



# Blockchain for Product Authenticity in the Cannabis Supply Chain

Sven Januszek, Andreas Siegrist, Torbjørn H. Netland

## ► To cite this version:

Sven Januszek, Andreas Siegrist, Torbjørn H. Netland. Blockchain for Product Authenticity in the Cannabis Supply Chain. IFIP International Conference on Advances in Production Management Systems (APMS), Sep 2021, Nantes, France. pp.62-69, 10.1007/978-3-030-85910-7\_7 . hal-03806504

**HAL Id: hal-03806504**

**<https://inria.hal.science/hal-03806504v1>**

Submitted on 7 Oct 2022

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License



This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

# Blockchain for Product Authenticity in the Cannabis Supply Chain

Sven Januszek<sup>(✉)</sup>[0000-0002-8653-4622], Andreas Siegrist<sup>[0000-0001-5004-2653]</sup>,  
and Torbjørn H. Netland<sup>[0000-0001-7382-1051]</sup>

ETH Zürich, Weinbergstr. 56/58, 8050 Zürich, Switzerland  
sjanuszek@ethz.ch

**Abstract.** Cannabis is an emerging industry and like other strictly regulated products prone to fraud. Its medical application and increased regulatory pressure call for secure supply chains and product authenticity. Blockchain’s capability to strengthen end-to-end traceability in supply chains has the potential to provide the required levels of assurance. In this study, we, describe effective ways of how to integrate Blockchain technology within the cannabis supply chain and other required technologies to ensure product authenticity. Our results show that blockchain is a powerful and promising technology that can effectively improve supply chain transparency and support regulatory compliance. Nevertheless, blockchain alone can only ensure data security and does not capture the linkage between the physical product and its data, which is an important consideration regarding product fraud. For this reason, we conclude that blockchain is an enabling technology that still needs to be supported by further supplementary technologies, such as nuclear magnetic resonance-based screening technology, Internet of Things, and communication standards. Used together, these technologies can ensure product authenticity in cannabis supply chains.

**Keywords:** Blockchain, Supply chain, Product authenticity

## 1 Introduction

Product fraud, especially in the pharmaceutical sector, is happening worldwide in high numbers. The global market of substandard (failing to meet quality standards) or falsified (deliberate misrepresentation of composition, identity, or source) medicines is estimated to be worth up to 200 billion USD [1]. The World Health Organization estimated that more than 10% of the global drug supply is counterfeit [2], threatening not only economic stability but also public health.

Medical cannabis is a fast-growing industry that is not excluded from product fraud. Like any crop, it can be tainted by natural (e.g., microbial toxins in soil) or artificial (e.g., pesticides, miticides, and fungicides) adulterants. Studies have shown that cannabidiol (CBD) products are subject to mislabeling and contamination indicating safety issues for consumers (Evans, 2020). For example, a study conducted by the U.S. Food and Drug Administration (FDA) analyzed 108 CBD products and found significant

discrepancies between the claimed and tested CBD and tetrahydrocannabinol (THC) amounts [3].

To protect consumers from exposure to drugs that may be fraudulent or otherwise harmful, US Congress has enacted the Drug Quality and Security Act, which requires pharmaceutical companies to establish an electronic and interoperable system to trace prescription drugs throughout their entire supply chains by 2024. To enhance the security of drug supply chains further, another requirement is to notify the FDA and other trading partners within 24 hours after identifying an illegitimate product.

Despite the regulatory pressure to develop effective ways of tracking, sharing, and reporting information, pharmaceutical supply chains still lack enough traceability to meet the new requirements. Blockchain's immutability and tracking capabilities could change that [cf. 4, 5]. In this study, we, therefore, set out to discuss applications of blockchain in the cannabis supply chain to minimize fraud and ensure product authenticity.

## 2 Fraud in the Cannabis Supply Chain

### 2.1 Product Fraud

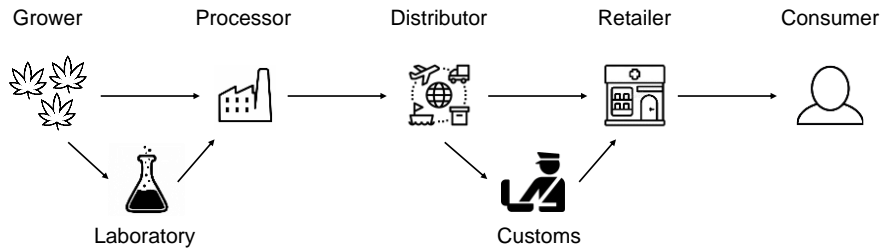
Fraud, in general, is the intentional deception, trickery, or misrepresentation of facts by one person alone or acting on behalf of an organization. Product fraud in particular is often economically motivated and can be classified into seven types (see Table 1). The higher the product value is, representing a popular brand, a quality label, or a specific health claim, the more it is prone to fraudulent activities. Product fraud can destroy consumer trust and has the potential, dependent on the nature of the fraud, to even risk human health and life [6, 7].

**Table 1.** Seven Types of Product Fraud (Spink and Moyer, 2011).

Type	Definition
Adulteration	A component of the finished product is fraudulent
Tampering	Legitimate product and packaging are used in a fraudulent way
Over-Run	Legitimate product is made in excess of production agreements
Theft	Legitimate product is stolen and passed off as legitimately procured
Diversion	The sale or distribution of legitimate products outside of intended markets
Simulation	An illegitimate product is designed to look like the legitimate product
Counterfeit	All aspects of the fraudulent product and packaging are fully replicated

## 2.2 Cannabis Supply Chain

The medical cannabis supply chain is governed by strict standards for safety and consistent quality. All participants of the supply chain, therefore, need to be licensed and the distribution of products requires a specialized, controlled distribution channel. Furthermore, all products must undergo a series of several tests and investigations before they are sold. Many laboratories and testing centers are even run by the government, but there is an increasing number of licensed private laboratories to handle quality control. Figure 1 shows a typical example of the Cannabis supply chain, for simplicity without any regulatory authorities.



**Fig. 1.** Example of a Cannabis Supply Chain.

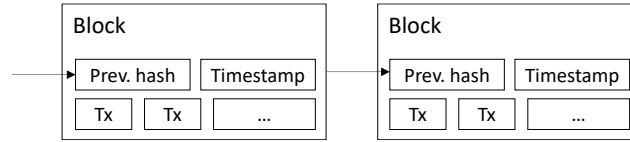
Despite being highly regulated and controlled, fraud is still happening in the cannabis supply chain—as in many food supply chains [8]. Examples include unlicensed growers selling cannabis to processors, adulterated test reports, and false labeling of the sold goods [9, 10].

Today’s global and complex supply chains, having multiple national and regulatory boundaries, make it more difficult to trace products, especially where products change hands several times on paper or physically [11]. In addition to the supply chain complexity, there is also a lack of visibility and trust, and the potential of data swamping retailers, businesses, and their employees [12]. Hence, the need for technological support to enhance traceability and control in the cannabis supply chain calls for further research.

## 3 Blockchain Technology

### 3.1 Blockchain Definition

Blockchain is a distributed ledger technology (DLT), which means it is a digital dataset being shared and synchronized without any central administrator. It consists of a series of connected blocks, which contain a cryptographic signature of the previous block, a timestamp, and transaction data (see Figure 2). A peer-to-peer network continuously solves cryptographic puzzles and validates transactions, this way adding new blocks to the chain [4, 5, 13].



**Fig. 2.** Linking of Blocks [13].

### 3.2 Blockchain Characteristics

Since all blocks are time-stamped and cryptographically connected to the previous block, it is impossible to retroactively alter previous transactions without alteration of all subsequent blocks in the chain. This chained structure of the blockchain and the collective computational power of the network make it therefore a generally immutable and tamper-proof technology [14].

Another important aspect of the blockchain is its distributed nature. The complete blockchain is a database file, which is replicated between all nodes on the network so that every node shares the same data. These networked copies create decentralization and shared responsibility. Since the classic blockchain is a shared open database of linked blocks, it provides a view of the full transaction history to all nodes. Any member can access it and see the available transactions. This creates traceability of assets over their lifetimes.

### 3.3 Blockchain Structures

Blockchains can be set up in different ways. The structure depends on their intended application [4, 15]. Generally, a *public blockchain* is open, decentralized, and fully visible to the public. It is not owned by a single entity, but any node can join or leave the blockchain. Any participant can also verify and add data to the blockchain.

A *private blockchain* is controlled by a centralized entity. Only nodes that are authenticated and permitted can join the network. The same applies to adding records to the blockchain and verifying them. Private blockchains do not offer the same decentralized security as public blockchains, which is why entries can be more easily altered by their owner.

In a *consortium* or *hybrid blockchain*, different stakeholders (e.g., suppliers, governments, regulators, producers, processors, retailers, etc.) build a group (a consortium) and operate the blockchain together. Interactions are performed within a limited group of entities that share a common goal. The validation process is often controlled by known, trusted users. The database of the blockchain is only distributed among entitled participants, which makes the network only partly decentralized.

## 4 Proposing a Framework for Cannabis Authenticity based on Blockchain technology

### 4.1 Blockchain Implementation

Hybrid blockchains are entirely customizable, as they allow granting special permissions to each participant of the network, such as reading, accessing, or writing information. This way, it is possible to control each participant's activities depending on their role. In the cannabis supply chain, the grower cultivates the plant, the processor manufactures the final product, laboratories test the product for various specifications (e.g., for fungal growth or THC amounts), distributors ship the product, customs authorities clear the product for entrance to their respective nation, and retailers sell the product. Each party plays a vital but specific role in the supply chain, so that a hybrid blockchain may offer the best fit.

Once, the blockchain technology has been implemented in the supply chain, each supply chain member represents a node in the blockchain and is known by the other participants. Depending on their permissions, each node can add product-related information to the blockchain. This can be location information, time, or any other product details as weight or volume. As scalability is an issue for blockchains, big data files should not be put directly on the chain, but off-chain in a separate repository. The only information stored on the ledger for such data can be a cryptographic token, which contains the data reference and a pointer to the off-chain data. With this approach, the ledger can then provide access authorization to members who need access to the data.

### 4.2 Linking Data to the Physical Product

While blockchains enable greater transparency and data integrity, they cannot ensure data accuracy and correct data entry [e.g., 8]. Data still can get collected on paper or in a spreadsheet and then be manually entered into a blockchain. Therefore, supplementary technologies are needed to ensure the proper linking of information about physical goods to the data stored on the blockchain.

First, a standard for product identification needs to be set up. The GS1 standardization is a potential solution, which provides systematic coding of the Global Location Number for all companies and their locations in the supply chain and their Global Trade Item Number (GTIN) for products [cf. 16]. Each production batch and every packing unit could be assigned its own GTIN, which can then be uniquely referred to in the blockchain ledger.

As individual products get mixed, processed, or divided along the supply chain, single events of the product flow along the supply chain need to be captured. GS1 again provides a solution for this with their Electronic Product Code Information Services (EPCIS) system. Each event keeps a record of product IDs entering a process and the IDs at the output. This also allows the exact tracking of product-related information (e.g., weight or volume) entering and leaving at each process step. As this information is immutably stored on the blockchain, tracing of material addition or removal is facilitated, and easy to verify for any involved player.

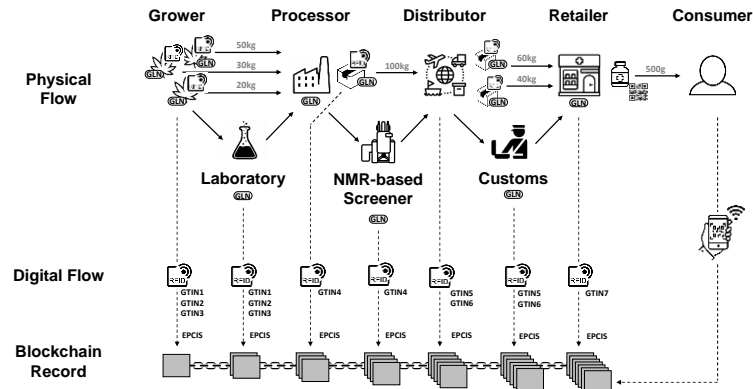
Next, to ensure that the product is always linked to the correct digital dataset on the blockchain, additional traceability systems need to be integrated. The GTIN can, for instance, be implemented as a barcode, QR code, or Electronic Product Code in a radio-frequency identification device (RFID). RFID is widely used for simplified digital tracking of products in supply chains and can be enhanced when integrated with blockchain [17]. Walmart and IBM together successfully use blockchain combined with RFID to track consumer products [18]. Using integrated NFC chips in the package, and an NFC reader (e.g., smartphone) makes it possible to directly read information about the product and authorize access to its traceability data stored in a blockchain. As NFC chips use unique identities, they cannot be copied as opposed to simple QR codes. IoT devices, which collect and enter data autonomously and automatically to the blockchain, can further enhance safety and build another level of trust in the product's supply chain [19].

Marking the product package, however, cannot guarantee that the *product* is untampered and original. For that, a promising approach is to integrate molecular screening technologies into the cannabis supply chain and put the molecular identity onto the blockchain ecosystem. For example, nuclear magnetic resonance-based (NMR) screening instruments could be installed between single supply chain participants as gateways that test the authenticity of the product and ensure it by being directly linked to the blockchain and automatically saving the test results onto the blockchain. To provide an example of such a technology, a suitable device is FoodScreener™ by Bruker Corporation, which allows testing origin authenticity, false labeling, and species purity among other factors [20]. Cannabis has—like humans—a unique molecular fingerprint. With reference to an original sample or a statistical model, the FoodScreener™ could detect inconsistencies in the molecular structure of the Cannabis. It would then indicate that the material or product has been altered and thus might have been subject to fraud.

Smart active devices locked to the physical product, accompanying it along the supply chain, offer an additional benefit that goes beyond mere protection. They can also monitor the product during idle states in warehouses or shelves for example. Active sensor devices can be placed in product containers, which record time, location, temperature, or other environmental parameters. Such devices can directly interact online with the blockchain, store data, and generate immediate alerts. They also allow communication about the content with the outside world without opening the package. Retailers and consumers immediately can detect whether a critical value (e.g., time or temperature) has been exceeded. A packaging label could change its color to indicate a cold chain interruption, a leaking package, or the unwanted presence of certain bacteria.

With the described standards and technologies in place (see Figure 3), the consumer or any other supply chain participant can easily back-trace products by using a unique product ID. The information gained can also help to improve the safety of products, as the collected environmental conditions are a source for deciding on the product quality. Adding location tracking enables to see instantly where a product currently is located or to identify at which GLN a potential recorded issue occurred.





**Fig. 3.** Blockchain-enabled Technological Supply Chain Framework for Product Authenticity.

## 5 Conclusion

The purpose of this study was to develop a technological framework to support product safety and authenticity in the cannabis supply chain. The supply chain transparency framework presented in this paper contains many technical elements, which combined provide powerful security against fraudsters and almost guarantee product integrity. Although such a framework with its numerous and detailed security elements remains a high aim, the technical foundation is available already today with the blockchain as a fundamental element.

The advantage of blockchain is that it can bring trust to a network of users through transparency and tamper-evidence. The distributed nature of the platform allows for greater oversight and control of products while real-time tracking via smart devices gives supply chain stakeholders the flexibility to make rapid decisions and update inventory levels continuously, thereby reducing working capital inactivity.

Despite the bright outlook, certain issues, such as interoperability of blockchains, remain and demand future research. Organizations that need to deal with several blockchains in different supply chains would highly benefit from the ability to see and access information across various blockchain systems.

## References

1. Ozawa, S. et al.: Prevalence and estimated economic burden of substandard and falsified medicines in low-and middle-income countries: a systematic review and meta-analysis, *JAMA Netw.* **1**(4), 1–22 (2018). <https://doi.org/10.1001/jamanetworkopen.2018.1662>
2. World Health Organization: Counterfeit medicines: the silent epidemic (2006). <https://www.who.int/mediacentre/news/releases/2006/pr09/en/>. Accessed March 5, 2021.
3. Food and Drug Administration: Sampling Study of the Current Cannabidiol Marketplace to Determine the Extent That Products are Mislabeled or Adulterated, Report to the U.S. House (2020). <https://hempindustrydaily.com/wp-content/uploads/2020/07/CBD-Marketplace->

- Sampling\_RTC\_FY20\_Final.pdf. Accessed March 5, 2021.
4. Babich, V., Hilary, G.: Distributed ledgers and operations: What operations management researchers should know about blockchain technology, *Manuf. Serv. Oper. Manag.* **22**(2), 223–240 (2020). <https://doi.org/10.1287/msom.2018.0752>
  5. Schmidt, C.G., Wagner, S.M.: Blockchain and supply chain relations: A transaction cost theory perspective, *J. Purch. Supply Manag.* **25**(4), 1–13 (2019). <https://doi.org/10.1016/j.pursup.2019.100552>
  6. Johnson, R.: Food fraud and economically motivated adulteration of food and food ingredients, Congressional Research Service (2014).
  7. Walker, M., Gowland, H.: Deadly fraud—Food allergen substitution in the food chain, *Clin. Transl. Allergy* **5**(3), 1 (2015). <https://doi.org/10.1186/2045-7022-5-s3-p137>
  8. McKenzie, J.: Why blockchain won't fix food safety—yet, (2018). <https://newfoodeconomy.org/blockchain-food-traceability-walmart-ibm/>. Accessed March 11, 2021
  9. Evans, D.G.: Medical Fraud, Mislabeling, Contamination: All Common in CBD Products, *Mo. Med.* **117**(5), 394–399 (2020).
  10. Food and Drug Administration: Statement from FDA Commissioner Scott Gottlieb, M.D., on signing of the Agriculture Improvement Act and the agency's regulation of products containing cannabis and cannabis-derived compounds (2018). <https://www.fda.gov/news-events/press-announcements/statement-fda-commissioner-scott-gottlieb-md-signing-agriculture-improvement-act-and-agencys>. Accessed March 5, 2021.
  11. Manning, L., Smith, R., Soon, J.M.: Developing an organizational typology of criminals in the meat supply chain, *Food Policy* **59**, 44–54 (2016). <https://doi.org/10.1016/j.foodpol.2015.12.003>
  12. Sarpong, S.: Traceability and supply chain complexity: confronting the issues and concerns, *Eur. Bus. Rev.* **26**(3), 271–284 (2014). <https://doi.org/10.1108/eb-09-2013-0113>
  13. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008). <https://bitcoin.org/bitcoin.pdf>. Accessed March 5, 2021.
  14. Queiroz, M.M., Telles, R., Bonilla, S.H.: Blockchain and supply chain management integration: a systematic review of the literature, *Supply Chain Manag. An Int. J.* **25**(2), 241–254 (2019). <https://doi.org/10.1108/scm-03-2018-0143>
  15. Mougayar, W.: The business blockchain: promise, practice, and application of the next internet technology. John Wiley & Sons, Hoboken (2016).
  16. Myhre, B., Netland, T.H., Vevle, G.: The footprint of food—a suggested traceability solution based on EPCIS, 5th Eur. Work. RFID Syst. Technol. 1–6 (2009).
  17. Sidorov, M., Ong, M.T., Sridharan, R.V., Nakamura, J., Ohmura, R., Khor, J.H.: Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains, *IEEE Access* **7**, 7273–7285 (2019). <https://doi.org/10.1109/access.2018.2890389>
  18. Reddy, V.P.V.: Emerging of Blockchain Technology in Business Industry, *Int. J. Innov. Res. Technol.* **6**(6), 227–230 (2019).
  19. Khare, A.A., Mittal, A.: Blockchain: Embedding Trust in Organic Products' Supply Chain, *J. Comput. Theor. Nanosci.* **16**(10), 4418–4424 (2019). <https://doi.org/10.1166/jctn.2019.8535>
  20. Bruker: NMR & EPR Food Analysis Solutions – FoodScreener. <https://www.bruker.com/en/products-and-solutions/mr/nmr-food-solutions/food-screener.html>. Accessed March 17, 2021.