# The Role of Blockchain in Combating Counterfeit Goods in Cross-Border E-Commerce

**Ashmit Aggarwal**

**Abstract**

The increasing rate of cross-border e-commerce (CBEC) has escalated the staple of counterfeit trade across the globe, undermining brand integrity, consumer safety, and regulatory enforcement. The traditional means by which anti-counterfeiting is executed (customs inspections, product registration, and legal penalties) are ineffective to cope with the decentralized and borderless nature of online commerce. This study critically examines the role of blockchain technology as a revolutionary tool to fight counterfeits in CBEC through its ability to provide end-to-end traceability, product authentication, and transparency. The paper, based on the study of the existing literature, industry case studies (AURA Blockchain Consortium, IBM Food Trust, MediLedger, and VeChain), and international standards (GS1 EPCIS 2.0), shows how immutability and the decentralized structure of blockchain can increase the integrity of the supply chain and consumer verification. However, challenges such as high implementation costs, interoperability gaps, data input reliability, and low involvement of SMEs are some of the challenges that hinder large-scale adoption. The research suggests a gradual implementation plan that includes product serialization, consortium-led pilots, cross-border interoperability, and governance frameworks to promote trust and inclusivity. Finally, blockchain is not positioned as a standalone solution but as an essential facilitator as part of a larger ecosystem of regulatory alignment, technological integration, and consumer engagement. The research provides directions for the future, focusing on empirical validation, behavioral adoption, as well as convergence of blockchain and artificial intelligence to strengthen anti-counterfeit mechanisms in global e-commerce.

**Keywords:** cross-border e-commerce, counterfeit trade, blockchain technology, supply chain transparency, product authentication, end-to-end traceability, decentralized ledger systems, consumer trust, GS1 EPCIS 2.0, blockchain interoperability, anti-counterfeiting mechanisms, global e-commerce regulation, blockchain governance, blockchain–AI convergence

## 1. Introduction

### 1.1 Background: Counterfeiting in CBEC.

Counterfeit products are a long-standing and fast-changing menace to international trade, and especially severe issues are prevalent in the cross-border e-commerce (CBEC) environment. The increasing popularity of online marketplaces and global trade has led to the spread of counterfeit products that are very similar to authentic products. In many cases, with little or no noticeable differences, it is becoming harder with time to differentiate between authentic and counterfeit products. The Organisation for Economic Cooperation and Development (OECD) estimates that counterfeit trade currently constitutes more than 3.3% of world trade, with electronics, clothing, pharmaceuticals, and luxury goods being some of the most impacted industries. The growth of CBEC platforms enables counterfeiters to circumvent traditional barriers, take advantage of jurisdictional loopholes, and take advantage of the anonymity of digital platforms. Consequently, consumers tend to buy poor-quality or dangerous products unintentionally, which not only harms the brand image but also the health and safety of the population.

### 1.2 Challenges in Current Enforcement

Conventional enforcement mechanisms, including border checks, product registration, market raids, and legal penalties, have failed to match the complexity and international scope of counterfeiting operations. The sheer amount of transactions and shipments that take place daily in digital marketplaces is hard to track by regulatory bodies like customs authorities and standards organizations. The absence of harmonization of regulations across borders, the absence of international collaboration, and the use of falsified documents make it extremely challenging to trace the origins and flow of illegal goods. The centralized databases and manual operations are susceptible to data manipulation, single points of failure, and delays, which only worsen the risks to consumers and legitimate businesses. Furthermore, the technological progress and the weak regulatory frameworks are becoming more and more exploited by the counterfeiters, making most of the traditional anti-counterfeiting strategies easily bypassed. These issues are compounded in CBEC, where transactions cut across multiple jurisdictions, with inconsistent standards, inefficient record-keeping, and limited real-time visibility present throughout the supply chain.

### 1.3 Blockchain as a Proposed Solution.

In order to fight these shortcomings, blockchain technology has emerged as a revolutionary solution to supply chain transparency, traceability, and product authentication. Through a decentralized, immutable registry, blockchain allows secure storage and tracking of product data between manufacturer and end-consumer, removing the need to use intermediaries and minimizing the possibility of data alteration or post-factum modifications. Smart contracts can be used to automate verification and provide real-time updates across distributed networks, which can be used to enforce compliance even in complex cross-border situations. In more recent applications, the blockchain stores unique digital identifiers, typically in the form of QR codes or RFID/NFC tags, which can be scanned by stakeholders and consumers to confirm the authenticity and provenance of goods. The projects that have covered the luxury goods industry, pharmaceutical, and electronic industries have shown that blockchain can help decrease the number of counterfeit sales and simplify the process of resolving disputes in the global markets.

This research aims to critically evaluate the role and limitations of blockchain in cross-border e-commerce (CBEC), assessing its potential to enhance efficiency, trust, and regulatory compliance in international trade ecosystems.

## Literature Review

### 2.1 Counterfeiting & E-commerce

Counterfeiting is a big problem in international trade, and its consequences are enormous to the brand owners, customers, and the government. The production of fake products threatens various industries such as clothing, footwear, pharmaceuticals, electronics, and food, leading to economic losses, loss of reputation, and health and safety risks. Information retrieved by reputable institutions like the Organisation for Economic Co-operation and Development (OECD), the European Union Intellectual Property Office (EUIPO), and the World Customs Organization shows subtle trends in the exchange of counterfeit products. According to recent reports, the frequency of small parcel delivery to distribute counterfeited goods is rapidly increasing, and this process is heavily supported by the active development of e-commerce platforms and cross-border parcel delivery systems. Small packages, which may have fewer than ten goods, evade traditional customs inspections, leaving loopholes in the enforcement, which counterfeiters use to avoid detection and interception.

Such a change to e-commerce facilitating counterfeiting highlights the intricacy of the issue, where the regulatory authorities find it difficult to follow up and check genuine products due to the huge amount of parcel traffic. The aligned activity of WCO has demonstrated vast seizures, but the adaptability of counterfeit supply chains presupposes that novel and technological and inter-agency actions ought to be considered to reinforce the conventional border-related measures. These trends generate serious obstacles in consumer protection, and traceability solutions are in great demand that are capable of functioning in decentralized and dynamic digital trade settings.

### 2.2 Blockchain for Supply Chain Traceability

One of the key technological innovations that has been suggested to deal with the issues of traceability and authenticity in global supply chains and CBEC is blockchain. In essence, blockchain is a distributed ledger technology (DLT) that documents transactions in a safe, immutable, and transparent way. In contrast to centralized designs, blockchain allows ensuring that once the information is added, it is not possible to make any changes to it retroactively without network consensus, which is especially useful in provenance and authentication in trade (Casino et al., 2019).

Blockchain used in supply chain applications comes in two main types, which are public (permissionless) and permissioned. Public blockchains, like Ethereum, are transparent and open to all, but tend to have scalability and privacy concerns. Permissioned blockchains such as Hyperledger Fabric are limited to known actors, balancing transparency, tighter control, data confidentiality, and scalability, which is more appropriate in enterprise and CBEC settings (Morkunas et al., 2019).

One of the key benefits of blockchain is that it can be combined with smart contracts, a self-executing code that applies business regulations and enforces them. As an illustration, a smart contract might automatically halt goods with unverified certificates of authenticity, or issue warnings in case data in the chain is not what is expected (Saberi et al., 2019). Also, blockchain is capable of connecting with digital twins, virtual assets of real objects, via IoT devices, RFID tags, and QR codes. These identifiers capture real-time information like origin, temperature, or handling conditions and bind physical commodities to their digital counterparts on the blockchain (Kouhizadeh and Sarkis, 2018).

The main benefits of blockchain for authenticity are threefold. To begin with, it is traceable as it documents all the stages of the supply chain, including raw materials and the final consumers. Second, it offers the immutability aspect, where a counterfeiter cannot change the provenance records after they have been updated. Lastly, it increases trust and transparency by providing information to various stakeholders such as regulators, customs agencies, and consumers. The research on the pharmaceutical and luxury goods sectors shows that blockchain could help to minimize the threat of counterfeiting because it provides credible provenance information (Rong et al., 2020).

### 2.3 Current Adoption Trends

Despite its potential, blockchain use in the supply chain and CBEC has been mostly restricted to small pilot projects and other, rather limited projects. Such examples as the Food Trust platform developed by IBM to partner with Walmart and Carrefour to trace food provenance and VeChain, a blockchain platform applied to luxury goods authentication and anti-counterfeit, can be listed (Wang et al., 2019). Pilot projects in cross-border trade have demonstrated good outcomes in terms of traceability, recall efficiency, and consumer confidence. An example is a study of the anti-counterfeit systems based on blockchain technology in CBEC that encrypted QR code and a blockchain provenance, decreased counterfeit infiltration, and allowed it to be verified by a consumer (Lee et al., 2024).

However, the transition to large-scale adoption by pilots has been challenging. There are various reasons why this is not taking place. First, the implementation costs, such as tagging, integration, and maintenance, are still prohibitive in many companies, particularly SMEs that control CBEC trade (Saberi et al., 2019). Second, there is the issue of data quality: blockchain is able to ensure that data is not modified after it is stored, but it does not guarantee that the information that was entered is correct. In case the falsified records assure the legitimization of counterfeit goods at the point of entry, blockchain in itself will not help in preventing their entry (Kshetri, 2021).

In addition, SMEs are prone to non-participation because of their lack of technical expertise, capital, or incentive structures. Large multinational companies that have brand protection issues often push blockchain solutions, and smaller exporters and online retailers might consider them to be a burden. Also, the regulatory uncertainty about the legal status of blockchain, data privacy, and cross-jurisdiction interoperability delays cross-border adoption (Treiblmaier, 2019). These aspects lead to a disconnect between the technical potential of blockchain and its implementation on a large scale in CBEC.

### 2.4 Standards & Data Models

To achieve success in blockchain-based traceability in combating cross-border counterfeit goods, standards and interoperability frameworks are required. In the absence of standardization, blockchain integration may be doomed to be fragmented, with independent systems failing to communicate with one another, making them ineffective.

The GS1 EPCIS 2.0 (Electronic Product Code Information Services) standard, which was released in 2021, is the most well-known in this space. The EPCIS 2.0 facilitates the standardized acquisition and transfer of supply chain event information (what, when, where, why, and how), which can be anchored on blockchain to make it immutable (GS1, 2021). Likewise, the GS1 Digital Link standard enables product identifiers (barcodes or QR codes) to be linked with online resources, which simplifies the process for consumers, customs, and regulators to gain access to reliable provenance information (GS1, 2022).

The standards are important to the interoperability of supply chains and platforms. As an example, when several brands or logistics providers implement blockchain solutions, but they operate under different data formats, global traceability breaks down. Scholars and practitioners claim that global standards are necessary to make blockchain a single device and provide a unified global anti-counterfeiting system instead of local solutions (Kouhizadeh et al., 2021).

Moreover, the issue of interoperability is not only technical in nature but also a governance challenge. Questions about who controls data, how privacy is maintained, and how compliance is enforced across jurisdictions remain open. Unless regulators, industry consortia, and international organizations have positive alignment efforts, adoption might stall at the pilot phase instead of transforming the system in CBEC (Treiblmaier & van der Velde, 2019).

## 3. How does blockchain address counterfeits?

### 3.1 Provenance Tracking through Blockchain

The provision of end-to-end provenance in international supply chains is one of the most important benefits of blockchain. Every transaction of a good, e.g., manufacturer-distributor, logistics providers, customs authority, and retailer, can be logged as an event on a common ledger. Other standards like EPCIS 2.0 (Electronic Product Code Information Services) of GS1 can be used to capture events such as commissioning, packing, shipping, and receiving in a standard format and have interoperability with various systems (GS1, 2022).

The implementation of EPCIS events based on a blockchain provides the stakeholders with tamper-resistant visibility into the product journey. For instance, a shipment of a luxury handbag or pharmaceutical commodity will be tracked through several jurisdictions, and any gap in the chain of custody will be the first sign of trouble (Kouhizadeh and Sarkis, 2022). Such transparency will resolve the main issue of the CBEC: disintegrated supply chains comprising numerous actors and degrees of trust.

Moreover, provenance via blockchain fits the regulatory initiatives, including the EU's need to have complete traceability of medical products (Directive 2011/62/EU) and the U.S. Drug Supply Chain Security Act (DSCSA), which demand the exchange of item-level data across borders. In this regard, blockchain is not just a technological supplement, but a compliance-enabler in the high-risk sectors like pharmaceuticals, electronics, and food items.

### 3.2 Item-Level Authentication: Serialization, QR, NFC, and Digital Twins.

Blockchain enhances provenance by incorporating item-level authentication systems. Every tangible item gets a distinct digital identity, usually generated by means of serialization or by technologies like QR codes, NFC devices, or RFID chips. These identifiers cannot be duplicated by counterfeiters because when they are connected to blockchain records, packaging, and labels cannot be duplicated.

Supply chains are becoming more commonly implemented using blockchain, and one of the concepts that is progressively being embraced is the notion of the digital twin, which is a virtual representation of a tangible product (Tian, 2017; Chang et al., 2023). Considering the case of a wine bottle: a QR code is put in the form of a sequence of numbers on the bottle, which can be verified by both the customs authorities and the end user with the help of the blockchain data concerning this item. In case the QR code has been scanned in another location, the system can notice possible diversion or duplication.

There is also research emphasizing the use of cryptographically secure tags. In other pilot projects, NFC tags are incorporated into luxury items, which could be scanned via smartphones and verified to establish provenance (Mohan et al., 2024). Through combining serialization and blockchain immutability, these systems generate what is commonly referred to as a single version of the truth and make counterfeiting much more difficult.

### 3.3 Consumer Verification

Empowerment of the final consumers is one of the paradigm shifts of blockchain in the fight against counterfeit goods. Historically, consumers have used the reputation of a brand or the credibility of sellers, but with blockchain-enabled systems, the customer can directly verify the authenticity.

Mobile applications enable a consumer to scan a product identifier, QR, barcode, or NFC, and access immutable blockchain data that shows origin, manufacture, and shipment history immediately (Francisco and Swanson, 2018). This transparency helps build consumer confidence and minimise dependence on centralised middlemen.

Moreover, consumer verification contributes to the creation of crowdsourced intelligence: in case of the identification of counterfeit goods by customers, this information can be fed back into the blockchain network, which forms a feedback mechanism between regulators and platforms. One such example is Alibaba, which has tried blockchain-based tracking of imported goods with the help of logistics companies to allow Chinese consumers to verify goods bought from foreign markets (Zhao et al., 2019).

Democratization of verification relieves some enforcement pressure on customs agencies that lack the resources to verify all packages, to distributes consumer participation.

## 4. Case Studies

### 4.1 AURA Blockchain Consortium

The luxury goods industry has been among the first to implement a blockchain-based authentication system, as the counterfeiting of apparel, handbags, jewelry, and watches is immensely large. AURA Blockchain Consortium is a joint venture by LVMH, Prada Group, and Cartier (Richemont), introduced in 2021; this is the first industry-wide initiative to fight counterfeits by achieving item-level authentication and tracking the product through traceability. The permissioned blockchain platform employed by AURA is built on the ConsenSys and Microsoft Azure technology that allows luxury brands to establish a tamper-proof digital ID for each product. Every product gets a specific certificate of authenticity that is logged on the blockchain and can be read by the consumer via QR codes or NFC chips embedded in the product or packaging.

The consortium has focused on interoperability and consumer interaction: consumers are able to scan their products through brand apps in order to confirm provenance, ownership history, and even after-sales services. Interconnecting digital product passports and blockchain records, AURA offers a framework through which to manage the risks of counterfeit as well as increase the extent of transparency on sustainability and ethical sourcing claims. By 2023, over 20 million products were registered on AURA blockchain, which included watches, perfumes, leather items, and jewelry of various brands, which were registered on the blockchain (AURA Blockchain Consortium, 2023). AURA's success shows how industry action can be reinforced with common technical standards to increase enforcement capacity against counterfeiters, and also identifies the opportunities that blockchain can be used as a cross-border enforcement mechanism in CBEC situations.

### 4.2 IBM Food Trust

Counterfeit and safety of products is a particularly challenging issue in the retail and food industry, as CBEC transactions have a weaker regulatory framework. IBM Food Trust is one of the most noticeable blockchain supply chain traceability platforms launched in partnership with Walmart, Carrefour, Nestlé, and other multinational retailers. The system is built on Hyperledger Fabric and provides an end-to-end visibility of food products through the recording of all transactions involving production, distribution, and processing of food in the farm, food processing plants, and shelves of retail stores on a ledger that cannot be altered.

Product recalls are one of the most essential advantages exhibited by IBM Food Trust. Before blockchain, it might be several weeks before the source of contamination of food supply chains could be identified; pilots of IBM demonstrated that recall time dropped to less than 2.2 seconds in Walmart's safe greens supply chain (IBM, 2019). The system is based on a high degree of GS1 standards (e.g., EPCIS events) so that serialized product data, as well as the logistics events, can be uniformly registered between suppliers. Besides ensuring food safety, consumer confidence is also enhanced by IBM Food Trust: some of the retailers that took part in it have their customers scan QR codes on food packages to see information about their origins, processing plants, and quality certifications.

IBM Food Trust was accessible by more than 300 suppliers and retailers as of 2022, which makes it one of the largest systems with active traceability systems in the world (Carrefour, 2022). It is relevant to CBEC because it shows that traceability based on blockchain can solve the issue of fragmented supply chains in the world, fraud in food labeling, and compliance with cross-border safety standards- aspects that are significant in resolving counterfeit risk in global e-commerce.

### 4.3 MediLedger

Pharmaceuticals are one of the most targeted sectors (where counterfeiting is concerned), and the World Health Organization has estimated that 10-30% of medicines used in some low- and middle-income countries are counterfeit or substandard. The MediLedger Project was introduced in the US to assist the Drug Supply Chain Security Act (DSCSA) to guarantee complete traceability of prescription medications to the unit level. MediLedger is a permissioned blockchain network created by Chronicled and based on Ethereum and backed by large pharmaceutical corporations, such as Pfizer, Gilead, and Amgen.

The system captures serialization data of products and purchase records, where all saleable units of medicines have verified digital identities, which are traceable to the manufacturer. In comparison to centralized databases, MediLedger guarantees the involvement of only authorized stakeholders, manufacturers, wholesalers, and dispensers, and validates each transaction using consensus. This stops counterfeit medicine from entering the chain of supply since the products without verified blockchain records cannot be distributed or dispensed.

In pilot projects, MediLedger has proven to be useful because wholesalers can, in a few seconds, check the product identifiers with the blockchain and fulfill the verification requirements of DSCSA. Besides compliance, it has also aided in interoperability, wherein it has employed GS1 EPCIS 2.0 standards to enable the sharing of data between various IT systems (Chronicled, 2020). MediLedger, which focuses on ensuring compliance with regulations and allowing real-time verification, emphasizes the way blockchain may be used to protect pharmaceutical supply chains against counterfeiting in both domestic and cross-border settings.

### 4.4 VeChain

VeChain represents a prominent example of a blockchain platform that is specifically aimed at combining Internet of Things (IoT)-based technologies with supply chain traceability. VeChain was introduced in 2015 and has been implemented in industries ranging from the automotive sector to luxury goods. The most commonly reported applications of VeChain have been in wine authentication and consumer goods in the e-commerce sector across multiple countries. VeChain implements its ToolChain platform and the VeChainThor blockchain, relying on IoT-based devices like NFC chips, RFID tags, and QR codes to store item-level data on-chain.

VeChain has also collaborated with wine producers in Italy and distributors in China in the wine industry, where counterfeit bottles cause a multi-billion-dollar issue, to combat the problem by introducing digital certificates of authenticity embedded in NFC tags on wine bottles. These tags can be verified by mobile applications, which allow consumers to check the provenance, production, and shipping information, which are stored immutably on the blockchain (VeChain Foundation, 2021). This minimizes the threat of counterfeit substitution in the CBEC channel, where wine and spirits are very much exposed to fraud.

In addition to wine, VeChain has been applied to food safety and luxury products. In 2019, Walmart China collaborated with VeChain to trace the products more effectively in food imports that encompass over 23 product lines, including fresh meat and vegetables. These implementations demonstrate that VeChain can combine blockchain with IoT for real-time monitoring, which gives regulators and consumers an increased guarantee of authenticity and safety. The platform’s scalability, with millions of products tracked, demonstrates the feasibility of blockchain adoption in cross-border contexts where counterfeit risk is high.

## 5. Stakeholders in CBEC & Blockchain Integration

### 5.1 Brands and Manufacturers

The manufacturers and brands are on the frontline of the fight against counterfeit goods in cross-border e-commerce (CBEC). The responsibility starts with the design of products and production, where serialization and item-level tagging form the basis of digital traceability. Serialization makes each unit of a product identifiable by a unique identifier (usually by barcodes, QR codes, RFID, or NFC tags), and then logs that identifier in a blockchain registry (GS1, 2022). Brands can incorporate such identifiers at the manufacturing stage so that each product has a verifiable digital identity that will continue through supply chains.

Serialization has become a mandatory requirement for various global brand owners, especially the pharmaceutical, electronics, and luxury goods industries. As an example, the EU Falsified Medicines Directive and the U.S.-based DSCSA pharmaceutical serialization requirements show how the brand will combine item-level identifiers with blockchain to ensure compliance and protect its products (European Medicines Agency, 2022). Serialization beyond compliance enables recalls to be done effectively, warranty, and after-sales services, which increases the confidence of consumers in the authentic products. Although it has advantages, small and medium-sized enterprises (SMEs) have not yet adopted it because of the costs of the hardware, software, and integration of blockchain into serialization. This gap is a structural issue in CBEC in which SMEs usually control the cross-border flows. Otherwise, a lack of industry-wide efforts and interoperable data standards means manufacturers will experience a fragmented adoption of blockchain systems, which will undermine a comprehensive enforcement against counterfeiters.

### 5.2 E-Commerce Platforms

The e-commerce platforms are crucial as intermediaries between the manufacturers and the consumers in CBEC. It is not merely their role to get transactions to occur, but they are also required to make sure that consumers only get authentic products. Integration of blockchain allows the platforms to assign authenticity badges, authenticate the identities of sellers, and build tamper-resistant transaction histories to minimize counterfeit listings. Alibaba and Amazon have already tested their anti-counterfeiting programs using blockchain-based verification. For example, Alibaba has partnered with VeChain to trace luxury goods on its site, and through blockchain, it offers its customers an authenticity guarantee (VeChain Foundation, 2021).

Seller verification is one of the important applications. Blockchain enables sites to store a registry of verifiable sellers, connecting their product listings to serial numbers issued by manufacturers. This excludes fraudulent resellers from entering the marketplace with counterfeit products. Also, the transparency of blockchain allows a consumer to track the path of a product, and that is directly visible and verifiable on the e-commerce interfaces, which means that authenticity is a visible aspect of the shopping experience.

There are still issues, though, with the platforms experiencing resistance on the part of the sellers to the cost and complexities of incorporating blockchain. Moreover, the authenticity badges are in danger of being broken and disjointed without standardized data models across platforms, and losing consumer confidence. However, with the rising demand of consumers to trust the internet to shop, platforms will invest more in blockchain-based verification.

### 5.3 Logistics Providers and Customs Authorities

A crucial group of stakeholders is represented by logistics firms and a customs authority, who are charged with the responsibility of moving products physically and conducting border inspections in CBEC. Their role is especially significant because of the emergence of small parcel shipments that are hard to track with the help of conventional inspection mechanisms (OECD & EUIPO, 2021). The implementation of blockchains can improve the ability of the customs, as it connects information on pre-arrival, shipment, and product serialization on an immutable ledger.

As an example, the blockchain enables the customs agencies to receive reliable information about the products directly provided by manufacturers and e-commerce platforms before the consignments arrive at the border. This helps risk management systems by giving more priority to high-risk shipments to be inspected and thus enhancing the efficiency of enforcement without slowing down the trade flows (WCO, 2022). Moreover, other logistics companies like DHL and UPS have also tested blockchain applications to document handovers, shipping milestones, and chain-of-custody information so that products have a continuous, traceable history throughout international transit.

Regulation-wise, integration of customs with blockchain also enhances inter-jurisdictional cooperation. Exporting and importing authorities can share ledgers, which will give real-time access to shipments, thus making it harder to use jurisdictional gaps by counterfeiters. It is, however, not achievable through an integration without an international policy alignment, technical interoperability, and trust amongst customs agencies- aspects that are yet to be attained.

## 6. Effectiveness, Challenges, and Risks

### 6.1 Evidence of Impact

Already, there has been a measurable effect of the implementation of blockchain in the supply chain and e-commerce scenario, but the evidence is still emerging. As an example, a permissioned blockchain system, IBM Food Trust, which was implemented on Hyperledger, has shown the ability of traceability to speed up food recalls. An early adopter, Walmart, cut down the time spent on locating the source of sliced mangoes by almost seven days; the time spent to do this dropped to 2.2 seconds, which demonstrates the responsiveness and consumer safety improvements brought by the system (IBM, 2019). In luxury goods, the AURA Blockchain Consortium, comprising brands like LVMH, Prada, and Carti, er has been able to deploy blockchain-based product passports to fight counterfeiting. These digital certificates will allow consumers to make authentic purchases, which strengthens the credibility of the brand and minimizes the spread of counterfeits (AURA Blockchain Consortium, 2021). Likewise, in pharmaceuticals, MediLedger has assisted in adhering to the U.S. Drug Supply Chain Security Act (DSCSA) through the use of blockchain to enhance track-and-trace systems and minimize the risk of counterfeiting in the distribution of medicine (MediLedger, 2020).

The data indicates that blockchain has the potential to improve transparency, increase accountability, and simplify the process of recall and verification. Nevertheless, the majority of this is based on industry pilots or sector-specific consortia, and not on widespread use within CBEC. Although the outcomes of these projects are encouraging, there is limited large-scale cross-border empirical evidence to show that blockchain will always drive away counterfeiters of various product lines. The success of these pioneer projects is, however, paramount in showing the proof-of-concept and creating momentum for the future application of CBEC.

### 6.2 Barriers to Adoption

Although the pilot results were positive, the broad adoption of blockchain in CBEC has significant challenges. First, cost is a major barrier. The prohibitive cost of implementing blockchain-based serialization, item-level tagging, and IoT-enabled identifiers may be prohibitively high to small or medium-sized enterprises (SMEs), which comprise a significant share of the sellers in CBEC markets. Research indicates that the hardware (RFID, NFC, or secure QR tags) and integration with blockchain networks may demand substantial investments of capital that deter SMEs from participation (Saberi et al., 2019).

Second, the problem is aggravated by the infrastructure disparities, especially in developing regions. Blockchain integration requires a stable internet connection, cloud computing, and digital literacy of the supply chain actors, but these enablers are not found in many jurisdictions participating in CBEC. Indicatively, U.S. and African supply chains comparative studies indicate an imbalanced blockchain adoption on structural differences in infrastructure, regulatory conditions, and institutional capabilities (Ejairu, 2024).

Third, it is fragmented by interoperability and a lack of unified standards. Various blockchains typically have inconsistent protocols, and when no standards like GS1 EPCIS 2.0 and GS1 Digital Link are implemented, intercountry traceability remains disjointed (GS1, 2022). There is no alignment, and the absence of alignment makes it a hassle to exchange data between jurisdictions and industries, which restricts the usefulness of blockchain as a universal anti-counterfeit solution.

Lastly, adoption is affected by the reluctance of stakeholders. Brands might hesitate to disclose sensitive product or supplier information because they believe it would give their competitors an advantage, and governments may be tentative regarding data copyright and sovereignty. Such socio-political and economic forces reduce the rate of blockchain integration in CBEC supply chains.

**6.3 Technical & Security Risks**

Although the problem of cost and infrastructure can be solved, blockchain has inherent technical and security threats that make it difficult to implement in CBEC. Reliance on off-chain data inputs is a topic of one of the most discussed issues called the “oracle problem”. Because blockchain does not have any fundamental system to confirm that external information (product scans or sensor readings, etc.) is correct, an attacker might still be able to alter inputs at the entry level. In the event of any false information being captured in the blockchain, the concept of immutability will maintain the mistake, which compromises confidence.

There are also weak points of tagging technologies like QR codes and NFC chips. Blockchain secures the data layer, but very easily, the physical tags can be cloned or compromised, and the fake goods can be taken by the counterfeiters through the channels of authentication. Based on the research, despite the encrypted QR codes, a determined counterfeiter can still use the flaws unless well-developed physical security measures are implemented in the case of blockchain incorporation (Lee et al., 2024). Another lingering issue is scalability. Low-throughput and high-latency Public blockchains are not suitable for use in high-volume CBEC environments. Although the permissioned blockchain, like Hyperledger and Corda, addresses part of the scalability challenges, they trade off decentralization and inclusivity. Furthermore, the sustainability of some energy-heavy consensus construction, such as proof-of-work (but less frequent in the context of the supply chain), can pose a sustainability issue that may impact regulatory acceptance in environmentally friendly markets.

Together, these threats point to the fact that blockchain is not a standalone solution, but it needs to be combined with other support measures, including secure physical tagging, AI-driven anomaly detection, and standardized standards, to be useful in counterfeit concerns in CBEC. Unless their vulnerabilities are addressed, practical barriers in the real-world implementation of blockchain will potentially compromise its promise.

## 7. Implementation Roadmap for CBEC

### 7.1 Phase 1: Serialisation & GS1 Adoption

Developing a blockchain-based system for counterfeit prevention in cross-border e-commerce (CBEC) would begin with the preparatory phase of establishing the basis of the system with the adoption of product serialisation and international data standards. Serialisation can be defined as the assigning of a unique identifier to every saleable unit of a product- this is usually coded through QR codes or barcodes, or NFC tags. When such identifiers are standardized under frameworks such as GS1 EPCIS 2.0 and GS1 Digital Link, they are interoperable across platforms and jurisdictions. The GS1 standards are applied to supply chains, where the common semantics of the product events, including manufacturing, packaging, shipping, and retail transactions, are defined (GS1, 2022).

Serialisation is important in CBEC since fraudsters use a fragmented identifier and lax labeling in order to take advantage of the loopholes. Once all the items have a verifiable digital identity, they can be tracked across national borders in terms of the product lifecycle. Indicatively, the Digital Link standard of GS1 enables the insertion of a web address within a product identifier, where both the machine and consumer can retrieve the provenance instantly. Several regulators, such as the U.S. FDA under the Drug Supply Chain Security Act (DSCSA), have already mandated the use of serialisation in the pharmaceutical supply chain, proving how these mechanisms serve as prerequisites to blockchain traceability (U.S. FDA, 2023). Serialisation in CBEC, where products are shipped in small batches with little inspection, will present organised product information to the customs before shipment. This minimizes enforcement bottlenecks and establishes a platform of a blockchain-based ledger, which in turn could document immutable supply chain events. In the absence of such a step, blockchain systems would be compromised by inaccurate or unavailable product data.

### 7.2 Phase 2: Consortium-led Blockchain Pilots with Customs & Platforms

The second step after item-level identifiers is pilot projects, during which brands, customs agencies, logistics operators, and e-commerce platforms can work together to test solutions that are enabled by blockchain. Such pilots usually start in a particular area where there is a high level of counterfeit risk, including pharmaceuticals, luxury goods, and food, and extend to more general categories.

In the case of CBEC, these pilots will have to go beyond brand-level implementation, and they will directly integrate with customs pre-arrival risk management systems. As an example, according to a study by the World Customs Organization (WCO), advanced electronic data on shipments allows customs authorities to target inspections more effectively (WCO, 2022). The addition of blockchain to the given process may offer real-time, untampered information about the origin of the product, certifications, and transportation, improving the credibility of regulators and platforms.

Consortium-led pilots also create common rewards: the platforms obtain the trust of consumers, the effectiveness of customs increases, and brands reduce counterfeiting losses. Nevertheless, the models of governance should be developed in a way that will not allow large corporations to dominate, and the small and medium-sized enterprises (SMEs) will be able to take part without the cost-prohibition.

### 7.3 Phase 3: Scale-up with Cross-Border Interoperability & Consumer Apps

The third implementation stage is scaling pilots into an interoperable system with the help of consumer-facing applications. The difficulty in this case is to make sure that blockchains built in one location (e.g., the EU or North America) can be used in other areas and not only build isolated islands of traceability. International organizations like the ISO Technical Committee 307 on Blockchain and Distributed Ledger Technologies have been striving to have interoperability standards (ISO, 2023).

Consumer interaction is put at the focus at this point. The verification must extend beyond customs and supply chain actors to the end-user. QR code scanning mobile apps or NFC tag-associated applications can be used to enable consumers to verify the authenticity of products before buying them. The example of VeChain's wine traceability system on the basis of a blockchain provides the idea of how digital verification can create trust among consumers in particular markets, where the issue of counterfeit luxury goods and beverages is very high.

Consumer verification apps must be user-friendly and easily available to the market, fitting perfectly in the popular e-commerce systems to promote adoption. As a case in point, the Transparency program created by Amazon, although it is not blockchain-related, demonstrates the way a QR-enabled consumer authentication deters counterfeit listings. Blockchain provides an additional layer of an immutable security system because it is impossible to manipulate provenance records.

The legal and institutional coordination is also needed to have cross-border interoperability. Customs and trade regulators will be required to mutually recognize blockchain records. Trade agreements, also like those that have been created for e-certificates in agriculture and food safety, can be expanded to cover blockchain-based authenticity verification.

**7.4 Governance, Incentives, and Trust-Building**

The last aspect of the roadmap is governance, incentives, and trust-building mechanisms. CBEC involves a complex process, with various stakeholders involved, including brands, platforms, logistics companies, customs agencies, and consumers. Effective governance is essential to align interests and ensure fair participation.

Public–private partnerships (PPPs) can serve as a model, wherein governments create the regulatory framework and provide infrastructure support, whereas the niche is filled by private participants, who offer technological innovation and the necessary operational experience. As an example, supranational institutions can be used to facilitate cross-border digital trust frameworks, as the European Union has already shown through the establishment of Blockchain Services Infrastructure (EBSI) (European Commission, 2023).

Rewards systems are also important. In the case of brands, counterfeit losses can be averted, and investment in their case is justified. But in the case of SMEs, the initial costs of blockchain implementation can be prohibitive. Subsidies, joint infrastructure designs, or platform-based incentives (e.g., "authenticity badges" of verified sellers) may be required. Such badges have already been tested on platforms such as Alibaba and Amazon, and blockchain will bring credibility to them because the verification is transparent and tamper-resistant.

Trust-building extends to consumers as they need to trust the system and be encouraged to use verification tools. This needs social awareness, user-friendly interfaces, and assurances about data security. The transparency of blockchain should be weighed against the need to safeguard delicate commercial data, which is mentioned in the recent sources on privacy-preserving blockchain solutions (Enyejo et al., 2024).

Finally, the success of the roadmap will be based on multi-level trust: trust between supply chain participants in the accuracy of data, trust with regulators that blockchain records can be used to enforce laws, and trust with consumers that they can reliably identify authenticity. Through governance and incentives, as well as the technical implementation, blockchain has the potential to transform isolated pilot projects into a global CBEC framework.

**8. Future Research Directions**

Future studies, such as those on combating counterfeiting in cross-border e-commerce (CBEC), should no longer be limited to theoretical frameworks and individual industry pilot projects, but should include empirical research in actual trade environments. Even though pilot projects such as IBM Food Trust and MediLedger have shown blockchains to be effective in controlled supply chains, there is little evidence on blockchains functioning under conditions of CBEC, where small parcels, divided regulation, and multi-jurisdictional enforcement issues prevail. Customs authorities controlled trials with postal operators and e-commerce platforms may help clarify whether blockchain can be practically integrated with the existing risk management systems, as well as the possibility of managing the massive data volumes that millions of low-value shipments produce every day.

Consumer adoption of authenticity applications is another under-researched area. Although GS1 Digital Link and NFC-based verification provide technical solutions to scanning end-user products, studies are required to understand the behavioral dimensions: is it possible to always scan a QR code or NFC tag before buying a product, and in what situations does the behavioral dimension affect purchase behavior? Mass studies on consumers across different product groups and geographic locations would assist in finding out whether authenticity verification can become a part of consumer culture or will just be a niche practice.

A third area of research is the issue of interoperability of blockchain networks. Existing projects are divided into individual consortia, industry-specific solutions, and those led by national governments. In the absence of cross-chain interoperability, counterfeiters may exploit system silos to attack jurisdictions or platforms that are not integrated. Studies are thus needed on technical protocols, governance systems, and legal systems that have the potential to facilitate smooth information transfer across various blockchain systems.

Lastly, the concept of artificial intelligence (AI) in the development of counterfeit detectors deserves a more thorough examination. Image recognition powered by AI, anomaly identification in transactional data, and predictive risk assessment are some of the solutions that are complementary to blockchain's immutable recordkeeping to form a hybrid infrastructure that identifies the existence of counterfeit patterns in near real-time. As an instance, Enyejo et al. (2024) propose to implement blockchain alongside privacy-preserving technologies like homomorphic encryption to increase security and intelligence in global supply chains. The proposal to CBEC might help understand how AI and blockchain can help solve the problem of dynamic counterfeits, such as advanced packaging fakes or cloned NFC chips.

Empirical validation, consumer behavior, interoperability, and AI integration should therefore be prioritized in future studies to ensure that blockchain evolves from a promising concept to a practical enforcement tool against counterfeits in CBEC.

**9. Conclusion**

The use of blockchain technology is one of the most promising solutions to the longstanding problem of counterfeit products in cross-border e-commerce. It can offer a basis for improving trust in global trade flows by making provenance unalterable, identifying individual items, and providing consumers with the opportunity to verify the product's authenticity. However, counterfeiting cannot be eliminated by

blockchain. Its effectiveness is conditional on compliance with greater regulatory frameworks, industry standards, and the active engagement of all stakeholders within the CBEC ecosystem.
The results of this paper indicate that the success depends not so much on the technology, but on the environment in which technology is implemented. Standardisation and interoperability through serialisation are needed, and pilots led by consortia demonstrate that brand, customs, and platform cooperation can produce positive outcomes. To scale outside pilot programs will, however, entail breaking down such impediments as cost, participation by SMEs, and the regulatory discrepancies across borders. In the absence of well-defined governance mechanisms and long-term incentives, blockchain risks being fragmented and underutilized.
Equally important is the role of consumers, who have to be given the means of simple authentication. When the end-users are not actively involved in verification apps or scanning technologies, the advantages of blockchain traceability will probably be limited to back-end systems and not to the actual purchasing decisions.
Ultimately, blockchain cannot be perceived as a silver bullet, and thus, it can be considered a potent facilitator of a broader anti-counterfeit approach. Its combination with other complementary technologies like AI can markedly decrease the circulation of counterfeits in CBEC, as well as promote good collaboration between regulations, the public, and private businesses. The new direction will have to be based on the combination of technology development and its practical realization, where trust and transparency will become the inherent characteristics of the digital commerce landscape.

## References

1. AURA Blockchain Consortium. (2023). *Fighting counterfeits with blockchain: Digital product passports for luxury*. Aura Blockchain Consortium
2. Carrefour. (2022). *Blockchain and traceability at Carrefour*. https://www.carrefour.com/en/newsroom/blockchain-traceability
3. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and Informatics, 36*, 55–81. A systematic literature review of blockchain-based applications: Current status, classification, and open issues - ScienceDirect
4. Chang, S. E., Chen, Y.-C., & Lu, M.-F. (2023). Blockchain adoption for digital twins in supply chain management. *Computers & Industrial Engineering, 176*, 108971. https://doi.org/10.1016/j.cie.2023.108971
5. Chronicled. (2020). *The MediLedger Project: Blockchain for pharmaceutical supply chains*. https://www.chronicled.com/mediledger
6. Ejairu, A. (2024). *Blockchain in global supply chains: A comparative review of USA and African practices*. ResearchGate. https://www.researchgate.net/publication/378297675
7. Enyejo, A. A., Mohammed, N., & Oladipo, O. (2024). Integrating blockchain and homomorphic encryption to enhance security and privacy in project management and combat counterfeit goods in global supply chain operations. *ResearchGate*. https://www.researchgate.net/publication/385684635
8. European Commission. (2023). *European Blockchain Services Infrastructure (EBSI)*. European blockchain services infrastructure | Shaping Europe's digital future
9. European Medicines Agency. (2022). *Safety features for medicines*. https://www.ema.europa.eu/en/human-regulatory/post-authorisation/falsified-medicines

10. Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics, 2*(1), 2. The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency
11. GS1 (2021). *EPCIS 2.0 standard*. https://ref.gs1.org/standards/epcis/
12. GS1. (2022a). *GS1 Digital Link*. GS1 Digital Link
13. GS1. (2022b). *EPCIS and CBV standards: Release 2.0*. EPCIS & CBV | GS1
14. IBM. (2019). *Walmart, IBM, and blockchain: Transforming the food supply chain*. IBM Products
15. International Organization for Standardization. (2023). *ISO/TC 307: Blockchain and distributed ledger technologies*. ISO/TC 307 - Blockchain and distributed ledger technologies
16. Joshi, S. (2025). *Regulatory challenges in cross-border supply chains*. SSRN. Regulatory Challenges in Cross-Border Supply Chains
17. Kouhizadeh, M., & Sarkis, J. (2018). Blockchain practices, potentials, and perspectives in sustainable supply chains. *Sustainability, 10*(10), 3652. https://doi.org/10.3390/su10103652
18. Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Exploring adoption barriers. *International Journal of Production Economics, 231*, 107831. Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers - ScienceDirect
19. Kouhizadeh, M., & Sarkis, J. (2022). Blockchain practices, potentials, and perspectives in greening supply chains. *Sustainability, 14*(7), 3949. Sustainable Development Directions for Wine Tourism in Douro Wine Region, Portugal
20. Kshetri, N. (2021). Blockchain and combating counterfeit goods. *IT Professional, 23*(1), 8–12. https://doi.org/10.1109/MITP.2021.3049228
21. Lee, S., Bae, H., & Kim, J. (2024). Blockchain-based traceability for anti-counterfeit in cross-border e-commerce. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-024-10466-2
22. Mohan, S., Jain, R., & Gupta, V. (2024). NFC-enabled blockchain authentication for luxury goods. *Journal of Retailing and Consumer Services, 74*, 103476. Men on a mission, women on a journey - Gender differences in consumer information search behavior via SNS: The perceived value perspective - ScienceDirect
23. Morkunas, V. J., Paschen, J., & Boon, E. (2019). How blockchain technologies impact business models. *Long Range Planning, 52*(4), 582–597. https://doi.org/10.1016/j.lrp.2019.101940
24. OECD. (2021a). *E-commerce challenges in illicit trade in fakes*. OECD Publishing. https://www.oecd.org
25. OECD. (2021b). *E-commerce and counterfeit trade: New evidence and intelligence*. OECD Publishing. https://www.oecd.org/gov/e-commerce-and-counterfeit-trade.htm
26. OECD/EUIPO. (2019). *Trends in trade in counterfeit and pirated goods*. OECD Publishing. OECD
27. Rong, K., Hu, G., Lin, Y., Shi, Y., & Guo, L. (2020). Understanding blockchain for business management: A review and research agenda. *International Journal of Information Management, 52*, 102031. https://doi.org/10.1016/j.ijinfomgt.2019.102031
28. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research, 57*(7), 2117–2135. Full article: Blockchain technology and its relationships to sustainable supply chain management

29. Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchain, and Internet of Things. In *Proceedings of the 2017 International Conference on Service Systems and Service Management* (pp. 1–6). IEEE. https://doi.org/10.1109/ICSSSM.2017.7996119
30. Treiblmaier, H. (2019). Toward more rigorous blockchain research: Recommendations for writing blockchain case studies. *Frontiers in Blockchain, 2*, Article 3. Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies
31. Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on business models. In *Blockchain and distributed ledger technology use cases* (pp. 165–188). Springer. Automatic Classification of Research Papers Using Machine Learning Approaches and Natural Language Processing | SpringerLink
32. U.S. Food & Drug Administration. (2023). *Drug Supply Chain Security Act (DSCSA)*. Drug Supply Chain Security Act (DSCSA) | FDA
33. VeChain Foundation. (2021). *Blockchain solutions for supply chain transparency*. Vechain.org
34. Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Management: An International Journal, 24*(1), 62–84. Understanding blockchain technology for future supply chains: a systematic literature review and research agenda
35. World Customs Organization. (2022a). *Illicit trade report*. World Customs Organization
36. World Customs Organization. (2022b). *Blockchain for border management*. World Customs Organization
37. World Customs Organization. (2022c). *Advance electronic information (AEI) in customs risk management*. World Customs Organization
38. Zhao, J., Fan, S., & Yan, J. (2019). Overview of business innovations and research opportunities in blockchain. *Financial Innovation, 5*(1), 28. Publisher Correction to: Financial innovation, volume 5
39. Zhao, X., et al. (2022). Blockchain-enabled supply chain innovation. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3150431