevalence of food allergies due to trace amounts of allergens is increasing (Mustafa & Andreescu, 2018). Biosensor relies on the biomolecule's recognition properties such as enzymes antibodies to monitor the product, through a variety of methods including colorimetric and mass-based detection (Mustafa & Andreescu, 2018).

The pilot project led by Modum showed the importance of having offline features, at the level of the tracking devices level, where data is stored internally until it can be uploaded on the blockchain (Bocek et al., 2017). This could provide the tracking system a more robust quality.

As observed in Table 2, multiple tracking devices are sometimes recommended to meet all the product tracking requirements. In their paper, Mackey et al. also highlight the same point and indicate how the most mature digital anti-counterfeit technologies include mobile and RFID-based technologies in order to enable fake drug detection, authentication and tracking (Mackey & Nayyar, 2017).

Data collected from the tracking devices are processed and sent to the storage system or blockchain. Ambrosus and Modum adopted different technologies to transfer data. We can mention RFID, BLE, NFC,

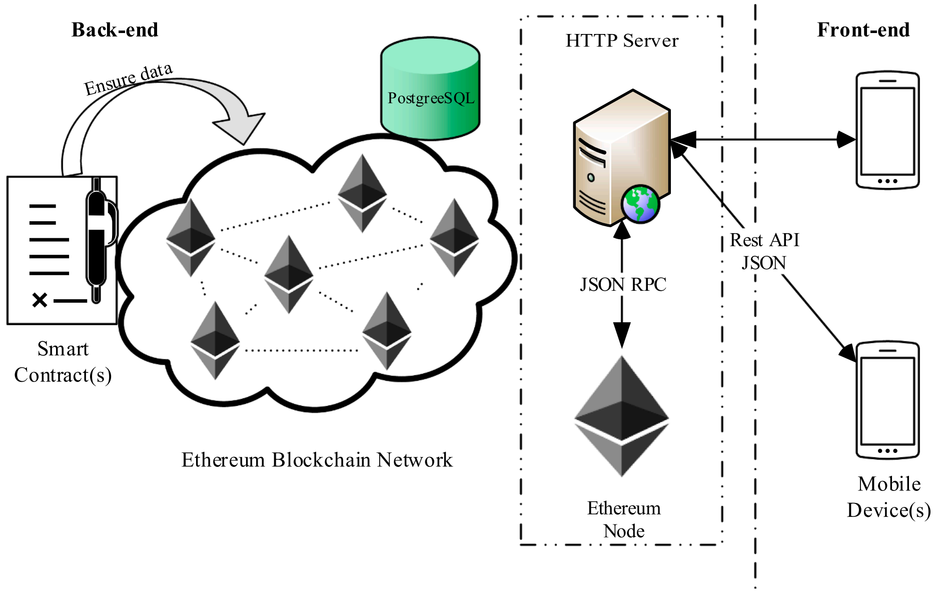

Fig. 3. Modum system (Modum white paper Data Integrity for supply chain operations powered by Blockchain Technology, 2017).

GPRS or 3G. Table 3 shows different criteria used to compare the communication protocols. According to Al-Sarawi et al., each protocol has benefits and limitations; the most suitable communication protocol is selected according to the application needs (Al-Sarawi, Anbar, & Alieyan, 2017).

RFID, BLE and NFC offer low power consumption and low setup time, but the maximum data rate for NFC is 424 Kbits per second, which is unsuitable for transferring large amount of data. It's not the case with RFID, which has the highest data rate of 4Mbps. In comparison, a widespread mobile network like 3G provides reliable high-speed internet connectivity, efficient for continuous streaming; however, 3G has a high-power consumption profile, making it unsuitable for local network communication (Samie, Bauer, & Henkel, 2016).

On the security level, we can identify multiple vulnerabilities for each protocol, that we must take into consideration during the implementation. For example, a device, if not encrypted, can be vulnerable to BLE attacks, such as replay attack or fuzzing attack (Ray, Raj, Oriol, Monot, & Obermeier, 2018). Collected and transferred data must be safe and reliable before being stored in an immutable decentralized database. Protecting data from hacking, fraud and manipulation during the whole supply chain process is crucial because the product's quality depends on it.

Ambrosus and Modum platforms have integrated security measures into their traceability system to guarantee integrity and authenticity of the handled data.

In Ambrosus, all authenticated devices sign data before transmitting it. The devices' signatures are verified before recording any message onto the blockchain. To verify the identity of a device, we can check the list of authorized devices publicly available in a smart contract. A measurement is ignored if it is sent from a non-authorized device. Besides, if a device becomes compromised or faulty, it will be disconnected from the system (Sensing system and integrity of supply chain data, 2017).

In Modum, all components with a serial number are registered in the database as authorized devices in order to identify forged, tampered or stolen loggers (Modum white paper Data Integrity for supply chain operations powered by Blockchain Technology, 2017). The sensor housing is tamper-resistant and water-proof; thus, it could not be physically disassembled or manipulated. All data, such as the measurements and timestamps, are signed by the logger before being transmitted. This will guarantee an end-to-end authenticity (Modum white paper Data Integrity for supply chain operations powered by Blockchain Technology, 2017). The private key is shielded by a cryptographic co-processor. Plus, Modum system offers a restricted access control, where only the authorized users can interact with the loggers.

Once building an effective traceability system, we need to study the efficiency of the blockchain technology to store and manage all transactions that occurred in the supply chain ecosystem. As shown in the Ambrosus and Modum platform, blockchain was integrated into their ecosystem to improve the tracking system and data management. Blockchain reduces fraud, errors, and delays identified in the actual supply chain ecosystem. It increases the trust between the customer and the supplier through the distributed ledger that is updated and validated in real time with each network transaction.

In the tracking system, blockchain was integrated to:

- Provide transparency, reliability, and integrity of the products' data collected throughout the entire lifecycle.
- Provide tracking device authenticity

In the data management, blockchain was integrated, to ensure availability, accuracy, and accessibility of data for all supply chain actors. Blockchain will improve business decisions and give deep insights into all the system's vulnerabilities.

Despite all these advantages, blockchain showed some limitations. In fact, Ethereum blockchain, adopted by both platforms, has a limited capacity in handling a large quantity of data. Ambrosus and Modum introduced a distributed file system: IPFS (Kirejczyk et al., 2017) and an object-relational database system PostgreSQL (Modum white paper Data Integrity for supply chain operations powered by Blockchain Technology, 2017) respectively, besides the blockchain, to store large data.

Using IPFS depends on the product's type and the client's demand. For products requiring a high level of security such as pharmaceutical products, IPFS is no longer used, because it's not secure. Plus, it fails in providing cumulative analysis and flexibility in handling interconnected data. IPFS will be replaced by the Ambrosus's own storing system: Ambrosus Blockchain. Ambrosus blockchain is implemented to enhance system performance by avoiding throughput degradation and latency faced in Ethereum blockchain.

According to D. Tien Tuan Anh et al., blockchain systems are not ready for mass usage (Anh, 2017). Following their comparative study of Ethereum, Parity and Hyperledger, where they used their BLOCKBENCH framework, they reached different conclusions. Among those

Table 3
Comparison between communication protocols.

	RFID	NFC	BLE	Cellular	
				GPRS	3G
Set-up time	< 0.1 msec (Jain & Dahiya, 2015)	< 0.1 msec (Jain & Dahiya, 2015)	Low	N.A.	N.A.
Power consumption	Ultra-low power (Al-Sarawi et al., 2017)	50 mA Low power (Al-Sarawi et al., 2017)	30 mA Low Power (Al-Sarawi et al., 2017)	High power Consumption (Al-Sarawi et al., 2017)	High power Consumption (Al-Sarawi et al., 2017)
Data rate	4 Mbps (Al-Sarawi et al., 2017)	106, 212 or 424 kbps (Al-Sarawi et al., 2017; Jain & Dahiya, 2015)	1Mbps (Al-Sarawi et al., 2017)	9.6- 172kbits/sec (Krishnaswamy, 2001)	7.2 or 56 Mbps
Communication range	Short range Up to 200 m (Al-Sarawi et al., 2017)	Short range 0–1 m (Al-Sarawi et al., 2017)	Short range ~100 m (Samie et al., 2016)	Several km (Al-Sarawi et al., 2017)	> 5 km (Samie et al., 2016)
Cost	Affordable (Jain & Dahiya, 2015)	Low (Jain & Dahiya, 2015)	Medium (Jain & Dahiya, 2015)	Expensive (Jain & Dahiya, 2015)	Expensive (Jain & Dahiya, 2015)
Security vulnerabilities	Tags face the risks of being broken, cloned, counterfeited and distorted (Changquing, Jixiong, Zhengyan, & Shengye, 2008) Security issues on wireless communication links Security risks within readers (Changquing et al., 2008)	Subject to security attack during transmission (ex: man, in the middle attack, eavesdropping, data corruption, data modification) (Jain & Dahiya, 2015; Madlmayr, Langer, & Kantner, 2008)	Susceptible to DoS attacks Fuzzing attacks and eavesdropping attacks (Ray et al., 2018)	Vulnerability in authentication procedure absence of a mechanism that ensures data integrity (Xenakis, Apostolopoulou, Panou, & Stavrakakis, 2008)	Wireless link threats Network services threats Terminal threats
Principal application domains	Industry (tracking, inventory, access) (Samie et al., 2016)	Smart cities, Industry, Secure transactions (payment) (Madlmayr et al., 2008)	Healthcare, Wireless headsets, Audio applications (Samie et al., 2016)	Local network (M2M) (Samie et al., 2016)	Smart cities, Smart building, Automotive (Samie et al., 2016)

findings, we highlight the most interesting ones in our case:

- In terms of throughput, Hyperledger performs the best. Compared to Ethereum, the gap is related to the adopted consensus protocol adopted. Hyperledger uses Practical Byzantine Fault Tolerance (PBFT), where the communication cost of broadcasting messages is cheaper than Proof-of-Work consensus protocol adopted by Ethereum.
- In terms of scalability, Parity performs best, due to its constant transaction processing rate. This is not the case with Ethereum and Hyperldeger, whose performance is affected by the number of used servers. In fact, Hyperledger will stop working when the number of servers and nodes reach a certain threshold because the number of dropped consensus messages will increase due to channel request congestion. In Ethereum, the consensus protocol is computationally based. Hence, increasing the number of servers and nodes will lead to throughput degradation since the computation difficulty has increased with the increase of the network's size in order to avoid long propagation delays.
- In terms of crash failures, Ethereum and Parity are both unaffected. This does not apply to Hyperledger, where the consensus protocol PBFT cannot tolerate more than 4 failures in a 12-server network.
- In terms of security attack, Ethereum and Parity are both vulnerable. The vulnerability is related to the consensus protocol adopted. For example, in Ethereum, the Proof-of-Work consensus is probabilistic. Hence, two blocks can append at the same time, creating a fork, exposing the system to double spending attack. It is not the case with Hyperledger where the Practical Byzantine Fault Tolerance consensus is considered safe with no forking problem.

Caro et al. implemented a fully decentralized traceability system for the Agri-food supply chain relying either on the Ethereum or the Hyperledger Sawtooth blockchain implementations. Based on their practical test, the implementation based on Hyperledger Sawtooth showed better results compared to the Ethereum one, in terms of latency, network traffic and CPU load. However, Ethereum is more advantageous in term of scalability, reliability and system maturity, enabling a large number of participants (Pincheira Caro, Salek Ali, Vecchio, & Giaffreda, 2018).

As revealed earlier, to deal with the blockchain limitations, some proposed to introduce a storage system next to the blockchain; some implemented their own transactional blockchain while others adopted a blockchain technology with some database functionality like BigchainDB.

Various blockchains are now publicly available and ready to be implemented such as Ethereum (Ethereum); Hyperledger Fabric (Hyperledger; LFS171x); Hyperledger Sawtooth (Hyperledger; LFS171x) and BigchainDB (McConaghy et al., 2016). It's important to consider the blockchain's different properties (decentralized control, immutability, creation and movement of digital assets) and capabilities (throughput, latency, capacity, scalability) before choosing a blockchain implementation over the other.

According to Baliga A., the security of a blockchain based system is related to the security and the robustness of the adopted consensus model (Baliga, 2017). The consensus protocol forms the core and the working entity of blockchain (Sankar et al., 2017). A bad consensus mechanism can compromise the data recorded on the blockchain. If the consensus mechanism fails it will lead to issues such as blockchain fork, consensus failure, dominance and cheating (Baliga, 2017). An efficient consensus protocol implementation can enhance economy growth, by ensuring the proper functioning of the blockchain and by avoiding any blockchain architecture malfunction (Sankar et al., 2017).

The security of a blockchain could be related to the blockchain type. Using Ethereum blockchain means that ledger can be viewed by anyone connected to the network. However, stored data can be sensitive; a certification authority is required to control the supply chain actors' role (read/write access) and identity. Data can be accessible to some supply chain members/stakeholders and limited to others. Hence, it's important to choose the blockchain type we want to adopt in our ecosystem, the one that will help us achieve the supply chain's main goal.

6. Conclusion

The blockchain is introduced to achieve the supply chain's objectives, by reducing the risk emerging from the tracking system and data management

Deploying blockchain in the supply chain ecosystem brought many benefits, notably:

- Creating more transparent and accurate end-to-end tracking
- Increasing trust between the producer and consumer, by improving visibility and product compliance with international standards
- Reducing paperwork and administrative costs
- Reducing or eliminating fraud and counterfeit products
- Facilitating origin tracking
- Recalling a product in a time-efficient way

However, integrating the blockchain into the supply chain ecosystem brought important new challenges notably on the blockchain level. We need to consider the properties and capabilities of available blockchain implementations before choosing the most suitable blockchain to such an ecosystem. To build a blockchain-based supply chain management, we need to take into consideration not only the blockchain technology suitable to our business but also the reliability of collected data.

Storing reliable information requires a reliable interaction between the blockchain and all ecosystems' constituents (These consists of tracking devices and actors).

To build a blockchain-based supply chain, we need to consider these requirements:

- Select a blockchain according to different key criteria notably: Throughput, latency, capacity and scalability (A multi-criteria decision-making can be applied to choose the most suitable blockchain to our deployed ecosystem.)
- Implement a dual storage architecture to handle large amount of data, without degrading the blockchain performance (An additional private blockchain could be introduced to the system architecture.)
- Choose the tracking devices based on the main product criteria we want to track or monitor
- Choose the communication protocol based on the speed, data rate, communication range, power consumption, cost or any criteria deemed essential in the supply chain environment
- Try to fill the security vulnerabilities found in the communication protocol to provide a secure and reliable traceability system
- Create a secure tracking environment beginning by authenticating the system tracking devices and making sure all transferred or collected data is encrypted and signed

Acknowledgements

The authors would like to acknowledge the National Council for Scientific Research of Lebanon (CNRS-L) for granting a doctoral fellowship to Rita Azzi. The authors are grateful to CAIE Editor-in-Chief, Mohamed Dessouky, as well as to many reviewers for their insightful and constructive comments on earlier version, which helped greatly in improving the paper.

References

Abad, E., Palacio, F., Nuin, M., Gonzalez de Zarate, A., Juarros, A., Gomez, J., & Macro, S. (2009). RFID smart tag for traceability and cold chain monitoring of foods: Demonstration in an intercontinental fresh fish logistic chain. *Journal of Food Engineering, 93*, 394–399.

Abeyratne, S., & Monfared, R. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology, 05*(09), 1–10.

Al-Sarawi, S., Anbar, M., & Alieyan, K. (2017). Internet of Things (IoT) communication protocols. In 8th International conference on information technology (ICIT).

Aung, M., & Chang, Y. (2014). Traceability in a food supply chain: Safety and quality perspectives. *Food Control, 39*, 172–184.

Badia-Melis, R., Mishra, P., & Ruiz-García, L. (2015). Food traceability: New trends and recent advances. *Food Control, 57*, 393–401.

Baliga, A. (2017). Understanding blockchain consensus models, April 2017. [Online]. Available: https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf.

Blockchain Based Anti-Counterfeit Solution. Blockverify, [Online]. Available: http://blockverify.io/.

Blockchain: The solution for transparency in prodcut supply chains, 21 November 2015. [Online]. Available: https://www.provenance.org/whitepaper. [Accessed 24 september 2017].

Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In 2017 IFIP/IEEE international symposium on integrated network management, Lisbon, Portugal.

Bocek, T., & Stiller, B. (2018). Smart contracts-blockchains in the wings. *Digital marketplaces unleashed* (pp. 169–184). Berlin, Heidelberg: Springer.

Caro, M., Ali, M., Vecchio, M., & Giaffreda, R. (2018). Blockchain-based traceability in agri-food supply chain management: A practical implementation. In In 2018 IoT vertical and topical summit on agriculture-tuscany, Tuscany.

Changquing, O., Jixiong, W., Zhengyan, L., & Shengye, H. (2008). An enhanced security authentication protocol based on hash-lock for low-cost RFID. In 2nd international conference on anti-counterfeiting, security and identification.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access,* 2292–2303.

Chronicled White Paper Open Registry for IOT, 15 August 2016. [Online]. Available: http://blockchainlab.com/pdf/whitepaper7.pdf. [Accessed 2017].

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering,* 92–95.

E. coli O157:H7 infections linked to romaine lettuce. Centers for disease control and prevention, 28 June 2018. [Online]. Available: https://www.cdc.gov/ecoli/2018/o157h7-04-18/index.html.

Eisenhard, K. (1989). Building theories from case study research. *The Academy of Management Review, 14*(4), 532–550.

Ethereum. [Online]. Available: https://www.ethereum.org/.

Food & Drug Administration. U.S. Food & Drug Administration, 05 April 2018. [Online]. Available: https://www.fda.gov/AboutFDA/default.htm. [Accessed March 2019].

Guerrini, M., Beccati, D., Shriver, Z., Naggi, A., Viswanathan, K., Bisio, A., ... Al-Hakim, A. (2008). Oversulfated chondroitin sulfate is a contaminant in heparin associated with adverse clinical events. *Nature Biotechnology, 26*(6), 669.

Gupta, M. (2018). *Blockchain for dummies 2nd IBM limited edition.* IBM.

Helo, P., Suorsa, M., Hao, Y., & Anussornnitisarn, P. (2014). Toward a cloud-based manufacturing execution system for distributed manufacturing. *Computer in Industry, 65*, 646–656.

Huang, J., Li, X., Xing, C., Wang, W., Hua, K., & Guo, S. (2017). DTD: A novel double-track approach to clone detection for RFID-enabled supply chains. *EEE Transactions on Emerging Topics in Computing, 5*(1), 134–140.

Hyperledger. [Online]. Available: https://www.hyperledger.org/.

Information on Heparin. U.S. Food And Drug Administration, 02 May 2018. [Online]. Available: https://www.fda.gov/Drugs/DrugSafety/PostmarketDrugSafetyInformationforPatientsandProviders/ucm112597.htm.

Jain, G., & Dahiya, S. (2015). NFC: Advantages, limits and futur scope. *International Journal on Cybernetics & Informatics, 04*(04), 1–12.

Kirejczyk, M., Kędracki, A., Rukhavets, I., & Trifa, V. (2017). Ambrosus white paper. [Online]. Available: https://ambrosus.com/assets/Ambrosus-White-Paper-V8-1.pdf.

Krishnaswamy, S. (2001). *Wireless communication methodologies and wireless application protocol.* Nashua: Rivier College Computer Science Department.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*, 1027–1038.

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89.

Laaper, S., Fitzgerald, J., Quasney, E., Yeh, W., & Basir, M. (2017). Using blockchain to drive supply chain innovation. In Hamburg international conference of logistics, Hamburg.

L. LFS171x. Blockchain for business - An introduction to hyperledger technologies, edX, [Online]. Available: https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2017/course/.

Mackey, T., & Nayyar, G. (2017). A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert opinion on Drug Safety, 16*(5), 587–602.

Madlmayr, G., Langer, J., & Kantner, C. (2008). NFC devices: Security and privacy. In The third international conference on availability, reliability and security.

McConaghy, T., & Holtzman, D. (2015). Towards an ownership layer for the internet. *ascribe GmbH*.

McConaghy, T., Marques, R., Muller, A., De Jonghe, D., McConaghy, T., McMullen, G., ... Bellemare, S. (2016). BigchainDB: a scalable blockchain database. *BigChainDB*.

Modum white paper data integrity for supply chain operations powered by Blockchain Technology, August 2017. [Online]. Available: https://modum.io/wp-content/uploads/2017/08/modum-whitepaper-v.-1.0.pdf. [Accessed september 2017].

Muckstadt, J., Murray, D., Rappold, J., & Collins, D. (2001). Guidelines for collaborative supply chain system design and operation. *Information systems frontiers, 3*(4), 427–453.

Mustafa, F., & Andreescu, S. (2018). Chemical and biological sensors for food-quality monitoring and smart packaging. *Foods, 7*(10), 168.

Nair, G., & Sebastian, S. (2017). Blockchain technology centralised ledger to distributed ledger. *International Research Journal of Engineering and Technology, 4*(3), 2823–2827.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

OwlChain, Owlchain, January 2017. [Online]. Available: https://www.owlting.com/owlchain/. [Accessed 2017].

Pincheira Caro, M., Salek Ali, M., Vecchio, M., & Giaffreda, R. (2018). Blockchain-based traceability in agri-food supply chain management: A practical implementation. In IoT vertical and topical summit on agriculture-tuscany, Tuscany.

Ramamurthy, B. Blockchain basics. Coursera, [Online]. Available: https://www.coursera.org/learn/blockchain-basics/home/welcome.

Ramamurthy, S. (2016). Leveraging blockchain to improve food supply chain traceability. [Online]. Available: https://www.ibm.com/blogs/blockchain/2016/11/leveraging-blockchain-improve-food-supply-chain-traceability/.

Ray, A., Raj, V., Oriol, M., Monot, A., & Obermeier, S. (2018). Bluetooth low energy devices security testing framework. In 11th international conference on software testing, verification and validation (ICST).

Recalls, Market Withdrawals, & Safety Alerts. U.S. Food & Drug Administration, 02 August 2019. [Online]. Available: https://www.fda.gov/Safety/Recalls/default.htm. [Accessed March 2019].

Samie, F., Bauer, L., & Henkel, J. (2016). IoT technologies for embedded computing: A survey. In In proceedings of the eleventh IEEE/ACM/IFIP international conference on hardware/software codesign and system synthesis.

Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. In Advanced computing and communication systems, Coimbatore, India.

Seibold, S., & Samman, G. (2016). Consensus: Immutable agreement for the internet of value. KPMG, US.

Sensing system and integrity of supply chain data, Ambrosus, 2017. [Online]. Available: https://ambrosus.com/assets/new4-3.-Sensing-System-and-Intregrity.pdf. [Accessed september 2017].

The TrustChain Initiative, April 2018. [Online]. Available: https://www.trustchainjewelry.com/.

Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In In 2016 13th international conference on service systems and service management (ICSSSM).

Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In 13th international conference on service systems and service management.

Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchai & Internet of things. In International conference on service systems and service management, Dalian; 2017.

Tien Tuan Anh, D., Ji, W., Gang, C., Rui, L., Beng Chin, O., & Kian-Lee, T. (2017). Blockbench: A framework for analyzing private blockchains. In Proceedings of the 2017 ACM international conference on management of data, New York.

Toyoda, K., Mathiopoulos, P., Ohtsuki, T., & Sasase, P. (2017). A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access, 5*, 17465–17477.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM, 59*(11), 15–17.

van kralingen, B. (2016). How blockchain could help to make the food we eat safer... around the world. Forbes , 01 november 2016. [Online]. Available: https://www.forbes.com/sites/ibm/2016/11/01/how-blockchain-could-help-to-make-the-food-we-eat-safer-around-the-world/#519addc7143d. [Accessed 01 september 2017].

VERISART, VERISART, 2015. [Online]. Available: https://www.verisart.com/. [Accessed september 2017].

Viswanadham, N., & Samvedi, A. (2013). Supplier selection based on supply chain ecosystem, performance and risk criteria. *International Journal of Production Research, 51*(21), 6484–6498.

Welcome to the digital vault of the future, Everledger, April 2015. [Online]. Available: https://www.everledger.io/. [Accessed 2017].

Xenakis, C., Apostolopoulou, D., Panou, A., & Stavrakakis, I. (2008). A qualitative risk analysis for the GPRS technology. In IEEE/IFIP international conference on embedded and ubiquitous computing, Shanghai, China.

Your rights as a consumer. Northern territory consumer affairs, [Online]. Available: http://www.consumeraffairs.nt.gov.au/ForConsumers/ConsumerRights/Documents/your_rights_as_a_consumer.pdf. [Accessed March 2019].

Zheng, Z., Xie, S., Dai, H., & Wang, H. (2016). Blockchain challenges and opportunities: A survey. *Researchgate*.

Zou, Z., Chen, Q., Uysal, I., & Zheng, L. (2014). Radio frequency identification enabled wireless sensing for intelligent food logistics. *Philosophical Transactions of The Royal Society A Mathematical Physical and Engineering Sciences, 372*.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In IEEE CS security and privacy workshops.

Rita Azzi is a Ph.D. student at the Ecole Supérieure des Ingénieurs de Beyrouth of Saint-Joseph University, Lebanon. Her Ph.D. is funded by the CNRS-L (Conseil National de la Recherche Scientifique - Lebanon). Rita Azzi graduated from the Engineering Faculty of the Holy Spirit University of Kaslik, with a Computer and Communication Engineering diploma, and holds a Research Master's Degree specialized in Telecommunication Network from the Engineering Faculty of Saint-Joseph University and Lebanese University.

Rima Kilany Chamoun holds a Ph.D. degree in Computer and Communication, from Ecole Nationale Supérieure de Télécommunications, Paris France. She is currently an Associate Professor at the Ecole Supérieure des Ingénieurs de Beyrouth of Saint-Joseph University, Lebanon. Her current research interests include Entreprise Application Integration, Data Integration, Semantic Web Technologies, Cloud and Digital Business Transformation.

Maria Sokhn is a professor at the Haute École de Gestion Arc, University of Applied Sciences and Arts of Western Switzerland, Neuchâtel. Maria Sokhn holds a PhD from Telecom Paris Tech in 2011 in multimedia knowledge management and visualization in collaboration with the CERN. She graduated from the Engineering Faculty of Saint Joseph University, with a Computer and Communication Engineering diploma, and holds a specialized master diploma from Telecom Paris Tech in Multimedia production and creation. Her current research activities interests are the mobility and touristic citizen centric services. She especially focus her work on accessibility for people with disabilities and therefore to reduce inequalities among the population. Her field of research also includes Linked Open Data and digitalisation of organization.