A Survey on Counterfeits in the Information and Communications Technology (ICT) Supply Chain

Samar Saleh, Rong Lei, Weihong Guo, and Elsayed A. Elsayed

Abstract One of the major threats to the information and communications technology (ICT) supply chain is the introduction of counterfeit parts and components. Global efforts have been intensified to defend against counterfeiters and counterfeit products due to their detrimental impact on the economy, safety, and security. Among the extensive literature of papers, reviews, books, and articles, this review attempts to include a detailed selection of most significant research work done in the intersection of ICT, supply chains, and counterfeits to provide a reference source for researchers. Citation network and global citation scores have been used to extract and analyze papers and discuss them in different types of clusters (electronic, medical, food, and anti-counterfeiting technologies and approaches). Our review approaches the clustered papers by focusing on (1) their contribution in documenting and modeling the intrusion of counterfeit electronic parts in the ICT supply chain, (2) the proposed counterfeits' detection and avoidance techniques in the ICT supply chain, and (3) the contribution of ICT in thwarting counterfeits in medical, pharmaceutical, and food supply chains. This review provides a better understanding of the global efforts to address counterfeits in the ICT supply chain, as well as the role of ICT in thwarting counterfeits in other supply chains, which can guide future research to minimize the impact of counterfeits on supply chains.

Keyword Supply chain · Counterfeit · Countermeasures · Citation network

S. Saleh · R. Lei · W. Guo (✉) · E. A. Elsayed
Rutgers University-New Brunswick, Piscataway, NJ 08854, USA
e-mail: wg152@soe.rutgers.edu

S. Saleh
e-mail: shs164@scarletmail.rutgers.edu

R. Lei
e-mail: rl839@scarletmail.rutgers.edu

E. A. Elsayed
e-mail: elsayed@soe.rutgers.edu

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 447,
https://doi.org/10.1007/978-981-19-1607-6_75

1 Introduction

The supply chain has gained a great amount of interest since it deals with the management of the entire process from the making of a product to its actual delivery to the customer. As supply chains expand globally and become more complex, managing the flow of materials, information, and data becomes more susceptible to threats that interrupt and/or impact its flow. One of the major threats to the information and communications technology (ICT) supply chain is the introduction of counterfeit parts and components, as electronics are an indispensable part of our lives [1].

A *counterfeit* is defined by the Society of Automotive Engineers (SAE International) as "a fraudulent part that has been confirmed to be a copy, imitation, or substitute that has been represented, identified, or marked as genuine, and/or altered by a source without legal right with intent to mislead, deceive, or defraud" [2]. Counterfeits can exist in non-deceptive forms where people intentionally buy counterfeit or fake items and in deceptive forms where people unknowingly buy counterfeit items believing they are genuine. Non-deceptive counterfeits lead to loss of sales and an increase in costs to control these fake products. Deceptive counterfeits that enter the supply chain during the production process could lead to low-quality products and consequently, high product recalls, lost sales, bad reputation, and even legal proceedings.

Whether deceptive or non-deceptive, counterfeit items are a real threat to the global economy, people's safety, overall security, and innovation. Threatening people's lives is the most detrimental impact of counterfeits. Hundreds of cases of deaths caused by counterfeit food or medicine have been reported. Incorporating counterfeit parts in life-supporting equipment, vehicles, aviation, etc., bears ominous consequences. The global economy is affected by the fact that some businesses lose sales or even shut down because of a bad reputation due to counterfeits; this loss was estimated to be around $323 billion in 2018. Besides, the number of jobs lost due to counterfeiting was 2.6 million in 2013 and is estimated to reach around five million by the year 2022 [3]. Moreover, counterfeiting hinders investments in countries notorious for importing or producing counterfeits. On the other side, detecting and mitigating counterfeits have become the interest of a significant proportion of investments and innovations globally. A significant amount of funds and intellectual efforts are dedicated to counterfeits instead of being dedicated to new developments.

Counterfeiting targets any item that can be produced at a lower price, and it accounts for 3.3% of world trade with no hint of declining. A study done in 2019 estimated the percentage of counterfeit parts in industries [4]. As illustrated in the pie chart in Fig. 1, footwear, clothing, and leather goods are the most hit by counterfeits. Electrical equipment goes next (12%). Amidst the other industries with lower percentages, there are critical industries like medical equipment and pharmaceuticals; counterfeited medical items directly threaten people's lives. The counterfeit industry is taking advantage of all circumstances. For instance, the COVID-19 pandemic favors the proliferation of counterfeit products such as substandard sanitizers or masks. Closed borders force authentic industries to rely on untrusted suppliers and

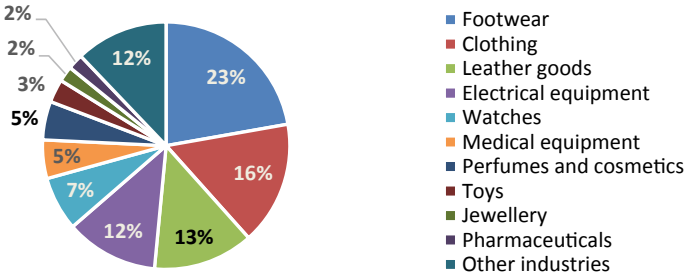

Fig. 1 Distribution of counterfeits on industries [4]

closed stores and social distancing increased online shopping, which is the most favorable venue for counterfeiting.

In addressing this problem, a significant number of detection techniques, mitigation strategies, policies, and campaigns to make people aware of the counterfeits' criticality have been made. The literature focusing on counterfeits in supply chains is vast. In our effort, we gather, connect, and analyze the work done in the intersection area of ICT, supply chains, and counterfeits to set forth an inclusive reference for future studies and enhancements in this field. This review provides a better understanding of the global efforts to address counterfeits in the ICT supply chain, as well as the role of ICT in thwarting counterfeits in other supply chains, which can guide future research to minimize the impact of counterfeits on supply chains.

The method for analyzing publications, including constructing, and visualizing bibliometric networks is described in Sect. 2. In Sect. 3, we analyze the literature in counterfeits in ICT supply chains, including how counterfeit parts are documented and modeled, as well as the related anti-counterfeiting approaches. In Sect. 4, we analyze the literature in ICT-related anti-counterfeiting technologies and approaches (countermeasures) in thwarting counterfeits in supply chains broader than just electronics. Section 5 concludes the review with a discussion of future research directions.

2 Methodology

Searching through Elsevier's Scopus citation database covering over 42,000 titles from approximately 11,680 publishers, we obtain over 900 articles using the keywords "supply chain" and "counterfeit." Scopus is chosen because it covers a big number of articles, and we can obtain bibliographic database files that can be used to construct and visualize bibliometric networks. We analyze this big data by creating a map based on the author keywords (i.e., keywords given by the authors). The co-occurrence of keywords in the network reveals a specific theme or trend in research that we need to identify [5]. Figure 2 shows the keywords co-occurrence network developed in VOSviewer [6], where a bigger circle indicates that the keyword appears

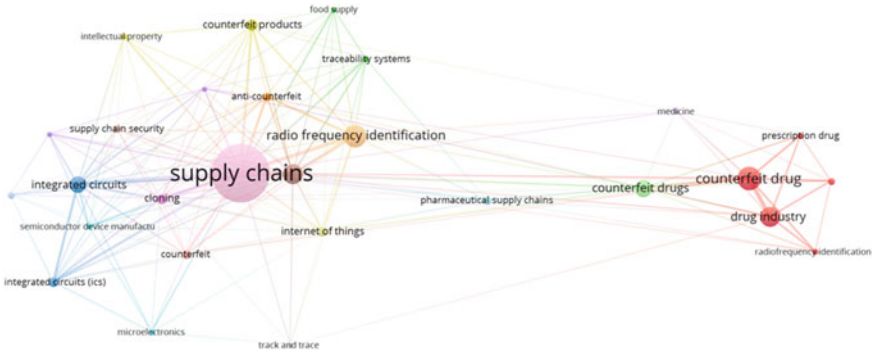

Fig. 2 Keyword co-occurrence network

more frequently in the publication set, the different colors represent the different clusters, these keywords are assigned to, and the lines indicate co-occurrence of the keywords.

According to the size of the circles, their colors, and their connections in Fig. 2, we identify four interconnected clusters of research areas in the literature tackling counterfeits in supply chains:

(1) Area One: Counterfeits in electronic parts in ICT supply chains
(2) Area Two: Counterfeits in medical and pharmaceutical supply chains
(3) Area Three: Counterfeits in food supply chains
(4) Area Four: Anti-counterfeiting technologies and approaches (countermeasures)

In addition to the keyword co-occurrence network, we perform citation analysis by developing a citation network in VOSviewer. The citation network reveals "interconnected" literature and "isolated" literature. Interconnected literature is identified as papers that add value to the studied topic, and it shows the trend in the research done. Figure 3 shows the citation network obtained using VOSviewer, where the size of the nodes illustrates the number of citations of the paper. The nodes in gray represent the isolated papers while nodes in the center represent the interconnected papers. Figure 4 shows a closer view of the interconnected citation network containing 131 references. The network shows the connection between literature and its clustering into four main clusters or areas. These areas coincide with the clusters identified from the author keyword network. Additionally, we notice that some gray nodes in Fig. 3 are relatively large, indicating high citations, but they are not directly linked to the four interconnected clusters. This suggests that although these isolated papers do not share common citations with the papers in the interconnected citation network, they still have significant impact in addressing counterfeits in supply chains. Therefore, the ten most cited isolated papers according to their global citation scores are matched to the preceding four areas and included in our survey. Furthermore, additional papers, beyond Scopus, selected by experts with elaborate research work on counterfeiting are incorporated into our survey.

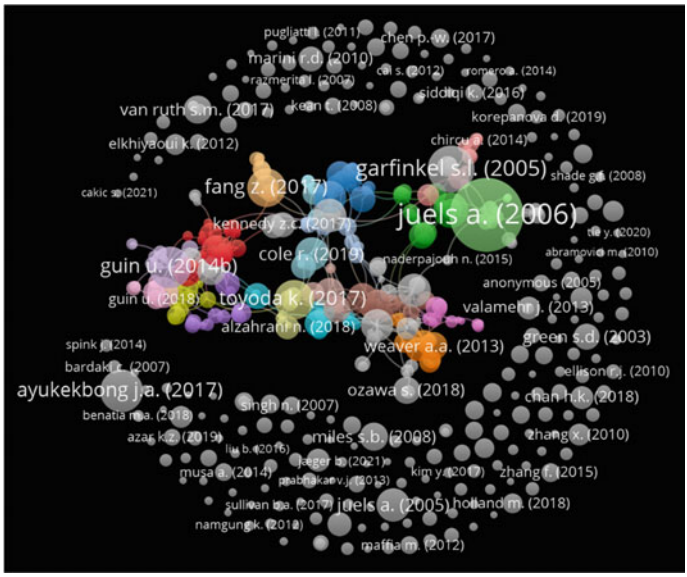

Fig. 3 Citation network for all papers in the publication set

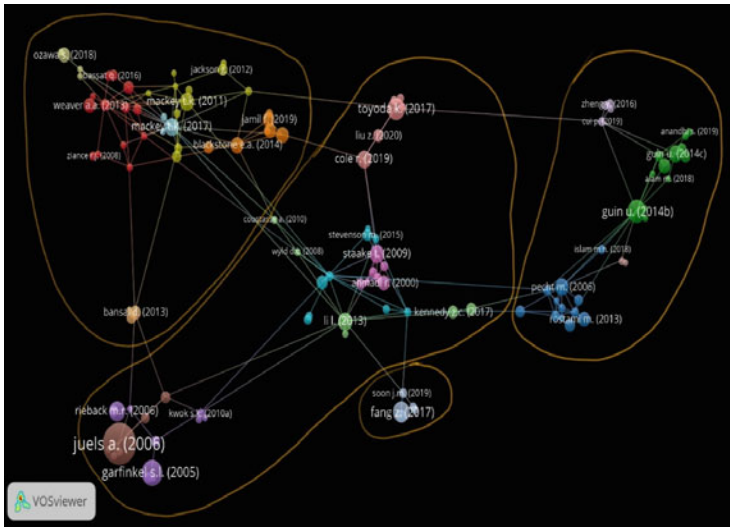

Fig. 4 Citation network for the interconnected papers in the publication set

In this paper, literature identified in the four areas is organized according to their relationship to ICT. Literature in area (1) is reviewed in Sect. 3, including how counterfeit electronic parts in the ICT supply chain are documented and modeled, as well as the detection and avoidance techniques in the ICT supply chain. Literature in areas (2), (3), and (4) is reviewed in Sect. 4, with a focus on how ICT is used in thwarting counterfeits in supply chains beyond electronics. For areas (2) and (3), we focus on the role of ICT in thwarting counterfeits in medical and pharmaceutical supply chains and food supply chains, rather than how the counterfeit drugs or food are introduced.

3 Counterfeits in Information and Communications Technology (ICT) Supply Chains

The increase of counterfeiting in electrical and electronic systems and components has been on the rise recently due to the production shift to less law-enforcing countries, online shopping, and more sophisticated counterfeiting techniques [7]. Counterfeit electronics in the defense and security supply chains represent one of the most critical threats to security and safety [8].

3.1 Documenting and Modeling Counterfeits

The increasing concern about counterfeit parts, especially in the ICT supply chain, has given rise to a robust literature that includes reports from components of the Department of Defense (DoD), NASA, and other government agencies, as well as from Lockheed Martin, IBM, the Aerospace Industries Association, and other companies/organizations in the private sector. Indeed, the presence of counterfeit and other unacceptable products have led to the formation of Government-Industry Data Exchange Program (GIDEP) [9] as a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production, and operational phases of the life cycle of systems, facilities, and equipment and report any counterfeit products. Likewise, Electronic Resellers Association International (ERAI) was founded in 1985 as a major resource for checking if a component is counterfeit [10]. It is the world's largest database of suspect counterfeit and nonconforming electronic parts. This tool, alone, has fully changed the way in which sectors of the supply chain research, track, identify, purchase, and sell material. It allows members to better mitigate risks in their procurement process, especially when dealing with end-of-life or obsolete parts. These two sources in addition to the DoD trusted suppliers list constitute the first "line of defense" to check for counterfeits parts or components.

The literature also describes best practices for government and industry. For instance, the Navy's Counterfeit Materiel Process Guidebook [11] aims to "equip DON [Department of the Navy] activities with a practical tool for implementing a risk-based counterfeit materiel prevention program." Wix [12] recommends clearly defining company-wide counterfeit risk mitigation strategies. Among those strategies are to prohibit sourcing electronic components from independent distributors, reducing number of vendors, requiring distributors to use third party test houses or conform to inspection standards, and to develop measurable quality criteria for distributors. Szakal and Pearsall [13] discuss the challenges of increasing reliance on commercial-off-the-shelf ICT components and describe a framework to mitigate the risk.

There is not much literature that looks at counterfeiting theoretically. Bodner [14] lays out a modeling framework to understand the counterfeiting problem, based on "the exogenous environment, policy, enterprise actors, supply chain flows, and system/constituent behavior," and presents a prototype agent-based simulation that implements the framework. Stevenson and Busby [15] describe a theoretical account of counterfeiting based on signaling theory that what counterfeiters' strategies aim to achieve often involves the generation, suppression, or exploitation of signals.

3.2 Anti-counterfeiting Approaches

The Society of Automotive Engineers developed a standardized process for detecting counterfeits. The semi-quantitative risk assessment method categorizes components into levels where each level has appropriate types of laboratory testing [16]. Clearly, there is a consensus on the need for a comprehensive approach utilizing technological solutions and decision-making for counterfeits detection and avoidance in the ICT supply chain [17]. Rostami et al. [18] summarize that the state-of-the-art defenses proposed for counterfeits in ICT supply chains are testing, using aging sensors that detect recycled products, and adopting proactive techniques like hardware metering, fingerprinting, and watermarking. Chatterjee and Das [19] state that a major contribution toward combatting counterfeits is done by the parts manufacturers in building trust in the supply chain, and they provide a set of measures for manufacturers to increase trust.

One focus in the ICT supply chain is counterfeit integrated circuits (ICs). Guin et al. [20, 21] provide a comprehensive background of the types of counterfeit ICs available, the testing effectiveness for detecting each type of counterfeit, and the available counterfeit avoidance techniques. More detailed information on the aforementioned topics can be found in the "counterfeit integrated circuits: detection and avoidance" book [22]. Guin et al. [23] also provide a thorough overview of the types of counterfeits in general and the available detection and avoidance methods. They also present a selecting algorithm that enables choosing the optimum method considering test time, cost, and application risks. Alam et al. [24] propose a low-cost and highly-accurate method to detect counterfeit ICs using a ring oscillator (RO)

and a nonvolatile memory where the digital signature and the corresponding RO frequency and conditions are stored. A similar attempt is used to detect counterfeit field-programmable gate arrays (FPGA) and ICs, in which the detection is accompanied with an aging analysis to detect recycled or out-of-specification ICs by their performance degradation [25, 26]. Ghosh and Chakraborty [27] propose an enhanced image texture analysis to detect counterfeit ICs. Their method shows high accuracy even when images are taken using ordinary digital cameras. Frazier et al. [28] present a new (near real-time) counterfeit detection process, which is based upon infrared thermal imaging, intensive statistical analysis, and machine learning, to differentiate between authentic and inauthentic electronic parts.

Lowering the cost of counterfeit detection can help widen the adoption of the detection techniques. Huang et al. [29] introduce a low-cost support vector machine to classify the authenticity of parts. This technique is useful in cases of recycled counterfeits. Similarly, Kumari et al. [30] provide a low-cost detection method for recycled memory chips which are incorporated in many electronic systems. The detection method depends on studying the chips' timing characteristics, which are sensitive to high usage, program, and read time [30, 31].

A lot of the existing counterfeit detection approaches depend on human decisions and consequently are vulnerable to error. To improve the accuracy in counterfeit detection, there is ongoing interest in automating the detection by leveraging the strength of data analytics, machine learning, and artificial intelligence. Ahmadi et al. [32] attempt to explore an automatic detection method using image processing techniques and machine learning algorithms. Zheng et al. [33] propose a method utilizing clock phase sweep, with low design and hardware requirements, to identify counterfeit FPGA. Experimental results show 99% accuracy of the proposed method. Zheng et al. [34, 35] claim that detection methods based on aging sensors require more design verification efforts and do not apply to legacy chips. They attempt to detect recycled chips using a more comprehensive approach. This approach combines exploiting differential aging to isolate aged chips under large die process variations and comparing transient current testing results between adjacent similar circuit structures in a chip. An added value to the methods proposed in Refs. [24–26, 34, 35] is that they do not require perfectly functioning chips as a reference that accounts for high-test complexity and cost.

The most common counterfeit avoidance techniques are secure split-test (SST) and physically unclonable function (PUF). Contreras et al. [36] emphasize the SST's effectiveness in securing ICs. Ben Dodo et al. [37] explain how spin transfer torque-magnetic random-access memory technology can make the existing PUF more secure and less vulnerable to tampering. A simulation model proves that this technique detects all tampered parts. Counterfeit avoidance techniques develop continuously. Chakraborty et al. [38] propose logic locking as a solution to thwart piracy and counterfeiting using a "keying" mechanism. Basak et al. [39] propose a similar mechanism by locking ICs using antifuse devices in input/output circuitry.

Traceability, via blockchain, and compliance verification using suitable testing methods and/or embedded PUF in conjunction with risk management are proposed as the major tools to identify the authenticity of products by tracking, tracing, and

analyzing parts during the entire life cycle [40–46]. Livingston [47] suggests that test methods in government and industry designed to verify integrity and performance of authentic parts are not as important as traceability programs to help detect counterfeits. He also suggests that documentations of certifications of conformance or test reports accompanying parts be investigated since they are sometimes not authentic.

Traceability can be enabled using RFID [48–50]. The effectiveness of RFID in protecting the supply chain from counterfeiters is modeled by Yang et al. [48] in an IoT supply chain using a printed circuit board prototype [49, 51]. Although experimental results obtained are promising and the cost of the technique proposed in Anandhi et al. [50] is low because the majority of the components needed already exist in modern IoT supply chains, experimental analysis shows that the authentication protocol relying on an asymmetric key cryptosystem, and one-way hash function is computationally expensive and cannot handle big data efficiently. Dimase et al. [52] note that an appropriate level of traceability must be implemented based on risk prioritization because the cost of implementing traceability at a wide range might outweigh its benefits.

4 ICT-Related Anti-counterfeiting Technologies and Approaches in Other Supply Chains

4.1 ICT-Related Anti-counterfeiting Technologies and Approaches (Countermeasures)

In this section, we take a closer look at the research focusing on the ICT-related anti-counterfeiting approaches themselves regardless of the type of the product and the supply chain. Li [53] categorizes and briefly describes all available technologies to combat counterfeits in supply chains, until 2013, into two types: 1) product authentication verification and 2) product tracking and tracing.

The Defense Logistics Agency [54] suggests different kinds of tests, including electrical testing, x-ray testing, and microscopic exam. Gansler et al. [55], in addressing the DOD supply chain, suggest stronger quality assurance standards tied to a risk-based approach to counterfeit mitigation. They also recommend stronger preventive measures. Among preventive measures suggested are tamper-proof packaging and x-ray inspection, debarring suppliers who repeatedly provide components with counterfeit parts, and providing penalties for suppliers not reporting suspect counterfeits. Rogers and O'Donnell [56] point out that the defense industry "routinely failed to report cases of suspect counterfeit parts," and Livingston [47] makes a similar observation. For reporting counterfeit parts, Gansler et al. [55] recommend using GIDEP as does Livingston. The Aerospace Industries Association [57] recommends developing a program of limited liability for those accurately reporting counterfeit parts using GIDEP.

Lockheed Martin [58] describes what makes a good counterfeit prevention plan. One of the ideas described is to allow customers to review what suppliers' processes are without disclosing proprietary information.

Digital watermarking is a growing approach to defend against counterfeiting. For example, DARPA is working on countermeasures that involve marking in an electronic component that can enable the authentication of genuine devices [59]. In applications other than ICT, Lingle [60] discusses digital watermarks on packaging and products for cosmetic and personal care products. The invisible digital watermarks can be viewed with a special app that will then authenticate the product. The Digital Watermarking Alliance [61] discusses how the watermark on packaging or an object can be used to uniquely identify specific items and also carry other information such as lot number and intended destination, and points out that watermarks can be encrypted so only authorized devices can access the data. In digital manufacturing, Chan et al. [62] propose the use of watermarking technology to protect the intellectual property of 3D printers' content. In pharmaceutical applications, watermarking is explored as a tool in producing tamper-resistant prescription forms in an attempt to prevent fraudulent prescriptions for controlled substances [63]. However, watermarking of physical components is also used in the pharmaceutical industry to make it possible to follow a pill bottle (and perhaps eventually an individual pill) from its inception in a plant to its final destination.

RFIDs are suggested as one of the most suitable solutions to track items in a supply chain especially with the decline in their cost in the past few years [64–66] and their capability to integrate with mobile technologies to obtain a self-validated location-based authentication system [67] and data processing and synchronization algorithm [68]. Besides, the development of RFID drives authorities to encourage the use of RFID. For instance, federal agencies and retailers are influencing the adoption of RFID in the pharmaceutical supply chain [69]. Azuara et al. [66] show the efficiency of RFID-enabled systems in counterfeit detection applied only at the manufacturing stage of the supply chain. RFIDs can also be used on unstable and non-uniform surfaces like textiles [70]. Security and privacy concerns are discussed, and proposed solutions are found in Refs. [71–75]. Cai et al. [76] initiate a secure and flexible protocol that enables each supply chain party to securely update tag keys and consequently ensure a safe transfer of RFID tags in the supply chain. However, this protocol is not financially justified for all types of products. Kumar et al. [77] suggest that the use of RFID in the drug supply chain has an important advantage of managing the reverse logistic process besides reducing the risk of counterfeits.

Electronic product code (EPC) tags are a form of RFID but highly vulnerable to cloning and counterfeit attacks. Juels [78] attempts to strengthen the EPC using personal identification number (PIN)-based access-control and privacy enhancement mechanisms. Miles et al. [79] provide comprehensive coverage of information related to RFIDs including their application in anti-counterfeiting.

Singh and Li [80] highlight the importance of trust in an RFID-enabled supply chain and provide an RFID trust framework. Ting and Tsang [81] develop a tool that can identify counterfeit sources in a supply chain by analyzing the relationship

between people. They depend on social network analysis in characterizing certain features that identify the relationship.

Quick-response (QR) code linked to blockchain databases have been used in avoiding counterfeit medications [82]. Using blockchain is extensively promoted to avoid counterfeit infiltration into a supply chain. Indeed, blockchains also bring improved quality, enhanced inventory, reduced cost of supply chain transaction, etc. [83]. Pun et al. [84] explicitly describe the effectiveness of adopting blockchain to combat counterfeits in a supply chain and encourage governments to provide subsidies for this technology. Liu and Li [85] propose a blockchain-based framework for e-commerce, which shows to be effective in protecting the supply chain against clone attacks, counterfeit tag attacks, and counterfeit product attacks. Kennedy et al. [86] propose the use of lanthanide nanomaterial in 3D printed parts and link the obtained unique chemical signature into a blockchain database. Smith and Skrabalak [87] review the use of metal nanomaterials in developing optical anti-counterfeit labels. Toyoda et al. [88] attempt to secure RFID-attached products from any tampering in the post-supply chain. They use Bitcoin's blockchain idea to allow customers to identify the genuineness of the item if the seller has the ownership. The proof-of-concept and cost performance are evaluated experimentally. Hepp et al. [89] identify the limitations of adopting blockchain technology for tracking physical assets. They suggest using PUF instead of RFID, which is susceptible to cloning, and using OriginStamp system that can aggregate events, reducing by that the number of transactions instead of logging each event on the blockchain individually.

In their attempt to understand how IoT technologies enable and constrain the actors' control capabilities, Boos et al. [90] use IoT applications for counterfeit detection in supply chains. They discuss how accountability (visibility, responsibility, and liability) and control (transparency, predictability, and influence) are affected by the IoT technologies' range to inform, automate, and transform.

4.2 The Role of ICT in Thwarting Counterfeits in Medical and Pharmaceutical Supply Chains

Counterfeits in the medical and pharmaceutical supply chain pose a huge threat with significant consequences for global health and patient safety. Although only 7% of the counterfeiting actions (as shown in Fig. 1) target medical and pharmaceutical products, counterfeit medication adds another 15% of the medical and pharmaceutical supply chain and is a threat to human lives. Moreover, it costs the legitimate pharmaceutical industry between $37.6 billion and $162.1 billion with 57,500–247,800 lost jobs in the U.S alone [91]. Refs. [92–97] investigate how counterfeit drugs are introduced and their impact on health and economics. Law enforcement, strict surveillance, and awareness are the most common solutions for counterfeit medicines [98–105].

An overview of the projects done by key organizations to halt the proliferation of counterfeit medicines is provided in Nayyar et al. [106], in which they also provide recommendations regarding technologies, communication, and laws to increase pharmaceutical governance. Chaudhry and Stumpf [107] emphasize the importance of the counterfeit detection device #3 or CD3 [108] developed by the U.S. Food and Drug Administration (FDA) that is inexpensive and enables inspectors to identify counterfeit drugs nationally and at border entry. By emitting light in ten different wavelengths, the device scans drug samples and compares them against authentic drugs in its memory. It is also capable of checking tampered packaging. Mackey and Liang [109, 110] propose a global policy framework to enable cooperation and coordination to combat counterfeit drugs. Davison [111] provides a thorough review on combatting counterfeit medicines. It discusses regulations, authentication strategies (packaging, analytical techniques), product tracking, and case studies from around the world.

Hamilton et al. [112] propose a combination of countermeasures at the different levels of the pharmaceutical supply chain; the main suggested countermeasures are global monitoring, pharmacovigilance, pharmacists training, customer awareness, and the adoption of testing technologies convenient to low-resource settings in addition to the emerging consumer verification techniques such as mobile authentication services (MAS). They suggest simple, inexpensive MAS, such as having a hidden barcode that when scratched and texted to a secure hotline a confirmation of the medication genuineness is received. Fadlallah et al. [113] express concern that authentication systems, such as RFID, are effective in the dispensing phase only and are challenging for less developed countries because they require an infrastructure connecting all pharmacies which requires time, effort, and commitment. Cohn et al. [114] investigate a successful response to falsified medications in Nairobi using a transparent quality assurance system where procurement parties, manufacturers, and other stakeholders are instantly notified about falsified medications, followed by immediate testing and recall processes. Cuomo and Mackey [115] and Mackey et al. [116] propose a surveillance mechanism using statistical analysis and geospatial modeling to identify the distribution of counterfeit cancer medication in the USA. This model can play an important role in predicting future counterfeit medicine incidents.

It is clear that there is a tendency of increased counterfeit drug incidents in low- and middle-income countries because of low production costs and weak law governance. Regulations for drug donation and safe drug disposals are especially important in poor countries which have stockpiles of donated drugs [113, 117, 118]. Countermeasures that reduce the impact of counterfeits include ensuring the authenticity of the drug, stock control, and awareness by caregivers. In some instances, these measures are shown to reduce the economic impact and number of deaths by about 40% when simulated using an agent-based model [119]. Low-cost tests to identify falsified drugs are also used to ensure the authentication of medications [120, 121]. Marini et al. [122] build a low-cost detection method for counterfeit medicines which is equipped with a deep ultraviolet radiation detector. To study the accuracy of the

prototype, they perform a full validation and method comparison study with other conventional detection methods, and the obtained results are promising.

Other research asserts the importance of monitoring technologies in applying the laws and regulations [123]. Lybecker [124] presents a theoretical model to characterize the implications of these technologies on counterfeiters. Mackey and Nayyar [125] present a review of all digital technologies that protect the supply chain from counterfeit medications and the technologies evolving in preventing the sale of counterfeit medications. Taylor [126] describes the emergence of radio-frequency identification (RFID) into the pharmaceutical barriers and stresses the fact that what RFID brings to patients and brands justifies its technological and investment requirements. Chen et al. [127] describe the use of the quantitative radio-frequency spectroscopic technique for a safer pharmaceutical supply chain, while Kwok et al. [128] construct a prototype to prove RFIDs' effectiveness. Trenfield et al. [82] propose a novel anti-counterfeit method to track 3D-printed medicines by adding a combination of material inks for detection using Raman spectroscopy. Similarly, Cozzella et al. [129] explain the use of white-light speckle theory, which is a speckle visible under ultraviolet fluorescence light, as a fingerprint for drug packages.

Adding to the above-mentioned descriptive papers, Raj et al. [130] explain the use of blockchain technology to increase visibility and traceability and control counterfeit medications, while Kumar et al. [131] suggest that the use of smart contracts along with blockchains for the drug supply chain increases the trust between stakeholders, automatic payments, and quality control. Meyliana et al. [132] propose the use of blockchain with smart contract in supply chain management to comply with the good manufacturing practices (GMP) regulation set by the Indonesian government. Alzahrani and Bulusu [133] propose a decentralized anti-counterfeiting supply chain using blockchain and near field communication technologies (NFC) to detect any modification attack and track products, introducing a new consensus protocol as well utilizing a small number of validators while maintaining a high level of security. Internet of things (IoT) and blockchains are envisioned in managing supply information across healthcare supply chain processes which allow better management for recalls, expiration, shortages, and counterfeits [134, 135]. Sylim et al. [136] develop a pharmaco-surveillance blockchain system prototype running on smart contracts. The use of a connector module connecting supply chain echelons with blockchain is simulated; the results prove increased collaboration, trust, and system performance measured by fill rate [137]. Jamil et al. [138] propose a system for secure drug supply chain records usage which is handled and conducted by Hyperledger Fabric based on blockchain. Moreover, a limited-access to patients' drug and health records is maintained by a smart contract. Experimental analysis validates the usability and efficiency of the proposed system. Kumar and Tripathi [139] propose a blockchain-based framework to enhance drug security and authenticity of manufacturers. Their methodology is based on digital signatures which are provided by the certificate authority following the public key infrastructure protocol. This is claimed to prevent replay and man-in-middle attacks. Global Governance Blockchain is suggested to address the counterfeiting problem and allows surveillance by every participant involved in the supply chain [140].

4.3 The Role of ICT in Thwarting Counterfeits in Food Supply Chains

All types of food products are susceptible to counterfeiting. Traceability is considered to be the best anti-counterfeiting technique for ensuring food quality. Shahbazi and Byun [141] propose a blockchain machine learning traceability system addressing the shelf life, weight, evaporation, warehouse transactions, and shipping time of perishable food which are sensitive due to discrepancy and deterioration. Tsang et al. [142] propose a traceability system by integrating blockchain, IoT technology, and fuzzy logic. Blockchain and IoT ensure products traceability and avoidance of counterfeits whereas fuzzy logic is used to evaluate quality decay.

Soon and Manning [143] use Scotch whisky as a case study for counterfeit in the supply chain and highlight the effectiveness of smart packaging in detecting counterfeits. They propose overt smart packaging technologies such as barcodes, RFID, or watermarks and covert ones such as intaglio printing, security threads, and fluorescence artifacts. Besides, they stress the effectiveness of collaboration between all members of the value chain in detecting counterfeiters. Smart packaging can also be combined with antimicrobial and antioxidant material, time–temperature indicators, freshness indicators, gas concentration indicators, etc., to promote microbial safety and longer shelf life [144, 145].

It is clear that the progress in combatting counterfeiting in the food industry is weak as compared to the other sectors since the cost of implementing critical countermeasures is significantly high compared to the product price.

5 Conclusion

In this study, we review a detailed selection of significant research work done in the intersection of ICT, supply chains, and counterfeits. The aim of the review is to provide a comprehensive reference for counterfeit detection and avoidance techniques, methods, and approaches proposed until now in the context of ICT supply chains and beyond. Using clustering and citation network analysis, we identified four main clusters of relevant work done in this topic: (1) counterfeits in electronic parts in ICT supply chains, (2) counterfeits in medical and pharmaceutical supply chains, (3) counterfeits in food supply chains, and (4) anti-counterfeiting technologies and approaches. We analyze the clustered research based on how ICT is incorporated to defeat counterfeits in ICT supply chains and other threatened supply chains. This review provides a better understanding of the global efforts to address counterfeits in the ICT supply chain, as well as the role of ICT in thwarting counterfeits in other supply chains, which can guide future research to minimize the impact of counterfeits on supply chains.

This review reveals the trend of using RFID and blockchains in avoiding counterfeits in all types of supply chains. It is clear that among all the proposed solutions

to thwart counterfeits, no single countermeasure can be generalized for all clusters. This is due to the continuous development of counterfeiters' techniques and also the vulnerabilities in the solutions proposed. The best solution for a supply chain should be customized from the set of available solutions and strengthening methods suggested based on the supply chain structure and expansion, cost, and local and international regulations.

Acknowledgements This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 17STQAC00001-05–00.

Disclaimer The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security. The authors thank Fred S. Roberts for his helpful input in revising this paper.

References

1. CISA Working Group 2 (2021) Information and Communications Technology Supply Chain Risk Management Task Force Threat Evaluation Working Group: Threat Scenarios Version 2.0: https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v2.pdf
2. SAE International (2019) SAE AS5553 Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition Standards
3. Frontier Economics Ltd (2017) The Economic Costs of Counterfeiting and Piracy
4. OECD, European Union Intellectual Property Office (2019) Trends in trade in counterfeit and pirated goods. Illicit Trade, OECD Publishing, Paris
5. Falagas ME, Pitsouni EI, Malietzis GA, Pappas G (2008) Comparison of PubMed, Scopus, Web of Science, and Google Scholar: strengths and weaknesses. FASEB J 22(2):338–342
6. Van Eck NJ, Waltman L (2010) VOSviewer: visualizing scientific landscapes [software]. https://www.vosviewer.com
7. Pecht M, Tiku S (2006) Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectr 43(5):37–46
8. Stradley J, Karraker D (2006) The electronic part supply chain and risks of counterfeit parts in defense applications. IEEE Trans Compon Packag Technol 29(3):703–705
9. GIDEP. https://www.gidep.org/about/about.htm
10. ERAI. https://www.erai.com/aboutus_profile
11. Office of the Assistant Secretary of the Navy (2017) Counterfeit Material Process Guidebook: Guidelines for Mitigating the Risk of Counterfeit Materiel in the Supply Chain. NAVSO P-7000
12. Wix SD (2017) Suspect/Counterfeit Electronics Overview. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States)
13. Szakal A, Pearsall K (2014) Open industry standards for mitigating risks to global supply chains. IBM J Res Dev 58(1):1–13
14. Bodner DA (2014) Enterprise modeling framework for counterfeit parts in defense systems. Procedia Computer Science 36:425–431
15. Stevenson M, Busby J (2015) An exploratory analysis of counterfeiting strategies. Int J Oper Prod Manag 35(1):110–144
16. Collier ZA, Linkov I, Keisler JM, Walters S, DiMase D (2014) A semi-quantitative risk assessment standard for counterfeit electronics detection. SAE Int J Aerosp 7(1):171–181

17. Lambert JH, Keisler JM, Wheeler WE, Collier ZA, Linkov I (2013) Multiscale approach to the security of hardware supply chains for energy systems. Environ Syst Decisions 33(3):326–334
18. Rostami M, Koushanfar F, Rajendran J, Karri R (2013) Hardware security: threat models and metrics. in 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). IEEE. pp 819–823
19. Chatterjee K, Das D (2007) Semiconductor manufacturers' efforts to improve trust in the electronic part supply chain. IEEE Trans Compon Packag Technol 30(3):547–549
20. Guin U, Huang K, Dimase D, Carulli JM, Tehranipoor M, Makris Y (2014) Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain. Proc IEEE 102(8):1207–1228
21. Guin U, Dimase D, Tehranipoor M (2014) Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. J Electron Test 30(1):9–23
22. Tehranipoor M, Guin U, Forte D (2015) Counterfeit integrated circuits: detection and avoidance
23. Guin U, Dimase D, Tehranipoor M (2014) A comprehensive framework for counterfeit defect coverage analysis and detection assessment. J Electron Test 30(1):25–40
24. Alam M, Chowdhury S, Tehranipoor MM, Guin U (2018) Robust, low-cost, and accurate detection of recycled ICs using digital signatures. in 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). pp 209–214
25. Dogan H, Forte D, Tehranipoor MM (2014) Aging analysis for recycled FPGA detection. in 2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT). pp 171–176
26. Guo Z, Xu X, Rahman MT, Tehranipoor MM, Forte D (2018) SCARe: an SRAM-based countermeasure against IC recycling. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 26(4): 744–755
27. Ghosh P, Chakraborty RS (2017) Counterfeit IC detection by image texture analysis. in 2017 Euromicro Conference on Digital System Design (DSD). pp 283–286
28. Frazier PD, Gilmore ET, Collins IJ, Samotshozo WE, Chouikha MF (2018) A novel counterfeit detection approach for integrated circuit supply chain assurance. Journal of Hardware and Systems Security 2(3):240–250
29. Huang K, Carulli JM, Makris Y (2013) Counterfeit electronics: a rising threat in the semiconductor manufacturing industry. in 2013 IEEE International Test Conference (ITC). pp 1–4
30. Kumari P, Talukder BMSB, Sakib S, Ray B, Rahman MT (2018) Independent detection of recycled flash memory: challenges and solutions. in 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). pp 89–95
31. Sakib S, Kumari P, Talukder B, Rahman M, Ray B (2018) Non-invasive detection method for recycled flash memory using timing characteristics. Cryptography 2(3):17
32. Ahmadi B, Javidi B, Shahbazmohamadi S (2018) Automated detection of counterfeit ICs using machine learning. Microelectron Reliab 88–90:371–377
33. Zheng Y, Wang X, Bhunia S (2015) SACCI: scan-based characterization through clock phase sweep for counterfeit chip detection. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 23(5): 831–841
34. Zheng Y, Basak A, Bhunia S (2014) CACI: dynamic current analysis towards robust recycled chip identification. in Proceedings of the 51st Annual Design Automation Conference. San Francisco, CA, USA: Association for Computing Machinery. pp 1–6
35. Zheng Y, Yang S, Bhunia S (2016) SeMIA: self-similarity-based IC integrity analysis. IEEE Trans Comput Aided Des Integr Circuits Syst 35(1):37–48
36. Contreras GK, Rahman MT, Tehranipoor M (2013) Secure Split-Test for preventing IC piracy by untrusted foundry and assembly. in 2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS). pp 196–203
37. Ben Dodo S, Bishnoi R, Mohanachandran Nair S, Tahoori MB (2019) A spintronics memory PUF for resilience against cloning counterfeit. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 27(11): 2511–2522

38. Chakraborty A, Jayasankaran NG, Liu Y, Rajendran J, Sinanoglu O, Srivastava A, Xie Y, Yasin M, Zuzak M (2020) Keynote: a disquisition on logic locking. IEEE Trans Comput Aided Des Integr Circuits Syst 39(10):1952–1972
39. Basak A, Zheng Y, Bhunia S (2014) Active defense against counterfeiting attacks through robust antifuse-based on-chip locks. in 2014 IEEE 32nd VLSI Test Symposium (VTS). pp 1–6
40. Livingston H (2007) Avoiding counterfeit electronic components. IEEE Trans Compon Packag Technol 30(1):187–189
41. Islam MN, Patii VC, Kundu S (2018) On IC traceability via blockchain. in 2018 International Symposium on VLSI Design, Automation and Test (VLSI-DAT). IEEE
42. Skudlarek JP, Katsioulas T, Chen M (2016) A platform solution for secure supply-chain and chip life-cycle management. Computer 49(8):28–34
43. Islam MN, Kundu S (2019) Enabling IC traceability via blockchain pegged to embedded PUF. ACM Transactions on Design Automation of Electronic Systems 24(3):1–23
44. Guin U, Cui P, Skjellum A (2018) Ensuring proof-of-authenticity of IoT edge devices using blockchain technology. in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE. pp 1042–1049
45. Cui P, Dixon J, Guin U, Dimase D (2019) A blockchain-based framework for supply chain provenance. IEEE Access 7:157113–157125
46. Negka L, Gketsios G, Anagnostopoulos NA, Spathoulas G, Kakarountas A, Katzenbeisser S (2019) Employing blockchain and physical unclonable functions for counterfeit IoT devices detection. in Proceedings of the International Conference on Omni-Layer Intelligent Systems. Crete, Greece: Association for Computing Machinery. pp 172–178
47. Livingston H (2010) Securing the DOD supply chain from the risks of counterfeit electronic components. BAE Systems
48. Yang K, Forte D, Tehranipoor M (2018) ReSC. ACM Transactions on Design Automation of Electronic Systems, 23(3): 1–27
49. Yang K, Forte D, Tehranipoor M (2015) An RFID-based technology for electronic component and system counterfeit detection and traceability. in 2015 IEEE International Symposium on Technologies for Homeland Security (HST). IEEE. pp 1–6
50. Anandhi S, Anitha R, Sureshkumar V (2019) IoT enabled RFID authentication and secure object tracking system for smart logistics. Wireless Pers Commun 104(2):543–560
51. Yang K, Forte D, Tehranipoor MM (2017) CDTA: a comprehensive solution for counterfeit detection, traceability, and authentication in the IoT supply chain. ACM Transactions on Design Automation of Electronic Systems (TODAES), 22(3): Article 42
52. Dimase D, Collier ZA, Carlson J, Gray RB, Linkov I (2016) Traceability and risk analysis strategies for addressing counterfeit electronics in supply chains for complex systems. Risk Anal 36(10):1834–1843
53. Li L (2013) Technology designed to combat fakes in the global supply chain. Bus Horiz 56(2):167–177
54. Metz C (2012) Defense Logistics Agency, America's Combat Logistics Support Agency Counterfeit Items Detection and Prevention, DLA J-334
55. Gansler JS, Lucyshyn W, Rigilano J (2014) Addressing counterfeit parts in the DOD supply chain, Center for Public Policy and Private Enterprise, School of Public Policy, University of Maryland, UMD-LM-14–012
56. Rogers RSM, O'Donnell J (2017) Supply chain security: DFARS – Detection & Avoidance of Counterfeit Electronic Parts, https://smtnet.com/library/files/upload/supply-chain-security.pdf
57. Aerospace Industries Association (2011) Counterfeit Parts: Increasing Awareness and Developing Countermeasures, https://www.aia-aerospace.org/report/counterfeit-parts-increasing-awareness-and-developing-countermeasures/
58. Lockheed Martin Counterfeit Prevention: What Makes a Good Control Plan?, https://slidetodoc.com/counterfeit-prevention-what-makes-a-good-control-plan/

59. DARPA A DARPA Approach to Trusted Microelectronics, https://www.darpa.mil/attachments/Obscurationandmarking_Summary.pdf
60. Lingle R (2014) In-mold labels use digital watermarking for authentication, https://www.packagingdigest.com/trends-issues/mold-labels-use-digital-watermarking-authentication. Packaging Digest
61. Digital Watermarking Alliance Authentication of content and objects (includes government IDs), https://digitalwatermarkingalliance.org/digital-watermarking-applications/authentication-of-content-and-objects/
62. Chan HK, Griffin J, Lim JJ, Zeng F, Chiu ASF (2018) The impact of 3D Printing Technology on the supply chain: Manufacturing and legal perspectives. Int J Prod Econ 205:156–162
63. CDC Tamper-resistant prescription form requirements, https://www.cdc.gov/phlp/docs/menu-prescriptionform.pdf
64. Staake T, Michahelles F, Fleisch E, Williams JR, Min H, Cole PH, Lee S-G, McFarlane D, Murai J (2008) Anti-counterfeiting and supply chain security. Springer, Berlin Heidelberg, pp 33–43
65. Chen C-l, Chen Y-Y, Huang Y-C, Liu C-S, Lin C-I, Shih T-F (2008) Anti-counterfeit ownership transfer protocol for low cost RFID system. WSEAS Transactions on Computers archive 7:1149–1158
66. Azuara G, Luis Tornos J, Luis Salazar J (2012) Improving RFID traceability systems with verifiable quality. Ind Manag Data Syst 112(3):340–359
67. Kwok SK, Ting JSL, Tsang AHC, Lee WB, Cheung BCF (2010) Design and development of a mobile EPC-RFID-based self-validation system (MESS) for product authentication. Comput Ind 61(7):624–635
68. Choi SH, Yang B, Cheung HH, Yang YX (2015) RFID tag data processing in manufacturing for track-and-trace anti-counterfeiting. Comput Ind 68:148–161
69. Wyld D, Jones M (2007) RFID is no fake: the adoption of radio frequency identification technology in the pharmaceutical supply chain. International Journal of Integrated Supply Management - Int J Integrated Supply Manag, 3
70. Agrawal TK, Koehl L, Campagne C (2018) A secured tag for implementation of traceability in textile and clothing supply chain. Int J Adv Manuf Tech 99(9):2563–2577
71. Juels A (2006) RFID security and privacy: a research survey. IEEE J Sel Areas Commun 24(2):381–394
72. Rieback MR, Crispo B, Tanenbaum AS (2006) The evolution of RFID security. IEEE Pervasive Comput 5(1):62–69
73. Garfinkel SL, Juels A, Pappu R (2005) RFID privacy: an overview of problems and proposed solutions. IEEE Secur Priv 3(3):34–43
74. Lee YK, Batina L, Singelee D, Preneel B, Verbauwhede I (2010) Anti-counterfeiting, untraceability and other security challenges for RFID systems: public-key-based protocols and hardware. Springer, Berlin Heidelberg, pp 237–257
75. Santos BLD, Smith LS (2008) RFID in the supply chain: panacea or Pandora's box? Commun ACM 51(10):127–131
76. Cai S, Li T, Ma C, Li Y, Deng RH (2009) Enabling secure secret updating for unidirectional key distribution in RFID-enabled supply chains. Springer, Berlin Heidelberg, pp 150–164
77. Kumar S, Dieveney E, Dieveney A (2009) Reverse logistic process control measures for the pharmaceutical industry supply chain. Int J Product Perform Manag 58(2):188–204
78. Juels A (2005) Strengthening EPC tags against cloning. in WiSe - 2005 ACM Workshop on Wireless Security. Cologne: Association for Computing Machinery (ACM). pp 67–75
79. Miles SB, Sarma S, Williams JR (2008) RFID technology and applications. RFID Technology and Applications. Vol. 9780521880930. Cambridge University Press. 1–218
80. Singh MKM, Li X (2010) Trust in RFID-enabled supply-chain management. Int. J. Secur. Networks 5:96–105
81. Ting SL, Tsang AHC (2014) Using social network analysis to combat counterfeiting. Int J Prod Res 52(15):4456–4468

82. Trenfield SJ, Xian Tan H, Awad A, Buanz A, Gaisford S, Basit AW, Goyanes A (2019) Track-and-trace: Novel anti-counterfeit measures for 3D printed personalized drug products using smart material inks. Int J Pharmaceutics 567:118443
83. Cole R, Stevenson M, Aitken J (2019) Blockchain technology: implications for operations and supply chain management. Supply Chain Management: An Int J 24(4):469–483
84. Pun H, Swaminathan JM, Hou P (2021) Blockchain adoption for combating deceptive counterfeits. Prod Oper Manag 30(4):864–882
85. Liu Z, Li Z (2020) A blockchain-based framework of cross-border e-commerce supply chain. International J Information Manag 52:102059
86. Kennedy ZC, Stephenson DE, Christ JF, Pope TR, Arey BW, Barrett CA, Warner MG (2017) Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology. J Materials Chemistry C 5(37):9570–9578
87. Smith AF, Skrabalak SE (2017) Metal nanomaterials for optical anti-counterfeit labels. Journal of Materials Chemistry C 5(13):3207–3215
88. Toyoda K, Mathiopoulos PT, Sasase I, Ohtsuki T (2017) A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. IEEE Access 5:17465–17477
89. Hepp T, Wortner P, Schönhals A, Gipp B (2018) Securing physical assets on the blockchain: linking a novel object identification concept with distributed ledgers. in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. Munich, Germany: Association for Computing Machinery. pp 60–65
90. Boos D, Guenter H, Grote G, Kinder K (2013) Controllable accountabilities: The Internet of Things and its challenges for organisations. Behaviour and Info Tech 32(5):449–467
91. Acri KML, Lybecker n (2018) Pharmaceutical counterfeiting: contributing factors. Fraser Institute. pp 6–23
92. Blackstone EA, Fuhr JPJ, Pociask S (2014) The health and economic effects of counterfeit drugs. American health & drug benefits 7(4):216–224
93. Hall A, Koenraadt R, Antonopoulos GA (2017) Illicit pharmaceutical networks in Europe: organising the illicit medicine market in the United Kingdom and the Netherlands. Trends in Organized Crime 20(3–4):296–315
94. Tremblay M (2013) Medicines counterfeiting is a complex problem: a review of key challenges across the supply chain. Curr Drug Saf 8(1):43–55
95. Khan MH, Akazawa M, Dararath E, Kiet HB, Sovannarith T, Nivanna N, Yoshida N, Kimura K (2011) Perceptions and practices of pharmaceutical wholesalers surrounding counterfeit medicines in a developing country: a baseline survey. BMC Health Serv Res 11(1):306
96. Rosen LS, Jacobs IA, Burkes RL (2017) Bevacizumab in Colorectal Cancer: Current Role in Treatment and the Potential of Biosimilars. Target Oncol 12(5):599–610
97. Mackey TK, Liang BA, York P, Kubic T (2015) Counterfeit drug penetration into global legitimate medicine supply chains: a global assessment. Am J Tropical Medicine and Hygiene 92(6_Suppl):59–67
98. Gautam CS, Utreja A, Singal GL (2009) Spurious and counterfeit drugs: a growing industry in the developing world. Postgrad Med J 85(1003):251–256
99. Stewart MW, Narayanan R, Gupta V, Rosenfeld PJ, Martin DF, Chakravarthy U (2016) Counterfeit Avastin in India: punish the criminals, not the patients. Am J Ophthalmol 170:228–231
100. Ozawa S, Evans DR, Bessias S, Haynie DG, Yemeke TT, Laing SK, Herrington JE (2018) Prevalence and estimated economic burden of substandard and falsified medicines in low- and middle-income countries: a systematic review and meta-analysis. JAMA Netw Open 1(4):e181662–e181662
101. Medina E, Bel E, Suñé JM (2016) Counterfeit medicines in Peru: a retrospective review (1997–2014). BMJ Open 6(4):e010387
102. Venhuis BJ, Oostlander AE, Giorgio DD, Mosimann R, du Plessis I (2018) Oncology drugs in the crosshairs of pharmaceutical crime. Lancet Oncol 19(4):e209–e217

103. Jackson G, Patel S, Khan S (2012) Assessing the problem of counterfeit medications in the United Kingdom. Int J Clin Pract 66(3):241–250
104. Chambliss WG, Carroll WA, Kennedy D, Levine D, Moné MA, Douglas Ried L, Shepherd M, Yelvigi M (2012) Role of the pharmacist in preventing distribution of counterfeit medications. J Am Pharm Assoc 52(2):195–199
105. Ziance RJ (2008) Roles for pharmacy in combatting counterfeit drugs. J Am Pharm Assoc 48(4):e71–e91
106. Nayyar GML, Breman JG, Mackey TK, Clark JP, Hajjou M, Littrell M, Herrington JE (2019) Falsified and substandard drugs: stopping the pandemic. Am J Trop Med Hyg 100(5):1058–1065
107. Chaudhry PE, Stumpf SA (2013) The challenge of curbing counterfeit prescription drug growth: Preventing the perfect storm. Bus Horiz 56(2):189–197
108. Ranieri N, Tabernero P, Green MD, Verbois L, Herrington J, Sampson E, Satzger RD, Phonlavong C, Thao K, Newton PN (2014) Evaluation of a new handheld instrument for the detection of counterfeit artesunate by visual fluorescence comparison. Am J Trop Med Hyg 91(5):920
109. Mackey T, Liang B (2011) The global counterfeit drug trade: patient safety and public health risks. J Pharm Sci 100:4571–4579
110. Mackey TK, Liang BA (2013) Improving global health governance to combat counterfeit medicines: a proposal for a UNODC-WHO-Interpol trilateral mechanism. BMC Med 11(1):233
111. Davison M (2011) Pharmaceutical anti-counterfeiting: combating the real danger from fake drugs. John Wiley & Sons
112. Hamilton WL, Doyle C, Halliwell-Ewen M, Lambert G (2016) Public health interventions to protect against falsified medicines: a systematic review of international, national and local policies. Health Policy Plan 31(10):1448–1466
113. Fadlallah R, El-Jardali F, Annan F, Azzam H, Akl EA (2016) Strategies and systems-level interventions to combat or prevent drug counterfeiting: a systematic review of evidence beyond effectiveness. Pharmaceutical Medicine 30:263–276
114. Cohn JE, von Schoen-Angerer T, Jambert E, Arreghini G, Childs ML (2013) When falsified medicines enter the supply chain: description of an incident in Kenya and lessons learned for rapid response. J Public Health Policy 34:22–30
115. Cuomo RE, Mackey TK (2014) An exploration of counterfeit medicine surveillance strategies guided by geospatial analysis: lessons learned from counterfeit Avastin detection in the US drug supply chain. BMJ Open 4(12):e006657
116. Mackey TK, Cuomo R, Guerra C, Liang BA (2015) After counterfeit Avastin®—what have we learned and what can be done? Nat Rev Clin Oncol 12(5):302–308
117. Kamba PF, Ireeta ME, Balikuna S, Kaggwa B (2017) Threats posed by stockpiles of expired pharmaceuticals in low- and middle-income countries: a Ugandan perspective. Bull World Health Organ 95:594–598
118. Reynolds L, McKee M (2010) Organised crime and the efforts to combat it: a concern for public health. Glob Health 6(1):21
119. Ozawa S, Haynie DG, Bessias S, Laing SK, Ngamasana EL, Yemeke TT, Evans DR (2019) Modeling the economic impact of substandard and falsified antimalarials in the Democratic Republic of the Congo. Am J Trop Med Hyg 100(5):1149–1157
120. Weaver AA, Reiser H, Barstis T, Benvenuti M, Ghosh D, Hunckler M, Joy B, Koenig L, Raddell K, Lieberman M (2013) Paper analytical devices for fast field screening of beta lactam antibiotics and antituberculosis pharmaceuticals. Anal Chem 85(13):6453–6460
121. Weaver AA, Lieberman M (2015) Paper test cards for presumptive testing of very low quality antimalarial medications. The American Society of Tropical Medicine and Hygiene 92(6_Suppl):17–23
122. Marini RD, Rozet E, Montes MLA, Rohrbasser C, Roht S, Rhème D, Bonnabry P, Schappler J, Veuthey JL, Hubert P, Rudaz S (2010) Reliable low-cost capillary electrophoresis device for drug quality control and counterfeit medicines. J Pharm Biomed Anal 53(5):1278–1287

123. Bansal D, Malla S, Gudala K, Tiwari P (2013) Anti-counterfeit technologies: a pharmaceutical industry perspective. Sci Pharm 81(1):1–14
124. Lybecker KM (2008) Keeping it real: anticounterfeiting strategies in the pharmaceutical industry. Manag Decis Econ 29(5):389–405
125. Mackey TK, Nayyar GML (2017) A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opin Drug Saf 16:587–602
126. Taylor D (2014) RFID in the pharmaceutical industry: addressing counterfeits with technology. J Med Syst 38:1–5
127. Chen C, Zhang F, Barras J, Althoefer K, Bhunia S, Mandal S (2016) Authentication of medicines using nuclear quadrupole resonance spectroscopy. IEEE/ACM Trans Comput Biol Bioinf 13(3):417–430
128. Kwok SK, Ting SL, Tsang AHC, Cheung CF (2010) A counterfeit network analyzer based on RFID and EPC. Ind Manag Data Syst 110(7):1018–1037
129. Cozzella L, Simonetti C, Schirripa Spagnolo G (2012) Drug packaging security by means of white-light speckle. Opt Lasers Eng 50(10):1359–1371
130. Raj R, Rai N, Agarwal S (2019) Anticounterfeiting in pharmaceutical supply chain by establishing proof of ownership. in TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON). IEEE. pp 1572–1577
131. Kumar A, Choudhary D, Raju MS, Chaudhary DK, Sagar RK (2019) Combating counterfeit drugs: a quantitative analysis on cracking down the fake drug industry by using blockchain technology. in 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE. pp 174–178
132. Meyliana, Surjandy, Fernando E, Cassandra C, Marjuki (2021) Propose Model Blockchain Technology Based Good Manufacturing Practice Model of Pharmacy Industry in Indonesia. in 2021 2nd International Conference on Innovative and Creative Information Technology (ICITech). pp 190–194
133. Alzahrani N, Bulusu N (2020) A new product anti-counterfeiting blockchain using a truly decentralized dynamic consensus protocol. Concurrency and Computation: Practice Exp 32(12):e5232
134. Raja J, Khaled S, Nelson K (2019) Improving opportunities in healthcare supply chain processes via the internet of things and blockchain technology. International Journal of Healthcare Information Systems and Informatics (IJHISI) 14(2):49–65
135. Singh R, Dwivedi AD, Srivastava G (2020) Internet of Things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. Sensors 20(14):3951
136. Sylim PG, Liu F, Marcelo AB, Fontelo PA (2018) Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. JMIR Research Protocols, 7(9): e10163
137. Longo F, Nicoletti L, Padovano A, d'Atri G, Forte M (2019) Blockchain-enabled supply chain: an experimental study. Comput Ind Eng 136:57–69
138. Jamil F, Hang L, Kim K, Kim D (2019) A novel medical blockchain model for drug supply chain integrity management in a smart hospital. Electronics (Switzerland) 8(5)
139. Kumar R, Tripathi R (2019) Traceability of counterfeit medicine supply chain through Blockchain. in 11th International Conference on Communication Systems and Networks, COMSNETS 2019. Institute of Electrical and Electronics Engineers Inc. pp 568–570
140. Tseng J-H, Liao Y-C, Chong B, Liao S-W (2018) Governance on the drug supply chain via Gcoin blockchain. Int J Environ Res Public Health 15(6):1055
141. Shahbazi Z, Byun Y-C (2020) A procedure for tracing supply chains for perishable food based on blockchain, machine learning and fuzzy logic. Electronics 10(1):41
142. Tsang YP, Choy KL, Wu CH, Ho GTS, Lam HY (2019) Blockchain-Driven IoT for Food Traceability with an Integrated Consensus Mechanism. IEEE Access 7:129000–129017
143. Soon JM, Manning L (2019) Developing anti-counterfeiting measures: the role of smart packaging. Food Res Int 123:135–143

144. Fang Z, Zhao Y, Warner RD, Johnson SK (2017) Active and intelligent packaging in meat industry. Trends Food Sci Technol 61:60–71
145. Sohail M, Sun D-W, Zhu Z (2018) Recent developments in intelligent packaging for enhancing food quality and safety. Crit Rev Food Sci Nutr 58(15):2650–2662