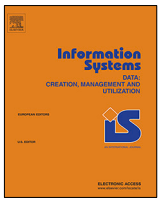
Information Systems 117 (2023) 102232

Contents lists available at ScienceDirect

Information Systems

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



A survey on the use of blockchains to achieve supply chain security

Md Didarul Islam

Department of Computer Science and Engineering, University of Nevada, Reno 1664 N Virginia St, Reno, NV, USA

ARTICLE INFO

Article history:
Received 20 April 2023
Received in revised form 25 May 2023
Accepted 27 May 2023
Available online 30 May 2023
Recommended by Dennis Shasha

Keywords:
Blockchain
Integration
Supply chain
Supply chain attacks
Supply chain security

ABSTRACT

Supply chain networks are becoming more complex and vulnerable to various attacks. We must tackle these attacks properly to ensure the required supply chain security. In this paper, I have classified major supply chain security issues with some real-life examples. I have also discussed the most recent countermeasures of these attacks. Furthermore, blockchain is a promising distributed information technology that creates opportunities for a new approach in the supply chain area. In my research work, I have described how to integrate blockchains into supply chain architectures to create more secure systems. I also discussed the benefits and challenges of introducing blockchain into the supply chain in this paper. To explain that better, I explored the performances of some in-practice blockchain platforms that we can apply to supply chains. I further mentioned the possible solutions for the challenges of integrating blockchain into supply chains.

Contents

E-mail address: green102@nevada.unr.edu.

https://doi.org/10.1016/j.is.2023.102232
0306-4379/

1. Introduction

Supply chains are the synchronized systems of all related entities, processes, resources, information, and technology involved, from the delivery of the source materials of products to the products' ultimate delivery to the customers [1]. To make the supply chains work perfectly, several parties, such as suppliers, producers, vendors, warehouses, transportation companies, distribution centers, retailers, logistic operators, and financial institutes, are interlinked to form an interactive network [2]. Fig. 1 illustrates a simplified structure of an essential supply chain.

But supply chains are only sometimes that simple; most of the time, they are rather complex. With more parties getting involved in the supply chain, the whole system has to go through an increased number of coordinations among different parties, creating several concerns. The main problem in a supply chain is ensuring the integrity of the product throughout the whole supply chain, and the secondary concern is protecting the supply chain-related vital information. Product integrity involves transforming, transporting, and storing raw materials and products. Moreover, information security is related to the supply chain parties' everyday and long-term plans, coordination with other parties, and so on.

As many entities are involved in modern-day supply chains, sharing products and information with business partners is unavoidable but also increases several supply chain security attacks. Attackers may perform these attacks on products, security devices associated with products, sensitive company information, and so forth. How to fight against these attacks has drawn much attention from researchers recently. Some large-scale supply chains are so complex that it is almost impossible to prevent all the attacks as the adversaries are constantly searching for the slightest weak point to attack. Some attacks are so dangerous that they harm not only the affected entity but also other connected parties as well.

Therefore, the operation of such large supply chains comprised of numerous interconnected entities will face some security, privacy, trust, and other concerns that may put the whole supply chain at risk and affect the connected entities. Although researchers have already conducted tremendous work addressing these concerns, it is still a complex problem to resolve, and researchers need to explore more. One possible solution might be blockchain.

Blockchain is a distributed ledger technology. This technology first evolved from the cryptocurrency Bitcoin concept introduced by Satoshi Nakamoto in 2008 [3]. Generally speaking, blockchain is immutable (write once and read-only), decentralized, and a shared database that records all the transactions within the system.

Applying blockchain technology to supply chains can add valuable features to the supply chain information, such as decentralization and immutability. On the other hand, linking supply chain products to the blockchain can also bring transparency, traceability, and non-repudiation. As a preferred alternative to the traditional centralized databases, blockchain can address specific supply chain management issues such as complicated record-keeping, provenance tracking of the products, and distrust among different supply chain parties. Utilizing blockchain technology to mitigate supply chain security concerns and make supply chains more resilient has recently become an attractive research proposition.

As a part of blockchain-integrated supply chain research, my work tries to contribute to the domain. The contribution of my research work is threefold:

First, I comprehensively reviewed the supply chain security attacks with some real-world examples. I have also mentioned the present countermeasures of these attacks.

Then, I explained how to integrate blockchain into supply chains step-by-step.

Lastly, I discussed the possible issues of integrating blockchain into the supply chain and their potential solutions.

The organization of the rest of the paper is as follows:

Section 2 discusses the backgrounds and related works. In Section 3, I have described the review methodology.

Section 4 illustrates supply chain attacks and their state-of-the-art countermeasures.

Section 5 discusses a detailed overview of integrating blockchain into supply chains.

In Section 6, I have highlighted challenges and probable solutions for blockchain integration into supply chains.

Section 7 concludes the paper and mentions future research.

2. Background and related work

2.1. Background on supply chain

A supply chain is an interconnected and synchronized system of all related organizations, personnel, resources, processes, information, and technology involved in the production and successful delivery of a finished product to the end user, including the moving of the product throughout the whole chain from

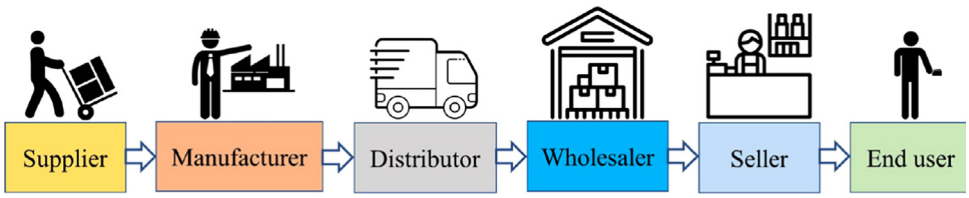


Fig. 1. Different stages of a basic supply chain.

the very beginning of the supply of the raw materials. A supply chain is a network of organizations and service providers working together to maintain the product's quality and protect information, equipment, and facilities in every stage of the supply chain [1]. Organizations directly involved in the supply chain are raw material suppliers (such as mines and farms), IP (Intellectual Property) owners, manufacturers or producers, assemblers, transportation, distributors, wholesalers, retailers, end users, and so on. However, many other entities participate in the supply chain for the smooth functioning of the system, such as inventory management like warehouses, vendors, logistic service providers, intermediate companies, financial institutes (e.g., banks), government agencies, etc. [2]. These organizations or companies interact with each other not only for better performance and enhanced supply chain security but also to make the supply chain global, which necessarily requires the movement of the products along with associated personnel and equipment across international borders.

2.2. Supply chain related works

Several technologies and procedures can be adopted to facilitate the automation process and secure the supply chain. For instance, GPS is used to locate the products. Quality information on the raw materials and products, such as temperature, vibration, humidity, aroma, etc., are collected using different sensors [4]. Products are identified using different identification technologies like barcodes, QR (Quick Response) codes, or RFID (Radio Frequency Identification).

RFID tags are considered more sophisticated than barcodes and QR codes when it comes to inventory and traceability management. Based on the type of tag, the reading distance can be several meters, and the line-of-sight requirement becomes trivial. In addition, some specific RFID tags can also store a significant amount of information [5]. Numerous research work has been done in the field of RFID attacks.

In one such work, Mitrokotsa et al. (2010) [6] discussed different attacks on RFID. Their work illustrated how these attacks could happen and linked them with different RFID communication layers: Physical layer, Network-transport layer, Application layer, and Strategic layer. A few examples of multilayer attacks have also been provided. Then they suggested some defense mechanisms against attacks on different layers. The authors Ahemd et al. (2017) [7], Andrea et al. (2015) [8], and Varga et al. (2017) [9] have conducted a similar type of research and advanced it further. Instead of staying only with RFID, they have explored different security attacks on internet of things (IoT). After connecting these attacks with different IoT layers, they proposed possible layer-based countermeasures against them. However, there are some works where the authors have mentioned various attacks on supply chains. Reed et al. (2014) [10] have broadly described supply chain attacks related to hardware, software, firmware, and system data. They have provided the origins and associated supply chain vulnerabilities of these attacks. In addition to that, they have also recommended some mitigation approaches to tackle these attacks.

Although different types of security attacks and their defensive approaches have been widely studied in the above-mentioned areas related to supply chains, there are still opportunities for further research in that field. Most of the research works conducted so far are not directly related to supply chain attacks, whereas they highlighted attacks on particular security devices rather than the whole supply chain.

2.3. Background on blockchain

Blockchain is a digital distributed ledger technology. It refers to a chain of blocks where all blocks contain digital information, and each block is connected to its previous block, hence the name blockchain. Blockchain is an emerging technology, and the underlying techniques are vast. This subsection describes various vital properties of a blockchain.

2.3.1. Features of blockchain

A. *Basic Structure of Blockchain:* A blockchain network consists of several nodes that record and share all transactions that occur within the network [11]. A single block may incorporate multiple transactions. Before adding the new suggested block to the blockchain, the network nodes verify that the block contains valid transactions and refers to the correct previous block through a cryptographic pointer. This whole process is determined by the consensus mechanism adopted by the blockchain network [12,13].
Fig. 2 illustrates the basic structure of a blockchain.
A block contains multiple transactions in the block body. The block header includes parameters like the current block's hash, the previous block's hash, the timestamp, and other information. Each block indicates its previous block to maintain the proper sequence among the blocks and create a valid blockchain. This indication is done by the 'hash of the previous block' field, the cryptographic pointer mentioned earlier. The very first block (termed as the genesis block) in the blockchain cannot refer to any previous block, and for that reason, the 'hash of the previous block' field of the genesis block is necessarily zero (0) [13,14].

B. *Blockchain Types:* Based on the permission system used, blockchain technology can be broadly categorized into the following three types.

- *Public:* A public blockchain is a truly decentralized permission-less blockchain. It is an open distributed ledger where any node can join the network, conduct transactions, and participate in the consensus mechanism without any authentication from the central agency [15]. The transaction speed of a public blockchain is slow compared to other blockchains.
- *Private:* A private blockchain is a permissioned blockchain. It is a controlled distributed ledger where joining the network is restricted. Not every node can participate in this blockchain; a Certificate Authority determines who can join the network [15]. All permissioned nodes are authenticated, and their identities are known to the whole network [11].

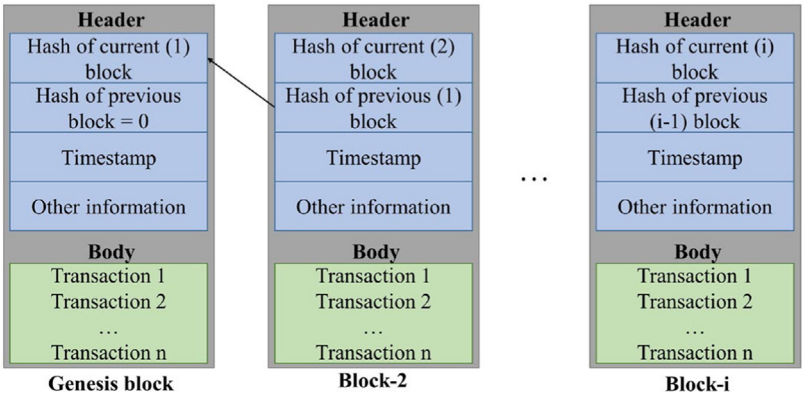


Fig. 2. Basic structure of blockchain.

- *Consortium:* Sometimes, it is necessary to coordinate both public and private types of blockchain rather than using completely public or completely private ledger architecture. A consortium blockchain is the bridge between the public and private blockchains and thus can be referred to as a semi-private blockchain. Here, the blockchain is not controlled by a single entity, as in the case of a private blockchain; instead, it is controlled by a group of approved individuals. In a consortium blockchain, access is granted to a group of pre-defined nodes on the network. The data in the blockchain can be public or private and can be considered partially decentralized [14,16].

C. *Different Consensus Algorithms:* A consensus algorithm is a procedure through which all the nodes present in the blockchain network reach a common agreement about the current state of specific data in the network. Fundamentally, the consensus algorithms achieve reliability in the blockchain network by establishing trust among unknown peers of the distributed system. The main purpose of the consensus mechanisms is to ensure that every new block added to the blockchain is verified as valid by the majority of the nodes in the blockchain.
There are several consensus algorithms in practice, each with pros and cons. Some widely used consensus algorithms are briefly discussed below.

- *Proof of Work (PoW):* This consensus algorithm's main concept revolves around solving a complex mathematical puzzle and providing the solution. This cryptographic puzzle is bound to a threshold known as the difficulty parameter. The PoW mechanism has special types of nodes, namely miners. Miners perform a resource-intensive computational task intending to generate a PoW that matches the required threshold and presents the block to the other nodes of the network. Once the majority of the nodes in the network verify that the block is authentic, the block is appended to the blockchain [3,17,18].
- *Proof of Stake (PoS):* In PoS, the nodes that want to participate in the block creation process must prove that they own a certain amount of resources. They must lock up this resource as a stake to guarantee that they will behave as per the network rules. The higher the node's stake is, the greater the chance of this node being selected as a validator. The validator will lose its stake if it validates a wrong block, and this way, PoS reduces the possibility of the validator's misbehavior [17–19].
- *Practical Byzantine Fault Tolerance (PBFT):* In PBFT, nodes are sequentially ordered in such a way that one node is elected as a leader node, and others are considered as backup nodes. Honest backup nodes are supposed to follow the instructions of the leader node. The communication level is pretty high among the nodes as they want to eliminate any false information in the network by verifying them through several stages (Request, Pre-prepare, Prepare, Commit, and Reply). If the maximum number of malicious nodes is not greater than or equal to one-third of all the nodes in the system, PBFT can achieve consensus [20,21].
- *Proof of Activity (PoA):* The core idea of PoA is to utilize the best of PoW and PoS algorithms to verify and append a block to the blockchain. This blockchain consensus protocol begins like the PoW algorithm. The difference is that the miners only mine the empty block header (does not refer to transactions). After the miners mine these empty block headers, the system moves toward the PoS algorithm. The header information inside a block indicates a random stakeholder. These stakeholders then mine the blocks and propose them to the network. After being validated by the network, the blocks are added to the blockchain [21,22].

Among the other consensus algorithms, Proof of Capacity, Proof of Burn, Proof of Elapsed Time, etc., can be mentioned.
Blockchain technology is evolving day by day. It moved from Blockchain 1.0 (digital currency) to Blockchain 2.0 (smart contract), and now it is moving toward Blockchain (DApp) and beyond [23]

There are some valid reasons why blockchain is becoming popular day by day. Blockchain technology comes with the following in-built advantageous properties [14]:

A. *Decentralized:* Blockchain technology does not need to rely on centralized authority. Data can be collected, saved, and updated in a decentralized manner by the nodes distributed worldwide.
B. *Transparent:* All existing and new data to be added to the blockchain is visible to every node in the blockchain network. This transparency impedes the attempt of any malicious modification in the blockchain.
C. *Immutable:* The inherent nature of blockchain is that new blocks can be added, but previous blocks cannot be modified. This way, once data is stored in the blockchain will remain intact forever.

D. *Anonymity:* While interacting with other nodes in the blockchain network, one node does not need to trust the other nodes because the whole network has ensured trust. So, nodes can interact with each other anonymously.

2.3.2. Smart contract

One of blockchain's most promising and practical applications is the smart contract. A smart contract is a code where the 'if, then' conditions are written, and the code is deployed over the blockchain network. The real-life use cases of blockchain cannot be imagined without smart contracts. As the name implies, smart contracts need to be 'smart.' The autonomous, distributed code embeds the contractual clauses on the blockchain platform, which does not require monitoring once triggered. This approach reduces the requirement of any trusted third party. A unique address identifies each smart contract. A transaction is required to be sent to that address to activate a smart contract [24]. The blockchain nodes do the verification and validation. If the network nodes agree on conditions, then smart contract events are executed. It requires extreme carefulness while writing the smart contract code. Once a smart contract is deployed on the blockchain, it becomes immutable. Therefore, if there is any bug in the contract coding, there is no way to fix that [25].

2.4. Blockchain related works

As an emerging technology, much research is going on related to blockchain, and these works are gradually enhancing blockchain technology. For instance, Ferna′ndez-Carame′s et al. (2018) [26] have mentioned a few application areas of blockchain apart from cryptocurrencies, such as supply chain management, financial transactions, healthcare, industry 4.0, intelligent transportation systems, energy management systems, telecommunications, defense & public safety, government & law enforcement, farming, data storage, timestamping services, mobile crowdsensing and so on. They have explained how blockchain technology can improve these sectors and discussed the challenges (e.g., privacy, security, energy efficiency, speed, and scalability) of integrating blockchain in these fields. It is highly relevant to mention that blockchain technology is also playing a significant role in solving security issues in areas closely related to the supply chain, such as IoT, Industrial IoT (IIoT), manufacturing, and so forth. Researchers are applying blockchain technology to these fields and constantly trying to make these areas more security attack resilient. In one such work, Kim et al. (2019) [27] have proposed a Blockchain of Things (BoT) model to overcome problems related to the hacking of IoT devices. They proposed a methodology to overcome security vulnerabilities by presenting a color spectrum chain among blockchain consensus algorithms. The blockchain used here stores the authentication status of the IoT devices and operates on various servers of the IoT device. In the server, the color spectrum chain confirms and preserves the device's information and also checks the authentication state of the device. The devices connected to the server are registered in the blockchain through the color spectrum chain and communicated through the authentication step.

In another work, Lin et al. (2018) [28] proposed a blockchain-based system, BSeIn for Industry 4.0, to enforce secure mutual authentication remotely with fine-grained access control. Their system comprises Terminals, Blockchain Network, Cloud, Industrial Network, and Physical Resources. They have integrated blockchain and attribute signatures to authenticate terminals anonymously. In the proposed system, the terminals can submit any request without revealing their identity and determine the gateways' authenticity with the help of the one-time public/private key pair. In addition, the message authentication code ensures that only the requester can extract the response from the authentic gateways. Their research also illustrated the security requirements of such a blockchain-based mutual authentication for Industry 4.0 deployments. Then they explained how BSeIn could ensure these security requirements.

2.5. Supply chains based on blockchain

Finally, I can shed light on some research where the authors have worked on the intersection of supply chain and blockchain. In one such work, Tian (2016) [29] has devised a conceptual traceability system framework for an agri-food supply chain using RFID and blockchain. This system exploits RFID technology to implement data acquisition and sharing in the production, processing, warehousing, distribution, and sales of the agri-food supply chain. The purpose of using blockchain technology is to guarantee that the information shared and published in this traceability system is reliable and authentic. The author claims that his proposed framework helps agri-food marketers enhance their food safety and quality while significantly reducing the losses during logistics. After comparing the proposed system with the traditional agri-food supply chain, he has also highlighted some advantages and disadvantages of adopting RFID and blockchain technology in this system. For instance, tracking, traceability, trust, and anti-counterfeiting are significant advantages, whereas cost and scalability are noteworthy drawbacks.

In another work by Bocek et al. (2017) [30], the authors focused on the pharmaceutical supply chain. They considered the start-up Modum.io AG as the research subject and illustrated how it integrated blockchain into the pharmaceutical supply chain. The system architecture shows how IoT sensors monitor each parcel's temperature and transmit these values to the mobile devices working in the front end. In the back end, blockchain with Ethereum smart contract collects, verifies, and stores these temperatures securely. The authors have also provided a sequence diagram to describe how the whole process is carried out.

Helo et al. (2019) [16] have conducted generalized research on incorporating blockchain into supply chains. Rather than focusing on a particular type of supply chain, they have indicated some fields of supply chains, such as assets, identity, and transactions, where blockchain technology can be applied. They have proposed a blockchain-based logistics monitoring system architecture and performed a software implementation of this system.

From the references mentioned above, it can be said that, in some research works, although the authors have focused on supply chain security attacks, they have yet to propose how to mitigate those attacks using blockchain. In other research works, the authors are mainly interested in blockchain technology, where the supply chain came as only a small subset of the blockchain applications. In the final type of research work, as mentioned above, the authors have actually discussed applying blockchain technology in supply chains. However, they still need to thoroughly investigate the different types of possible attacks on supply chains, and they also should have discussed the various aspects of blockchain in detail.

Some recent research works in the field of blockchain, along with my work, are mentioned in Table 1. Compared to the previous works, my paper aims to provide a comprehensive study where all possible kinds of supply chain attacks have been discussed. Moreover, I have pointed out the countermeasures of these supply chain attacks. Furthermore, I have thoroughly discussed the process of integrating blockchain into supply chains with benefits and probable drawbacks. I have also mentioned some potential solutions for the challenges of integrating blockchain into supply chains. Incorporating all these aspects of the supply chain is unique relative to the reviewed

Table 1
Relevant blockchain research.

Research work in blockchain	Reference
The authors address several application areas of blockchain and explain how blockchain technology can improve these sectors. They also discuss the challenges of integrating blockchain into these fields.	Ferna′ndez-Carame′s et al. (2018) [26]
BLE: A blockchain-connected gateway for Bluetooth Low Energy (BLE) enabled IoT devices to maintain secure and adaptive user privacy.	Cha et al. (2018) [31]
BoT: A Blockchain of Things (BoT) model to overcome the problems related to the hacking of IoT devices. They proposed a methodology to overcome the security vulnerabilities by presenting a color spectrum chain among blockchain consensus algorithms.	Kim et al. (2019) [27]
BSeIN: A blockchain-based system named BSeIn for Industry 4.0 to enforce secure mutual authentication remotely with fine-grained access control.	Lin et al. (2018) [28]
A conceptual framework for agri-food supply chain traceability system using RFID and blockchain technology.	Tian (2016) [29]
They have illustrated how the start-up Modum.io AG has integrated blockchain into the pharmaceutical supply chain for temperature monitoring.	Bocek et al. (2017) [30]
They have indicated some fields of supply chains, such as assets, identity, and transactions, where blockchain technology can be applied. They have performed a software implementation of a blockchain-based logistics monitoring system.	Helo et al. (2019) [16]
Discusses supply chain attacks and countermeasures. Illustrates techniques for integrating blockchains into supply chains, and solutions for performance issues caused by integration.	My work

Table 2
Categorized list of finally selected papers to answer research questions.

Supply chain topic	Subtopic	Reference (Year)
Attacks	Counterfeits	Spink et al. [32] (2013), Guin et al. [33] (2014)
	Physical attacks	Andrea et al. [8] (2015), Mitrokotsa et al. [6] (2010), Goodin [34] (2021)
	Data attacks	Sengupta et al. [35] (2019), Reed et al. [10] (2014)
Countermeasures	Anti-counterfeiting	Al-Bahri et al. [36] (2019), Pathak [37] (2010)
	Physical attacks countermeasures	Aman et al. [38] (2017), *Mitrokotsa et al. [6] (2010), *Andrea et al. [8] (2015)
	Data attacks countermeasures	Ahemd et al. [7] (2017), *Reed et al. [10] (2014)
Blockchain integration		Binance Academy [39] (2021), Lo et al. [40] (2019), Bocek et al. [30] (2017), Mondal et al. [41] (2019), Hepp et al. [42] (2018), Saad et al. [43] (2019)
Integration issues	Centralization	Lin et al. [14] (2017), Courtois et al. [44] (2014)
	Scalability	Juma et al. [45] (2019), Vukolic′ et al. [46] (2016), *Hepp et al. [42] (2018)
	Cost	Longo et al. [47] (2019), Aniello et al. [48] (2019)
	Privacy	Terzi et al. [23] (2019), Xu et al. [49] (2017)
Integration issues' solutions	Scalability solution	Bruce [50] (2014), Ferna′ndez-Carame′s et al. [26] (2018), *Longo et al. [47] (2019)
	Cost solution	*Ferna′ndez-Carame′s et al. [26] (2018), Coinpursuit [51] (2021)
	Privacy solution	Schukat et al. [52] (2014), Hayouni et al. [53] (2016)

*Means the paper has been repeated.

literature. Any person or organization interested in dealing with the supply chain can be familiarized with the possible attacks and their present countermeasures. In addition, they can have the preliminary idea of integrating blockchain in their supply chain to secure their supply chain. Finally, they can be aware of the probable issues of integrating blockchain into the supply chain and their potential solutions.

3. Methodology

I have systematically conducted this review. I have answered some research questions (RQs) related to supply chain security in this paper. The research questions are as follows:

RQ1: What are the present supply chain attacks?

RQ2: What are the state-of-the-art countermeasures of these attacks?

RQ3: How to integrate blockchains into supply chains?

RQ4: What are the drawbacks of integrating blockchains into supply chains?

RQ5: What are the potential solutions for the issues of integrating blockchains into supply chains?

To answer these research questions, I have searched research papers online using the following keywords: supply chain attacks, supply chain attack countermeasures, supply chain blockchain integration, supply chain blockchain integration issues, and supply chain blockchain integration issue solutions.

Then after reading the paper title and abstract, ten (10) papers (from 2010 to 2021) were initially selected from each keyword's search results. Lastly, all the papers were read thoroughly, and the final selected papers are listed by search keywords in Table 2. The papers listed here have some repetition, as one paper might have answers to multiple research questions.

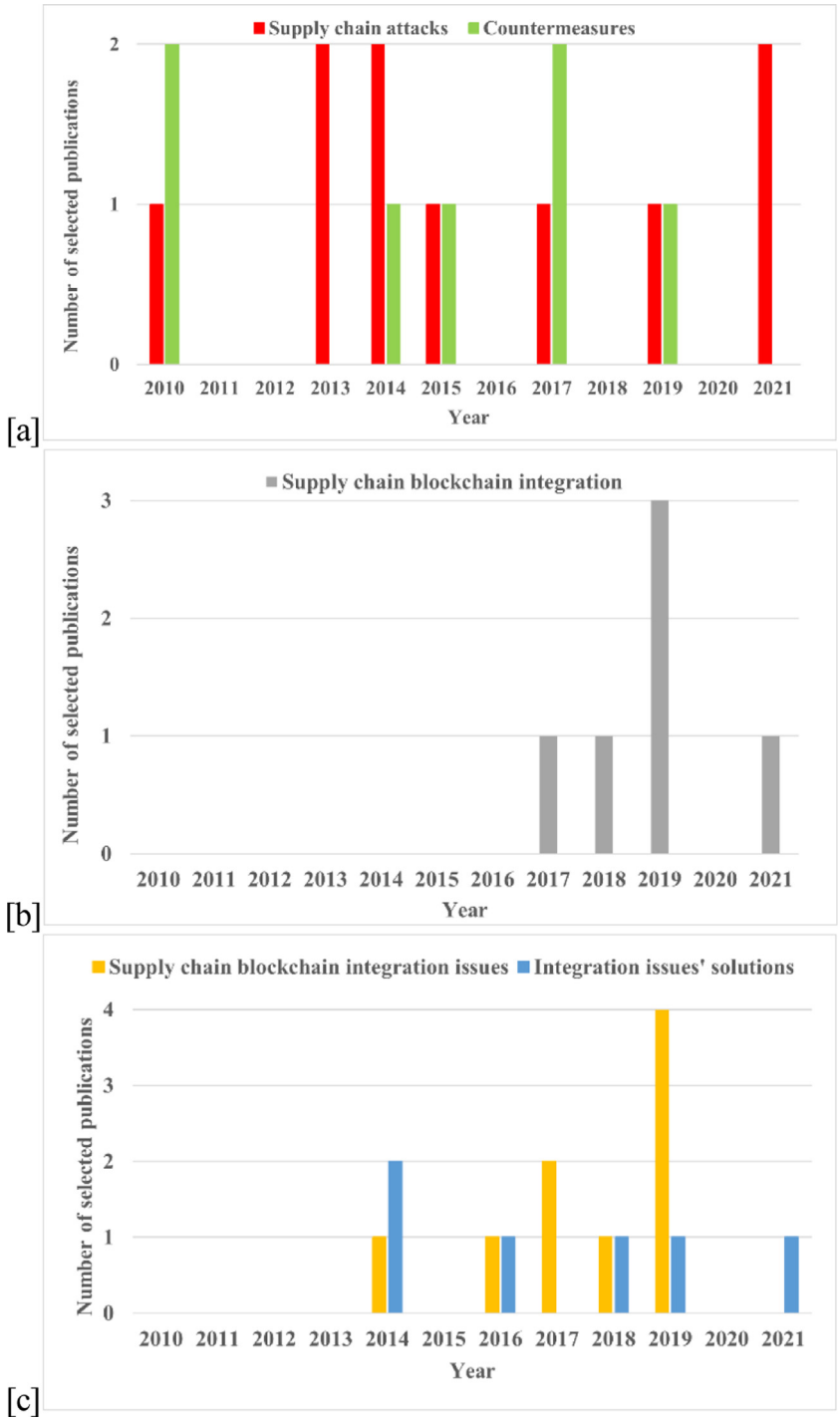


Fig. 3. Number of selected papers (includes repetition) from the year 2010 to 2021 for (a) supply chain attacks and countermeasures, (b) supply chain blockchain integration, (c) supply chain blockchain integration issues, and solutions.

The year-wise distribution of the selected papers is depicted in Fig. 3. A paper repeated within the same topic is counted once, but a paper repeated on a different topic is mentioned separately.

4. Supply chain attacks and state-of-the-art countermeasures

Supply chain security attacks cause a significant threat to modern-day organizations, and these attacks are not only limited to any specific sector but also may affect any organization or industry with a complex supply network. Due to globalization, decentralization, and outsourcing of supply chains, the number of weak points in the supply chains has also increased because of the greater number of entities involved who are scattered worldwide. Basically, there are two types of supply chain attacks. Both types of supply chain attacks with real-life historical examples are discussed below.

The former targets attack the actual supply chains. An attack on the food supply chain can be considered as an example here. Between the years 2006 to 2008, some terrorists deliberately contaminated foods using salmonella or E. coli to attack certain food supply chains. These contaminations took place in the USA; some victims required hospitalization, and a few were dead. [54].

These types of attacks on the food supply chain are most likely intended to create fear and anxiety in the industry, community, or country to provoke economic losses, trade disruption, or political unrest.

The latter use supply chains as a channel to attack numerous connected partners [55]. By identifying and using exposed links, attackers can hop between linked entities, stealing data, spying, or destroying information as they move forward [55]. One of the noteworthy examples was committed in 2014 by the cyber-espionage group 'Dragonfly.' This supply chain-oriented security breach targeted attacking smaller supply chain entities to gain access to larger pharmaceutical/energy suppliers in Europe and North America. Dragonfly used techniques like attaching malware to third-party programs, emails, and websites to gather system information, including the computers' Outlook address book and list of files and programs installed. They also uploaded stolen data, downloaded new files, and ran them on infected computers [56].

Supply chain security should be a high priority for organizations, as a breach within the system could lead to loss of intellectual property, revenue, and inefficient delivery schedules. Delivering unauthorized or tampered products could harm customers and lead to unwanted lawsuits [57]. Supply chains might be affected by both product attacks and cyber attacks. Product attacks include counterfeit products, tampered products, reduced quality, declined manufacturing practices, unauthorized production, etc. On the other hand, cyber attacks refer to vulnerabilities in IT and software systems, like interfering with information and communication, hacking, theft of intellectual property or company data, unauthorized access, malware, etc. [58]. Supply chain security incorporates many parameters (e.g., cargo security, facility security, information management, human resources management, etc.) [59]. Discussing all of them in detail is out of the scope of this paper. I have categorized supply chain security attacks into four major types: counterfeits, physical attacks, data attacks, and general attacks. Their common forms with possible countermeasures and some real examples are discussed in this section.

4.1. Counterfeits

Counterfeit or fake products are the main concern of any supply chain. These products' or components' qualities are significantly degraded than the originals' and compromise the basic purpose of a secured supply chain. The most common types of counterfeit products are as follows [32,33]:

4.1.1. Adulterated

In this type of counterfeit product, one or more component(s) of the product is fake. Adversaries do that to reduce production costs and to represent the product as authentic at the same time.

4.1.2. Recycled

In the case of recycled products, components are taken from a used system, repackaged, and then resold in the market as fresh. These recycled parts are either damaged or with severely reduced performance from the previous usage.

4.1.3. Cloned

An illegal replica of a product is referred to as cloned. In cloning, the counterfeiters copy a design to minimize the product's development cost. Cloning can be accomplished by two means: by reverse engineering or by obtaining IPs illegally.

4.1.4. Overproduced or over-run

Companies contract different factories to produce various components to minimize production costs. When an unfaithful factory produces components in an excess amount outside of the contract and sells them in the open market, the components are referred to as overproduced or over-run.

4.1.5. Defective

Products that were found defective/out-of-specification/rejected during the manufacturing tests might be sold in the open markets intentionally or unintentionally. These components are a severe threat to any sophisticated system.

4.1.6. Information tampered

Faking the quality information of a product is also considered counterfeiting. The actual information of a lower quality product is edited to a higher one. This attack can be categorized into two major types:

A. *Remarked:* Here, marking on the product is tampered with to represent that the product is of better configuration.
B. *Forged documentation:* Documentation of products such as certificates or catalogs is revised to circumvent the customers.

Counterfeit products cause loss of revenue for any industry and degrade the reputation of manufacturers and sellers. An example of counterfeit electronics products can be drawn here to demonstrate the gravity of the situation. In 2008, the FBI seized $76 million of fake Cisco networking equipment, which was sold to the U.S. Navy, the U.S. Marine Corps., the U.S. Air Force, the U.S. Federal Aviation Administration, and the FBI [60].

4.2. Physical attacks

Here, the attacker targets the security devices in the supply chain. Most often, the adversary's prime focus is to take control or shut off these devices. Sometimes, they are also interested in extracting valuable information from these devices. Some physical attacks related to the supply chain are:

4.2.1. Tampering

This type of attack refers to physically modifying a device [8]. Tampering can be modifying the security device associated with the supply chain, like IoT devices or RFID tags, or the actual supply chain products for the cases of electronic devices. This attack concerns both the supply chain's security and the product's quality.

4.2.2. RFID tag disabling

Permanently disabling an RFID tag is another major threat to the supply chain. Tag disabling can be done in a few ways [6]. The most common of them are as follows:

A. *Tag removal:* In this type of attack, tags are removed from the corresponding products. This attack may also be called tag switching when a removed tag from one product is attached to another.
B. *Tag destruction:* The adversaries might destroy the tags permanently by physically damaging them. To perform this attack, the attacker must get close to the tag. Therefore, this attack will likely happen when the tag is not within proper physical security.
C. *KILL command:* This is a particular type of command where the tag owner can disable it with its corresponding password. Similarly, an attacker can permanently turn off or erase data from the tag using this command.

Table 3
Supply chain attacks and their countermeasures.

Attacks	Countermeasures	Reference
Counterfeits	Analytical techniques: X-ray, microscopy, and chemical analysis	Shearon (2019) [62]
	ID technologies: barcodes, QR codes, RFID, NFC, and digital watermarking	Al-Bahri et al. (2019) [36]
	DOA	Al-Bahri et al. (2019) [36]
	APL	Pathak (2010) [37]
Physical attacks	PUF	Aman et al. (2017) [38]
	Effective password management. CRP authentication	Mitrokotsa et al. (2009) [6]
	Secure communication	Andrea et al. (2015) [8]
Data attacks	Error detection mechanisms such as parity bit, checksum, etc. for each device.	Ahemd et al. (2017) [7]
	Cryptography (e.g., digital signatures, encryption).	Reed et al. (2014) [10]

4.2.3. Unauthorized tag cloning

This is one kind of integrity attack. A tag's identifying information and incorporated data are captured and implanted into a new tag by the adversaries [6,61]. Although the cloned tag has the same attributes as the original one, the internal physical configuration of the authentic tag is not replicated here [8].

RFID is the most widely used among several security devices in the supply chain. Many global organizations, such as Walmart, Gillette, Procter and Gamble, and Coca-Cola, are implementing RFID in their supply chain. As the number of RFID tags increases, the possibility of physical attacks on RFID tags is also growing. Researcher Chris Paget has demonstrated with his $250 proof-of-concept device that it is possible to sniff and clone RFID tags without their owners' knowledge [34]. If this technology comes into the hands of adversaries and they apply it in the supply chain RFIDs, then the security of the supply chain might be compromised.

4.3. Data attacks

As the supply chain grows bigger and bigger, the data linked with the supply chain also increase in volume. Data consistency throughout the supply chain is one of the prime requirements for a resilient supply chain. Some noteworthy attacks on supply chain data are discussed below:

4.3.1. Data breach

Data breach results from attacks on data integrity. Inappropriate disclosure of personal or confidential data may occur when the authorization or control of access is compromised [35].

4.3.2. Information leakage

Confidential information stored in the RFID tag can be hacked in several ways. The below-mentioned attacks are the most related to my research:

A. *Unauthorized tag tracking:* This attack concerns the privacy of the tag. The location of the tags can be traced by the adversaries [61]. This attack will likely happen when the authentication between the tag and the reader is compromised [63].
B. *RFID unauthorized access:* Unlike tag modification, this attack focuses on extracting the information stored in the tag. Malicious personnel can read, modify, or delete data present on the RFID nodes [8]. A weak authentication mechanism is a primary reason for this attack to occur.
C. *Person's privacy threats:* RFID tags can be used to collect the buyers' personal information. Personal information may refer to the location of the buyer, which can be achieved by coupling the tag with a surveillance system [64]. Purchasing habits of the buyer might be considered as personal information as well [6].

4.3.3. Malicious insertion of system data/information

This attack refers to inserting erroneous data into the supply chain system. The substitution and alteration of vital data, such as design, manuals, architectures, roadmaps, etc., also fall under this category [10].

The average number of third parties with sensitive information access is increasing daily for any organization. Data attacks from any party may expose the organization to high threats. A study conducted by the Ponemon Institute in 2018 found that 56% of organizations suffered a data breach caused by one of their vendors [65].

4.4. General attacks

Apart from the above-mentioned supply chain attacks, several cyber-attacks are quite general and are not solely designed for supply chains. Discussing all of them with possible countermeasures in detail is beyond the limitation of this paper. A few of them are briefly mentioned below:

1. **Different Denial of Services** *(such as RF interference/ Jamming [6,7], sleep denial attack [7,8], permanent Denial of Service (PDoS) [66], passive interference [6], distributed denial of service (DDoS) [67], replay attack [9])*,
2. **Side channel attack** [6,8],
3. **Spoofing attacks** [7,68],
4. **Different sniffing attacks** *(e.g., traffic analysis attack [6,8], password sniffing [68])*,
5. **Sybil attack** [8],
6. **Malware** [10],
7. **Malicious insertion of firmware** [10],
8. **Routing information attacks** [8,69],
9. **Communication link tampering** *(such as selective forwarding [9], sinkhole attack [7,9,70], wormhole attack [9,71], fake node injection [7])*,
10. **Covert channels** [72],
11. **Buffer overflows** [6].

Some major supply chain attacks and their corresponding state-of-the-art countermeasures are highlighted in Table 3.

4.5. Present countermeasures for counterfeiting

Until now, counterfeits have been tried to be prevented by different security measures, informative labeling, and tamper-proof packaging. In addition, several analytical techniques such as X-ray, microscopy, and chemical analysis are used to detect counterfeit products [62]. Any anti-counterfeiting system must have a physical identifier for each product. Physical identifiers are generally two types: covert and overt [73]. Many identifying technologies such as barcodes, QR codes, RFID tags, NFC tags, LASER security marks, and digital watermarking are in practice now to perform anti-counterfeiting. As counterfeiters are getting smarter daily, researchers are working increasingly on anti-counterfeiting.

In one such work, Al-Bahri et al. (2019) [36] have proposed an anti-counterfeiting system based on digital object architecture (DOA). The manufacturer (the originator) wants to convert the product's data into a digital object and requests the handle generator. The handle generator responds with a handle, a unique identifier for the digital object. The digital identifier is encoded in a physical identifier, and the physical identifier is then attached to the desired product. The digital identifier is retrieved by decoding the physical identifier and compared with a trusted reference to verify the product's authenticity.

Pathak (2010) [37] has devised a mechanism where the counterfeit product is detected, and the source of the counterfeit in the supply chain can be pinpointed. A new type of product label based upon digital signatures named authenticated product label (APL) is introduced here. APLs are attached to the goods as they move along the different stages of the supply chain. Although APLs can only be created by the producer, they can be easily verified by anyone in the supply chain. The producer has a database of all the APLs. If there is any verification request due to an APL mismatch, the producer looks up the database to locate the origin of the counterfeit.

4.6. Present countermeasures for physical attacks

Much research has been done and continues to be done to defeat physical attacks. The most relevant countermeasures against physical attacks are discussed below:

Aman et al. (2017) [38] have proposed a PUF-based authentication mechanism in their work. They used the hash of the device's ID and challenge-response pair for authentication. They have shown that their protocol can be used to combat tampering and malicious code injection by making the following assumptions: PUFs cannot be separated from the device's microcontroller, and an attacker cannot eavesdrop on the communication between the microcontroller and the PUF.

In another work, Andrea et al. (2015) [8] have shown that RFID unauthorized access can be addressed by establishing secure communication between devices, implementing routing security, and securing the user data in the devices. Secure communication can be ensured by exploiting network authentication, point-to-point encryption, and cryptographic hash function. A secured routing might be achieved by using multiple paths, encrypting, and hashing routing tables. User data on the device might be protected by data authentication and by keeping data confidentiality and integrity intact.

4.7. Present countermeasures for data attacks

The consequences of vital supply chain data getting into the wrong hands might be detrimental. A few works dealing with supply chain security are mentioned here.

In one such work, Ahemd et al. (2017) [7] have explained that each device in the network should come with an error detection mechanism to minimize the risk of data tampering. Some unique error detection mechanisms are parity bit, checksum, etc. They have also suggested applying the cryptographic hash function to make the data more secure. In addition, different authentication mechanisms, such as point-to-point encryption, can be exploited to achieve data privacy by preventing illegal access to the network nodes.

In another work, Reed et al. (2014) [10] discussed how cryptography can be utilized to limit the malicious insertion of system data. Digital signatures, encryption, checksums, and/or other cryptographic techniques can be used to verify the source authenticity of all received data/information. Additionally, critical and sensitive system information concerning the design, development, maintenance, and delivery is assessed for trustworthiness. This vital data/information is monitored from origination to storage and delivery to ensure that the integrity of the information is not violated.

5. Integrating blockchains into supply chains

A supply chain is a network of suppliers, carriers, wholesalers, retailers, and customers [47]. The flows of goods and information among these entities are the main activities in a supply chain. Supply chain risks lie in the product's origin, processing, and shipping journey. Transparency and traceability need to be enhanced to mitigate those risks. The users also desire easy verifiability of the product's integrity throughout the whole supply chain. Data need to be collected accurately and stored securely to ensure data integrity; third parties currently perform these tasks through centralized information depositories [13].

A blockchain-based supply chain is a capable solution to the issues mentioned above. A decentralized ledger technology like blockchain can be applied in supply chains to track all the activities within the supply chain network, such as which action is being performed by whom, when, and where. Every entity in the supply chain will be able to track product shipments, deliveries, and progress, and this information will be saved in a distributed fashion. Therefore, a blockchain-based supply chain can ensure traceability and provide authentic information about the product's quality [74]. Many mainstream industrial supply chains (luxury goods, foods, medicines, etc.) already use blockchain. Among these supply chains, diamonds and luxury watches can be considered as examples to explain blockchain integration into supply chains.

As diamonds are one of the most expensive luxury goods, complete transparency along the supply chain is highly desirable. Blockchain can provide a reliable tracing of diamonds throughout the supply chain. As an example, the blockchain technology supported (BTS) platform Everledger [75] uses blockchain with artificial intelligence, IoT, and other technologies to create a digital twin of every diamond. To improve transparency, the diamond's information on the origin, cutting process, general characteristics, measurements, and ownership throughout the life cycle are recorded on the blockchain, eventually ensuring diamond provenance [76].

Another example of luxury goods is luxury watches. Customers expect product provenance to avoid purchasing replica products. Blockchain might bring that to the luxury watch industry. For instance, the Swiss start-up Adresta [77] creates digital certificates containing information on the entire lifecycle of the watch for luxury watches and uses blockchain to store them securely. All following sales, services, repairs, and owners are also registered on the blockchain. Adresta's BTS watch platform provides a tamper-proof and transparent supply chain history of the intended luxury watches [78].

Fig. 4. Binding product information with the product.

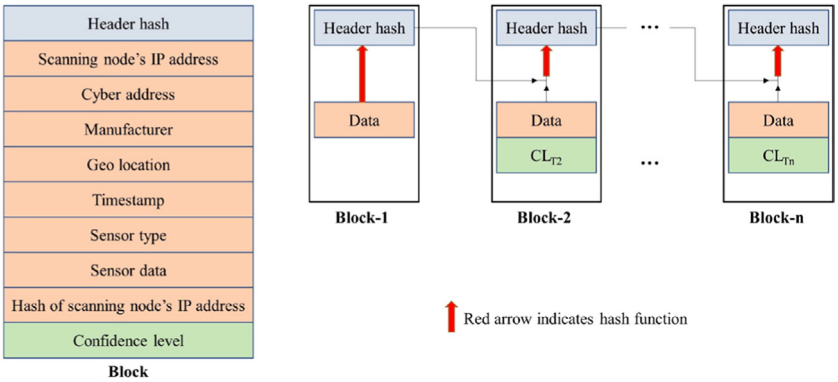


Fig. 5. RFID blockchain.

5.1. How to integrate blockchains into supply chains

While adding blockchain into supply chains provides several benefits, it should be noted that blockchain can only secure the digital representation of the physical item, not the physical item directly [40]. By using different tags and IoT sensors and making them work properly, we can get the location and status of the product and thus take necessary actions when the integrity of the product is compromised. Although the actual product cannot be stored in the blockchain, the product information, such as product description, image, serial number, and product owner's credentials, can be easily stored in the blockchain [79,80].

In order to bind a product of the physical realm to its digital twin in the digital realm, each product must have a unique cryptographic identifier (such as a serial number), which needs to be stored in the blockchain. Later, the identifier is used to authenticate the physical product in several supply chain stages. The physical identifier (i.e., the tag containing the cryptographic identifier) must be provided with either physical security or a unique unclonable fingerprint to ensure the cryptographic identifier is not forged.

Fig. 4 provides a basic visualization of how product information can be bounded with the actual product.

Different tagging techniques, such as barcodes, QR codes, RFID, and NFC, are used to link the physical item to its digital representation. But the major drawback of these techniques is that they can be copied [40]. Therefore, it would be possible that counterfeiters could add the tracking history of a genuine product to their fake products. That is why physical security must be ensured, or a unique fingerprint such as Physical Unclonable Function (PUF) should be used to avoid this attack, as mentioned earlier.

A transaction is created in the blockchain with all the necessary information to register the ownership of a product [81]. Ownership becomes immutable once a product is registered in the blockchain [79]. Later, as the product passes through the supply chain, every time the physical identifier is scanned, the ownership of that product is transferred using smart contracts. This way, it is possible to identify which supply chain party had that particular product at a specific time, and thus the authenticity and transaction integrity of the physical item is maintained.

It should be noted that the blockchain cannot access the data itself, which is outside of the blockchain network. Here, the blockchain oracles come into play. A blockchain oracle is a mechanism that fetches the off-chain data from the external world to the blockchain network. Blockchain oracles serve as bridges between blockchains and the outside world. In other words, they provide a link between off-chain and on-chain data [39]. The blockchain oracle also needs to be connected to APIs (Application Programming Interfaces), which can interact with different IoT devices [40].

5.1.1. Block creation for transactions

After providing the elementary idea of integrating blockchain with the supply chain, I would like to demonstrate how a new block is created for supply chains. To do that, I have considered the research work of Mondal et al. (2019) [41]. A test prototype of the RFID integrated sensor is used in this paper for the food supply chain (FSC). The RFID-integrated sensor can be attached to a food package to extract information regarding the package throughout the FSC.

The sensor, along with the RFID, is termed as "sensorID". The node that scans a sensorID, and collects and processes data, is defined as "terminal". The scanning of a sensorID by a terminal is termed as "transaction". Once a transaction is validated based on the consensus of participating terminals, the transaction is converted into a "block" and included in the blockchain. Each packaged food product with an embedded sensorID travels through multiple transactions at different terminals, from packaging through transportation, storage, and finally to a consumer for purchase. A data block is created containing the information about the package at each valid transaction.

The blockchain data is stored individually in all nodes, and once a new block is added, it is updated in all the nodes. The consumer can scan the sensorID and obtain the product details, such as the physical conditions of the package at different locations and times, from the blockchain.

In this architecture, the authors have used dual addressing: cyber address and RFID address. The cyber address is public and stored in the blockchain memory. The RFID address is a physical address that is private and specific to a food package. Additionally, the physical and cyber addresses should be linked to each other so that the cyber address can be derived from the physical address, but the inverse operation is computationally expensive.

Their proposed block structure is shown in Fig. 5. The block consists of the header hash value, the transaction data information, and the block level confidence value. The transaction

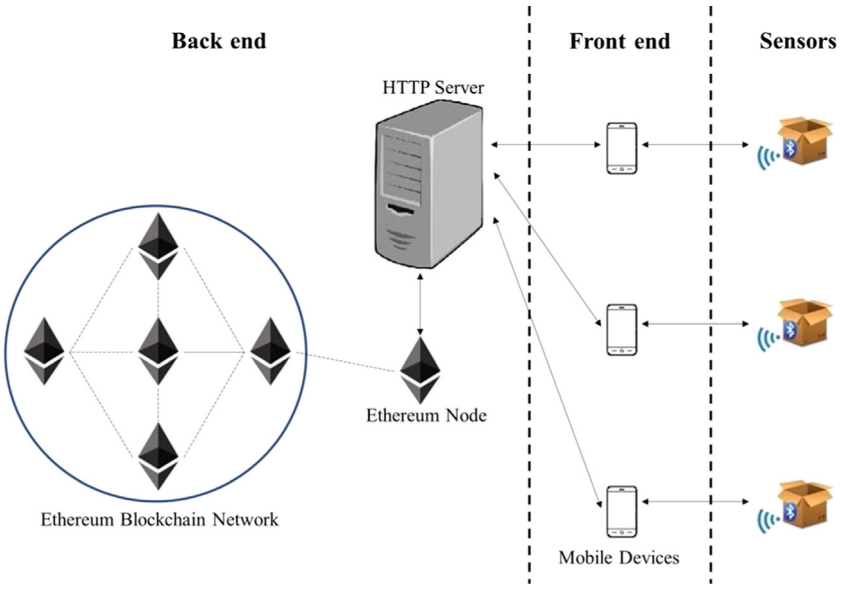


Fig. 6. Modum.io AG system architecture.

data information can be segmented into (1) cyber address of the sensorID; (2) manufacturer of the sensorID; (3) geolocation of the place of the scan; (4) timestamp of the scan; (5) sensor type; (6) sensor data; (7) hash of the scanning node's IP address; and (8) encrypted information of the IP address of the scanning terminal. Anyone with a valid key can decrypt the scanning node's IP address.

5.1.2. System architecture

To conduct a case study on a company's system architecture with blockchain integrated into the supply chain, I have considered the Zurich-based pharmaceutical start-up Modum.io AG. The modum.io AG system architecture is divided into back end, front end, and IoT sensor devices, as shown in Fig. 6.

They have used the Ethereum blockchain network to verify temperature data registered in the front end. The purpose of the HTTP server is to link the blockchain network and front-end users and create and modify smart contracts. The end users use mobile devices to register new shipments and track/send temperature data records to the server. Temperature sensors compatible with Bluetooth Low Energy (BLE) technology are configured to transmit data every 10 min to a mobile device. The sensor has both identification and sensing capabilities, which allows for acquiring precise temperatures at specific points.

In the back end, for every new shipment or group of medical products, a smart contract is configured and deployed on the server side to ensure the temperature requirements. The server hosts an Ethereum node that participates in the Ethereum network and communicates with the server.

In the front end, users can register new shipments using a mobile phone. A suitable API should be used to allow mobile devices to upload the temperature measurements recorded by the sensor to the server. The mobile devices can start and stop the measurements (using BLE), read the raw temperature data, and send it to the HTTP server.

A track-and-trace number (attached to the packet, represented by a barcode) must be associated with the sensor device's MAC address (represented by a QR code). The mobile device captures both with its camera. Then the mobile device starts the temperature measurements on the sensor device and sends the track-and-trace number/MAC address association to the server. The server stores the association, creates, and broadcasts the smart contract, and stores the smart contract ID on the sensor device. Now the sensor device can be placed inside the medical product's packet at strategic points. The sensor device records the temperature and stores it in its internal memory. After receiving the packet at the destination, the track-and-trace number is scanned. The mobile device requests the MAC address from the server to connect to the sensor device. Then the mobile device downloads all temperature data via BLE and sends it to the smart contract. Once the smart contract checks the temperature, the temperature can be verified on the Ethereum blockchain to see if it is within the desired specifications [30].

5.1.3. Consensus mechanisms

Consensus mechanisms are mainly of two types: lottery-based and voting-based. Examples of lottery-based algorithms are Proof of Elapsed Time (PoET) and Proof of Work (PoW). A few voting-based methods are Redundant Byzantine Fault Tolerance (RBFT) and Paxos. Lottery-based algorithms are preferable when it is required to incorporate a large number of nodes in the network, and voting-based algorithms are utilized when a unique consensus is desired [82]. Section 2.3.1 conducts a detailed discussion on consensus algorithms.

However, researchers often propose modified consensus algorithms while integrating blockchain into supply chains to eliminate the mining cost (and thus eventually reduce the product cost). In one such work [41], the authors have proposed a proof-of-object (PoO)-based new consensus algorithm for the food supply chain. PoO means any node that claims the possession of the physical object must prove it cryptographically. Once a node claims for PoO, other participating nodes verify the claim's authenticity.

5.1.4. Data synchronization

Nodes in a blockchain network might be geographically distributed in several places. The nodes will have to synchronize with each other when a new block is mined to maintain the fundamental property of a blockchain [42]. A blockchain only adds a new block only when the consensus algorithm's set conditions are fulfilled. The overall process can be described in-depth for a PoW-based blockchain.

Assume Alice wants to generate a transaction for Bob. The transaction is broadcast to the entire blockchain network and

temporarily stored in a transaction repository (memory pool). The memory pool is a space allocated in the RAM of a full node that stores and relays transactions to other nodes. Special nodes in the network, known as the miners, are responsible for verifying transactions and computing a block. They search the memory pool and select the transactions of their choice to put into blocks. Then miners compete to solve the cryptographic puzzle for that particular block. Whoever solves the puzzle first is the winner and proposes the new block to the network. After that, every node checks the PoW, and if verified, they append the new block to their own copy of the blockchain [43].

5.2. Handling supply chain attacks by integrating blockchains

Supply chain security refers to the efforts to improve the security of the supply chain. It combines traditional supply chain management practices with the security requirements driven by several supply chain security attacks. It is a common interest that the stakeholders in the supply chain want to improve the overall security of the supply chain. Integrating blockchain into supply chains brings numerous advantages. Blockchain technology can be used to tackle supply chain attacks due to its in-built properties.

I. *Handling counterfeiting:* Counterfeiting can be handled by blockchain in several ways. One approach could be storing only the product ID in the product's tag and keeping the original product information in the blockchain.
Anyone who wants to retrieve the product information will have to scan the tag, get the ID, and use that ID to get product information from the blockchain. Since the adversaries do not have permission to edit the blockchain data, it is considered counterfeit when the information from the blockchain does not match the product. This technique will not work when the original removed or cloned tag is attached to the fake product. How that attack can be handled is explained in the 'Handling physical attacks' subsection.

II. *Handling physical attacks:*
With the help of different tags, sensors, and IoT, blockchain can add physical security to the supply chain products by sharing real-time information about the product's location and condition among different supply chain parties. A system can be designed by establishing a (physical or wireless) link between the tag and the product. The link will be broken if the tag is removed from the product without authorization. Unauthorized removal of the tag will trigger a signal sent and stored in the blockchain. It can be notified to the blockchain nodes immediately, and anyone else willing to get the product information by scanning the replaced (with the same ID) tag later can get the notification as well. In addition, blockchain can also prevent adversaries from cloning an authentic tag and attaching the cloned tags to counterfeit products. To get the product ID, an adversary outside the blockchain must purchase the product. Once the product has been purchased, the history is stored in the blockchain. The next time anyone wants to buy a product with the same ID, it is considered a counterfeit.

III. *Handling data attacks:* The prime concern of today's supply chain is data attacks. As the supply chains are growing bigger and bigger, attacks on supply chain data are also increasing due to the involvement of several parties and exposed weak points. Data attacks can be prevented by keeping the company-related sensitive information in a permissioned blockchain. Anybody willing to get the product information must join the blockchain first by getting permission and then accessing the information using the ID. Without permission, adversaries cannot retrieve or insert any product-related information.

5.3. Drawbacks of integrating blockchains into supply chains

Successfully integrating blockchain into supply chains is not everything. There are some challenges as well in the process of integrating blockchain into supply chains. Even though blockchain technology comes with several benefits, there are a few drawbacks of this technology that cannot be overlooked. The most important of them are discussed below.

5.3.1. Centralization

Blockchain system uses distributed consensus algorithm. However, there is always a threat of this consensus mechanism being centralized. Malicious nodes can join together and, being the majority, might take control of the network. This way, the group of adversaries will have a higher probability of being selected as miners/validators [44]. They may split the block rewards or transaction fees according to the proportion of their contribution or even manipulate the transactions occurring within the blockchain network [14].

5.3.2. Scalability

Attacks on blockchains are only a possibility, but blockchains will undoubtedly go through some scalability issues. Scalability refers to the capability of the network to handle the number of transactions per second. Every moment, several transactions happen within blockchain networks. As a result, blockchains are growing, and the data in blockchains are increasing. Collecting, processing, and storing these data requires much time and substantial computational power [83]. Things get even more complicated when a node with a lower capacity wants to run this massive system with limited resources. Private blockchains are more scalable compared to public blockchains. This is because, in public blockchains, all nodes perform identical responsibilities, whereas, in private networks, different tasks are assigned to different nodes, thus improving performance [45].

Public permissionless blockchains (e.g., Ethereum) have very limited throughput, whereas consortium blockchains (e.g., BFT-based blockchains) can commit tens of thousands of transactions per second with some minor performance imperfections [46].

Ethereum can currently process only about 15 transactions per second [42]. Let us examine whether this number is sufficient for the practical integration of blockchain into the supply chain. If we assume that each person in the United States of America consumes a particular product at least once a month, then around 328 million products need to be tracked. That single product will have to travel through several supply chain stages, such as manufacturer, distributor, retailer, seller, and buyer. Hence, the product will change hands at least four times, which means four transactions will be necessary for each product. After calculation, we can see that a minimum of 506 transactions per second will be required for a single product just in the USA.

5.3.3. Cost

Whenever a transaction happens within a public blockchain network, a transaction fee must be paid to process that transaction. This transaction fee is utilized to incentivize the miners/validators of the blockchain [47]. This incentive will motivate nodes to mine/validate more blocks. Blockchain often uses protocols where miners/validators are encouraged to mine/validate blocks with more transaction fees. On the other hand, if a consensus algorithm such as PoW is used, it will require miners to use extensive computational power, eventually affecting the cost of the blockchain.

Regarding blockchain cost-effectiveness, consortium blockchains are preferable to public permissionless blockchains. Consortium blockchains eliminate transaction fees. For instance, submitting transactions in Hyperledger Fabric is entirely free, whereas supply chain tracking solutions based on Ethereum have a per-transaction cost [48].

5.3.4. Privacy

Public permissionless blockchains such as Bitcoin and Ethereum [84] allow anyone to join the network. Although this creates an entirely transparent network, which is required for some supply chain use cases, this type of uncontrolled data exposure might be unwanted when data privacy is a top priority. In other words, there are better solutions than public blockchains for cases where sensitive company information should be kept secret from business competitors. From the perspective of the global supply chain, which consists of multiple parties, consortium blockchains might be utilized here. Permissioned private blockchains like Quorum and Hyperledger have been developed for that purpose [23]. Some other blockchain platforms support the deployment of consortium or private blockchains, e.g., Multichain and Eris [49]. The networks formed by these frameworks are private and require permission for each participant to provide the privacy needed. Although the permissioned blockchain may address this issue, it makes the system more centralized [23].

Over the past few years, supply chains have gone through massive advancement, and they are improving more and more daily. The unique features of blockchains can add a new dimension to supply chains. However, the inherent issues of blockchains need to be addressed for efficient integration.

6. Possible solutions and future research

As mentioned earlier, there are several challenges while integrating blockchain into supply chains. Researchers are trying to address these challenges. Adversaries are also attacking a few of the proposed solutions. Some of the noteworthy solutions for the above-mentioned drawbacks are discussed below:

6.1. Solution for scalability issue

The issue of blockchain scalability can be solved using mini-blockchain. The mini-blockchain is just a usual blockchain, except that copies of historic blocks are discarded. This type of blockchain uses an account tree, which stores the current state of every blockchain user. Thus, only the most recent transactions are stored on the blockchain, lowering a full node's computational requirements [50].

An alternative solution could be using lightweight nodes. These nodes can perform blockchain-based transactions but do not necessarily store the blockchain. They only keep the block header for the verification of a block. This approach requires some full nodes to maintain the blockchain for the resource constrained lightweight nodes [26].

Another proposed solution is to store the original data in off-chain data storage (such as IPFS, SWARM, or conventional databases) and store only the hash of the data in the blockchain. Anyone with access to the hash stored on the blockchain can easily verify the origin and authenticity of data by checking whether the data map onto a given hash value [47].

6.2. Solution for cost and energy consumption

Most blockchain technologies are power-hungry mainly because of the mining protocols used. For instance, PoW is very power-consuming. In order to move towards more energy-efficient solutions, other less power-consuming consensus algorithms might be used.

Apart from that, new hashing algorithms are also being developed, which are less energy-consuming. A few recent hashing algorithms are Scrypt, X11, Blake-256, and Myriad [26]. The lower the hash rate (hash/second) required for successful mining, the greener the mining process will be. An example can be drawn here to illustrate the scenario: for successful mining SHA-256 often requires hash rates of gigahashes per second (GH/s) range or higher, whereas Scrypt's hash rates for successful mining usually range in between kilohashes per second (KH/s) to megahashes per second (MH/s) [51].

6.3. Solution for privacy issue

One possible solution for addressing the privacy issue associated with blockchain might be Zero Knowledge Proof (ZKP). ZKPs are challenge/response authentication protocols in which parties are required to provide the correctness of their information without revealing the information. During the authentication procedure, a prover must respond to challenges issued by a verifier over several accreditation rounds. The prover must be able to answer all the challenges to prove their identity. The verifier's confidence in the prover's identity increases every round. In this type of protocol, the verifier cannot extract any secret from the authentication procedure. On the other hand, the prover cannot cheat the verifier because the protocol is repeated if the verifier is not satisfied [52].

Another way to deal with the privacy issue could be homomorphic encryption (HE). HE is a form of encryption that allows someone to perform calculations on encrypted data without decrypting it. The result of the computation is in an encrypted format. When decrypted, the output is the same as if the operations had been performed on the unencrypted data. The main advantage of these techniques is that they can provide end-to-end privacy and allow third-party services to process a transaction without revealing unencrypted data [53].

However, some shortcomings of integrating blockchain into supply chains (e.g., the possibility of centralization) still need to be appropriately addressed and require further research.

Table 4 suggests different blockchains preferable for a particular type of performance. This table also describes some solution techniques for those performance issues.

7. Conclusion

Supply chains are complex systems. Several parties are directly or indirectly connected to a single supply chain. As the number of connected parties grows, the complexity of supply chain management increases. There will be inherent challenges with the growing number of involved supply chain entities. For instance, all the relevant parties will want to continuously share and access product-related information transparently in real-time using a common platform. However, apart from these challenges, there might be several attacks on the supply chain. Notable supply chain attacks include counterfeiting, physical attacks, data attacks, and so on. These attacks will impact several supply chain concerns, such as privacy, trust, authentication, and access control.

Blockchain technology seems to be a perfect solution to the issues mentioned above since it establishes a shared, distributed, transparent, and immutable record of data that can be accessed by anyone who is permitted. Deploying blockchains in the supply chain management systems can address issues like counterfeiting, origin tracking, and lack of trust among supply chain parties. Therefore, exploiting blockchain technology can facilitate supply chain management by solving several challenges.

In this context, I have organized my research work sequentially, discussing both the attacks on supply chains and their countermeasures. I have also explained the integration process of blockchain into the supply chain. Finally, I have illustrated the drawbacks and potential solutions of integrating blockchain into supply chains.

Table 4
Solution for different blockchain performance issues.

Performance	Preferable blockchain type	Reference	Solution	Reference
Scalability	Consortium blockchains e.g., BFT-based blockchains	Vukolic′ (2016) [46]	Mini-blockchain	Bruce (2014) [50]
			Lightweight nodes	Ferna′ndez-Carame′s et al. (2018) [26]
			Keeping the original data in off-chain and only the hash in the blockchain	Longo et al. (2019) [47]
Cost	Consortium blockchains (e.g., Hyperledger Fabric)	Aniello et al. (2019) [48]	Different consensus algorithms	King et al. (2012) [19], Bentov et al. (2014) [22]
			Hashing algorithm that requires fewer hash rate	Ferna′ndez-Carame′s et al. (2018) [26]
Privacy	Permissioned private blockchains like Quorum and Hyperledger; or consortium blockchains (e.g., Multichain and Eris)	Terzi et al. (2019) [23]	ZKP	Schukat et al. (2014) [52]
			HE	Hayouni et al. (2016) [53]

The RQs asked in the Methodology Section were answered throughout the paper:

***RQ1:* What are the present supply chain attacks?**

RQ1 was answered in Section 4.

***RQ2:* What are the state-of-the-art countermeasures of these attacks?**

RQ2 was also answered in Section 4.

***RQ3:* How to integrate blockchains into supply chains?**

RQ3 was answered in Section 5.1.

***RQ4:* What are the drawbacks of integrating blockchains into supply chains?**

RQ4 was answered in Section 5.3.

***RQ5:* What are the potential solutions for the issues of integrating blockchains into supply chains?**

RQ5 was answered in Section 6.

My work is the only work so far that discusses all the above-mentioned aspects of the supply chain sequentially in detail. Although my work provides almost a complete study on blockchain for the security of supply chains, there are still promising opportunities in this field in which future research can be carried out.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article

References

[1] David Closs, John McConnell, Edmund McGarrell, Enhancing Security Throughout the Supply Chain, in: Special Report Series, 2004.

[2] Kari Korpela, Jukka Hallikas, Tomi Dahlberg, Digital supply chain transformation toward blockchain integration, in: Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.

[3] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009, Cryptography Mailing list at https://metzdowd.com.

[4] Roque Torres-Sánchez, María Teresa Martínez-Zafra, Noelia Castillejo, Antonio Guillamoń-Frutos, Francisco Artés-Hernández, Real-time monitoring system for shelf life estimation of fruit and vegetables, Sensors 20 (7) (2020).

[5] Tiago M. Fernáendez-Caramés, Oscar Blanco-Novoa, Iván Froiz-Míguez, Paula Fraga-Lamas, Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management, Sensors 19 (10) (2019) 2394.

[6] Aikaterini Mitrokotsa, Melanie Rieback, Andrew Tanenbaum, Classifying RFID attacks and defenses, Inf. Syst. Front. 12 (2010) 491–505.

[7] Mian Ahemd, Munam Shah, Abdul Wahid, Iot security: A layered approach for attacks defenses, 2017, pp. 104–110.

[8] Ioannis Andrea, Chrysostomos Chrysostomou, George Hadjichristofi, Internet of things: Security vulnerabilities and challenges, in: 2015 IEEE Symposium on Computers and Communication, ISCC, IEEE, 2015, pp. 180–187.

[9] Pal Varga, Sándor Plósz, Gabor Soos, Csaba Hegedus, Security threats and issues in automation Iot, 2017.

[10] Melinda Reed, John F. Miller, Paul Popick, Supply Chain Attack Patterns: Framework and Catalog, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 2014.

[11] Tien Dinh, Ji Wang, Gang Chen, Rui Liu, Beng Ooi, Kian-Lee Tan, Blockbench: A framework for analyzing private blockchains, 2017.

[12] Konstantinos Christidis, Michael Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 1.

[13] Rita Azzi, Rima Kilany, Maria Sokhn, The power of a blockchainbased supply chain, Comput. Ind. Eng. 135 (2019).

[14] I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges, Int. J. Netw. Secur. 19 (2017) 653–659.

[15] Lakshmi Sankar, M. Sindhu, M. Sethumadhavan, Survey of consensus protocols on blockchain applications, 2017, pp. 1–5.

[16] Petri Helo, Yuqiuge Hao, Blockchains in operations and supply chains: A model and reference implementation, Comput. Ind. Eng. 136 (2019).

[17] GeeksforGeeks, Consensus algorithms in blockchain, 2021, http://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/. (Online; Accessed 28 March 2021).

[18] Md. Sadek Ferdous, Mohammad Chowdhury, Mohammad Hoque, Alan Colman, Blockchain consensus algorithms: A survey, 2020.

[19] S. King, Scott Nadal, Ppcoin: Peer-to-peer crypto-currency with proof-of-stake, 2012.

[20] Miguel Castro, Barbara Liskov, Practical byzantine fault tolerance, in: OSDI, 1999.

[21] 101 Blockchains, Consensus algorithms: The root of blockchain technology, 2021, https://101blockchains.com/consensus-algorithms-blockchain/. (Online; Accessed 28 March 2021).

[22] Iddo Bentov, Charles Lee, Alex Mizrahi, Meni Rosenfeld, Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y, SIGMETRICS Perform. Eval. Rev. vol. 42 (3) (2014) 34–37.

[23] Sofia Terzi, Angeliki Zacharaki, Alexandros Nizamis, Konstantinos Votis, Dimosthenis Ioannidis, Dimitrios Tzovaras, Ioannis Stamelos, Transforming the supply-chain management and industry logistics with blockchain smart contracts, 2019.

[24] Bhabendu Mohanta, Soumyashree Panda, Debasish Jena, An overview of smart contract and use cases in blockchain technology, 2018.

[25] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz, On blockchain and its integration with Iot. Challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190.

[26] Tiago Fernández-Caramés, Paula Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.

[27] Seong-Kyu Kim, Ung-Mo Kim, Jun-Ho Huh, A study on improvement of blockchain application to overcome vulnerability of Iot multiplatform security, Energies 12 (2019) 402.

[28] Chao Lin, Debiao He, Xinyi Huang, Kim-Kwang Raymond Choo, Athanasios Vasilakos, Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, J. Netw. Comput. Appl. 116 (2018) 42–52.
[29] Feng Tian, An agri-food supply chain traceability system for china based on RFID blockchain technology, 2016, pp. 1–6.
[30] Thomas Bocek, Bruno Rodrigues, Tim Strasser, Burkhard Stiller, Blockchains everywhere a use-case of blockchains in the pharma supply-chain, 2017, pp. 772–777.
[31] Shi-Cho Cha, Jyun-Fu Chen, Chunhua Su, Kuo-Hui Yeh, A blockchain connected gateway for ble-based devices in the internet of things, IEEE Access PP (2018) 1.
[32] John Spink, Douglas Moyer, Hyeonho Park, Justin Heinonen, Defining the types of counterfeiters, counterfeiting, and offender organizations, Crime Sci. 2 (2013) 8.
[33] Ujjwal Guin, Daniel Dimase, Mark Tehranipoor, Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead, J. Electron. Test. Theory Appl. 30 (2014) 9–23.
[34] Dan Goodin, RFIDs cloned wholesale by $250 eBay auction spree, 2021, http://www.theregister.co.uk/2009/02/02/low_cost_{RFID}_cloner/. (Online; Accessed 29 December 2021).
[35] Jayasree Sengupta, Sushmita Ruj, Sipra Dasbit, A comprehensive survey on attacks, security issues and blockchain solutions for Iot and IIot, J. Netw. Comput. Appl. (2019).
[36] Mahmood Al-Bahri, Anton Yankovsky, Ruslan Kirichek, Aleksey Borodin, Smart system based on DOA Iot for products monitoring anticounterfeiting, in: 2019 4th MEC International Conference on Big Data and Smart City, ICBDSC, 2019, pp. 1–5.
[37] Vivek Pathak, Improving supply chain robustness and preventing counterfeiting through authenticated product labels, in: 2010 IEEE International Conference on Technologies for Homeland Security, HST, 2010, pp. 35–41.
[38] M.N Aman, K.C Chua, B Sikdar, A light-weight mutual authentication protocol for Iot systems, in: GLOBECOM 2017 2017 IEEE Global Communications Conference, 2017, pp. 1–6.
[39] Binance Academy, Blockchain oracles explained, 2021, https://academy.binance.com/en/articles/blockchain-oracles-explained/. (Online; Accessed 31 December 2021).
[40] Sin Kuang Lo, Xiwei Xu, Chen Wang, Ingo Weber, Paul Rimba, Qinghua Lu, Mark Staples, Digital-physical parity for food fraud detection, 2019, pp. 65–79.
[41] Saikat Mondal, Kanishka Wijewardena, Saranraj Karuppuswami, Fnu Nitya Kriti, Deepak Kumar, Premjeet Chahal, Blockchain inspired RFID-based information architecture for food supply chain, IEEE Internet Things J. (2019) 1.
[42] Thomas Hepp, Patrick Wortner, Alexander Schoenhals, Bela Gipp, Securing physical assets on the blockchain: Linking a novel object identification concept with distributed ledgers, 2018, pp. 60–65.
[43] Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles A. Kamhoua, Sachin Shetty, DaeHun Nyang, Aziz Mohaisen, Exploring the attack surface of blockchain: A systematic overview, 2019, CoRR, abs/1904.03487.
[44] Nicolas Courtois, Lear Bahack, On subversive miner strategies and block withholding attack in bitcoin digital currency, 2014.
[45] Hussam Juma, Khaled Shaalan, I. Kamel, A survey on using blockchain in trade supply chain solutions, IEEE Access PP (2019) 1.
[46] Marko Vukolić, The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication, in: Jan Camenisch, Doğan Kesdoğan (Eds.), Open Problems in Network Security, Springer International Publishing, Cham, 2016, pp. 112–125.
[47] Francesco Longo, Letizia Nicoletti, Antonio Padovano, Gianfranco d'Atri, Marco Forte, Blockchain-enabled supply chain: An experimental study, Comput. Ind. Eng. 136 (2019) 57–69.
[48] Leonardo Aniello, Basel Halak, Peter Chai, Riddhi Dhall, Mircea Mihalea, Adrian Wilczynski, Towards a supply chain management system for counterfeit mitigation using blockchain and PUF, 2019.
[49] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, Paul Rimba, A taxonomy of blockchain-based systems for architecture design, 2017.
[50] J.D. Bruce, The mini-blockchain scheme, 2014.
[51] Coinpursuit, http://www.coinpursuit.com/pages/bitcoin-altcoin-SHA-256-scrypt-mining-algorithms/. (Online; Accessed 28 March 2021).
[52] Michael Schukat, Padraig Flood, Zero-knowledge proofs in M2M communication, in: 25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies, ISSC 2014/CIICT 2014, 2014, pp. 269–273.
[53] Haythem Hayouni, Mohamed Hamdi, Secure data aggregation with homomorphic primitives in wireless sensor networks: A critical survey and open research issues, in: 2016 IEEE 13th International Conference on Networking, Sensing, and Control, ICNSC, 2016, pp. 1–6.
[54] Roberto Setola, Maria Maggio, Security of the food supply chain, in: Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference, Vol. 2009, 2009, 7061–4.
[55] VentureBeat, 5 reasons why supply chain security must be on your agenda, 2021, https://venturebeat.com/2020/01/08/5-reasons-why-supplychain-security-must-be-on-your-agenda/. (Online; Accessed 06 April 2021).
[56] BBC, Energy firms hacked by 'cyber-espionage group Dragonfly', 2023, https://www.bbc.com/news/technology-28106478. (Online; Accessed 23 May 2023).
[57] Gavin Wright, Sarah Lewis, Supply chain security, 2021, https://searcherp.techtarget.com/definition/supply-chain-security. (Online; Accessed 29 December 2021).
[58] Kirsten Koepsel, The aerospace supply chain and cyber security: Challenges ahead, 2018, pp. i–vii.
[59] Juha Hintsa, Ximena Gutierrez, Philip Wieser, Ari-Pekka Hameri, Supply chain security management: An overview, Int. J. Logist. Syst. Manag. 5 (2009).
[60] ESG: a division of TechTarget. ESG research report: Cyber supply chain security revisited, 2021, https://research.esgglobal.com/chapters/CyberSupplyChainRevisited/ExecutiveSummary. (Online; Accessed 28 March 2021).
[61] Breno de Medeiros, RFID security: Attacks, countermeasures and challenges, in: Proceedings of the 5th the RFID Journal Conference RFID Academic Convocation, 2007.
[62] C.E. Shearon, A practical way to limit counterfeits, in: 2019 Pan Pacific Microelectronics Symposium, Pan Pacific, 2019, pp. 1–7.
[63] Christian Floerkemeier, Roland Schneider, Marc Langheinrich, Scanning with a purpose – supporting the fair information principles in RFID protocols. Volume 3598, 2005, pp. 214–231.
[64] John Ayoade, Roadmap to solving security and privacy concerns in RFID systems, Comput. Law Secur. Rev. 23 (2007) 555–561.
[65] Maria Korolov, Supply chain attacks show why you should be wary of third-party providers, 2021, http://www.csoonline.com/article/3191947/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-partyproviders.html. (Online; Accessed 28 March 2021).
[66] Data Foundry, What is a permanent Dos (Pdos) attack?, 2021, http://www.datafoundry.com/blog/what-is-a-permanent-dos-pdos-attack. (Online; Accessed 29 December 2021).
[67] Rambus, Industrial Iot: Threats and countermeasures, 2021, http://www.rambus.com/iot/industrial-iot/. (Online; Accessed 29 December 2021).
[68] Matthew Warren, William Hutchsinson, Cyber attacks against supply chain management systems: A short note, Int. J. Phys. Distrib. Logist. Manage. 30 (2000) 710–716.
[69] Wai Chen, Ratul K. Guha, Taek Jin Kwon, John Lee, Irene Y. Hsu, A survey and challenges in routing and data dissemination in vehicular ad-hoc networks, in: 2008 IEEE International Conference on Vehicular Electronics and Safety, 2008, pp. 328–333.
[70] S. Ahmad Salehi, M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, Detection of sinkhole attack in wireless sensor networks, in: 2013 IEEE International Conference on Space Science and Communication, IconSpace, 2013, pp. 361–365.
[71] Khin Sandar Win, Analysis of detecting wormhole attack in wireless networks, Int. J. Electr. Comput. Energetic Electron. Commun. Eng. 2 (2008) 2704–2710, World Academy of Science, Engineering and Technology.
[72] A. Karygiannis, T. Phillips, A. Tsibertzopoulos, RFID security: A taxonomy of risk, in: 2006 First International Conference on Communications and Networking in China, 2006, pp. 1–8.
[73] Dan Jiang, Cheun Chong, Anti-counterfeiting using phosphor PUF, 2008, pp. 59–62.
[74] Nir Kshetri, Blockchain's roles in meeting key supply chain management objectives, Int. J. Inf. Manage. 39 (2018) 80–89.
[75] Everledger, The Everledger platform: Where supply chains meet the blockchain, 2023, http://www.adresta.ch/en. (Online; Accessed 02 May 2023).
[76] Tsan-Ming Choi, Blockchain-technology-supported platforms for diamond authentication and certification in luxury supply chains, Transp. Res. E 128 (2019) 17–29.
[77] Adresta, It's about time, 2023, http://www.adresta.ch/en. (Online; Accessed 02 May 2023).

[78] Christoph G. Schmidt, Maximilian Klöckner, Stephan M. Wagner, Blockchain for Supply Chain Traceability: Case Examples for Luxury Goods, Springer International Publishing, Cham, 2021, pp. 187–197.
[79] Nasdaq, Using the blockchain to track assets for proof of ownership, 2021, http://www.nasdaq.com/articles/using-blockchain-track-assets-proof-ownership-2016-11-30. (Online; Accessed 31 December 2021).
[80] Yannik Goldgräbe, Authenticity and transaction integrity of physical goods, 2021, https://medium.com/magicofc/authenticity-and-transactionsof-physical-goods-a-blockchain-application-c25c02a4b93a. (Online; Accessed 31 December 2021).
[81] BlockchainCan, Blockchain can register physical assets, 2021, http://blockchaincan.com/project/blockchain-can-register-physical-assets/. (Online; Accessed 31 December 2021).
[82] Hyperledger, Hyperledger architecture volume 1, 2021, http://www.hyperledger.org/wp-content/uploads/2017/08/HyperledgerArchWGPaper1Consensus.pdf. (Online; Accessed 31 December 2021).
[83] Ghassan Karame, On the security and scalability of bitcoin's blockchain, 2016, pp. 1861–1862.
[84] Vitalik Buterin, A next generation smart contract & decentralized application platform, 2015.