

Article

Enhancing Food Supply Chain Security through the Use of Blockchain and TinyML

Vasileios Tsoukas ^{1,2,*}, Anargyros Gkogkidis ^{1,2,*}, Aikaterini Kampa ², Georgios Spathoulas ^{1,2,*} and Athanasios Kakarountas ^{1,2}

¹ Department of Computer Science and Biomedical Informatics, University of Thessaly, 35100 Lamia, Greece; kakarountas@uth.gr

² Intelligent Systems Laboratory, 35131 Lamia, Greece; kampakaterina@isl.dib.uth.gr

* Correspondence: vtsoukas@uth.gr (V.T.); agkogkidis@uth.gr (A.G.); gspathoulas@uth.gr (G.S.)

† These authors contributed equally to this work.

Abstract: Food safety is a fundamental right in modern societies. One of the most pressing problems nowadays is the provenance of food and food-related products that citizens consume, mainly due to several food scares and the globalization of food markets, which has resulted in food supply chains that extend beyond nations or even continent boundaries. Food supply networks are characterized by high complexity and a lack of openness. There is a critical requirement for applying novel techniques to verify and authenticate the origin, quality parameters, and transfer/storage details associated with food. This study portrays an end-to-end approach to enhance the security of the food supply chain and thus increase the trustfulness of the food industry. The system aims at increasing the transparency of food supply chain monitoring systems through securing all components that those consist of. A universal information monitoring scheme based on blockchain technology ensures the integrity of collected data, a self-sovereign identity approach for all supply chain actors ensures the minimization of single points of failure, and finally, a security mechanism, that is based on the use of TinyML's nascent technology, is embedded in monitoring devices to mitigate a significant portion of malicious behavior from actors in the supply chain.

Keywords: blockchain; food supply chain; transparency; traceability; smart contracts; internet of things; hardware; machine learning; TinyML; security; integrity



Citation: Tsoukas, V.; Gkogkidis, A.; Kampa, A.; Spathoulas, G.; Kakarountas, A. Enhancing food supply chain security through the use of blockchain and TinyML. *Information* **2022**, *13*, 213. <https://doi.org/10.3390/info13050213>

Academic Editor: Nelly Leligou

Received: 15 March 2022

Accepted: 18 April 2022

Published: 20 April 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Food safety is an essential and foundational right for customers. Despite several significant advancements in food science and safety, foodborne infections remain a serious public health concern around the world. The Centers for Disease Control and Prevention (CDC) reported that around 48 million people die due to contaminated food ingestion every year in the United States. As a result, 128,000 of them are hospitalized, and 3000 die [1].

According to research, the financial impact of foodborne diseases in the United States is estimated to be around \$55.5 billion [2]. This financial cost is incurred due to hospitalizations, decreased productivity, economic losses, and a variety of other factors. Additionally, these official estimates exclude other costs, such as the life-long health repercussions of foodborne infections. In January 2013, the discovery of horse DNA in frozen beef burgers attracted attention to the issue of meat adulteration [3]. Horsemeat is utilized in place of beef due to its lower cost of production. Table 1 presents various foodborne illness outbreaks that occurred around the world, as analyzed in the work of Gourama [4].

Table 1. Recent Foodborne Illness Outbreaks.

Date Occurred	Location	Foodborne Illness	Food Product	Cases	Deaths	Reference
2010	Texas	Listeriosis	Diced celery	10	5	[5]
2011	Germany	E. coli O104:H4	Sprout	3816	54	[6]
2011	USA	Listeriosis	Cantaloupe	147	33	[7]
2014	USA	Listeriosis	Mung bean sprouts	5	2	[8]
2014	Utah	Campylobacteriosis	Raw milk	99	0	[9]
2015	USA	Salmonellosis	Bean sprout	115	0	[10]
2019	USA	Salmonellosis	Pre-cut melons	137	0	[11]

Food safety and food security are connected concepts that have a significant impact on the quality of human life, and both of these areas are influenced by a variety of external circumstances. These concepts are of great importance for the health of consumers, and experts in various fields are constantly trying to cope with any challenges met across the food supply chain. New and emerging technologies such as Internet of Things (IoT), blockchain and tiny machine learning (TinyML) seem to be the tools capable of enhancing any expert attempts of ensuring the two complementing elements in consideration.

More precisely, food safety is a process that involves a variety of activities completed by people who come into contact with various forms of food at various development and operation stages throughout the world, in order to achieve a fixed food safety standard that meets both general and specific requirements. The potential problems associated with the world's population growth underlined the vital role of all actors in resolving food safety issues, including producers, distributors, consumers, government agencies, scientists, and medical experts. Food safety culture is mirrored in an organization's technological and managerial aspects, as well as in its personnel and working environments. Food safety should include a variety of management strategies, including the regular monitoring and surveillance of food production, in order to improve public health and avoid foodborne infections [12–14].

In contrast, the notion of food security ensures that everyone has access to appropriate, secure, and healthy food in order to maintain a healthy and active lifestyle. The determinants of IoT that facilitate data generation and collection, such as electronic control, smart contracts, policy enhancement, and the use of radiofrequency identification (RFID), are argued to be critical enablers for a motivated food security system, food safety, and environmental sustainability [15]. Food waste reduction and appropriate waste management mitigate the negative environmental impacts of food waste, preserve economic resources, and promote food security [16]. Blockchain technology is a promising approach for reducing food loss, increasing transparency, stakeholder confidence, and food security [16].

One of the most pressing problems nowadays is the provenance of the food and food-related items that people consume, owing to several food scares and the globalization of food markets, which has resulted in food movement between nations and continents. Food product documents and paper trails may have mistakes or even be faked by criminals, resulting in inaccurate or insufficient information on product labeling. For instance, Halal certification, Islamic values, and Halal food safety are among the most critical markers of a Halal sustainable food supply chain [12]. However, an innovative system for ensuring the "Halalness" of items, such as the Halal label, has recently lost the faith of Muslim customers due to a rash of food fraud instances [17]. Thus, establishing traceability and visibility via the use of proper methodologies is critical to fostering confidence among stakeholders [18].

Globalization has altered the food system, and consumer demographics and behavior are changing. A sizable segment of the population is aging or becoming immunocompromised. Consumers are requesting a greater variety of fresh fruits and vegetables, as well as minimally processed goods [19]. In Europe, people are ready to pay a premium for high-quality items that include information on the product's origin, species, and variety. Food scientists present a considerable difficulty in validating labeling compliance in a way that is acceptable to the whole food business and the customer [20]. The only way to overcome these obstacles is for stakeholders across the food system to be willing to experiment in new and innovative ways.

Furthermore, temperature [19] has always been an element that attracts great interest from researchers and food technologists because it demonstrates a wide variety of interactions between microbes and food matrices. The temperature significantly affects the growth and inactivation rates of pathogenic bacterial infections. Foodborne infections are generally mesophilic, flourishing between 20 and 45 °C.

For *B. cereus* spores, a slight temperature increase from 2 to 8 °C can result in a tremendous expansion of up to 10³ *B. cereus*/mL in around nine days [21]. This slight temperature increase may occur during the transportation of refrigerated goods and may also correspond with the temperature of commercial refrigerators. This is one of the first indications of why IoT devices must be utilized for temperature monitoring, and write this information to a system such as the blockchain. If a product is affected or partially affected by the spores in discussion, having this information is crucial for the recall process, since the product is not safe for consumption according to the European Commission regulation No 2073/2005 [22]

The cooling rates of various foods can be used to assess whether microbes require cold shock proteins or are able to adapt to changes in the microenvironment. Inadequate chilling periods can promote microbe development, particularly those whose spores survived the cooking process [23]. Spore-formers such as *Clostridium botulinum*, *Clostridium perfringens*, and *Bacillus cereus* can germinate and proliferate rapidly when foods are not properly chilled, resulting in foodborne disease [24].

Microorganisms' capacity to develop and survive within a food product is governed by the food's composition and environment, the processing parameters used, and the storage conditions used during the food's shelf life. The term "intrinsic factors" refers to the properties of the food matrix. In comparison, extrinsic variables are the characteristics of the surrounding environment, particularly during processing and storage. From the raw components to the finished product during storage, the food matrix and ambient circumstances undergo several changes, all of which may contribute to product development [25].

Some works [26–28] analyze the need for records to provide evidence to buyers and regulators that the product followed the correct procedures before reaching the customer. Other studies such as [29–31] discuss the significance of food traceability and how it may assist in solving food safety problems and enhance supply chain performance, particularly in terms of sustainability and customer transparency. Additionally, it is noted that, in order to retain public confidence, comprehensive and sustainable tracking and recall procedures must be built and maintained. This is now possible thanks to advancements in technology such as blockchain and IoT sensors.

Blockchain technology can be identified as a way to improve existing systems by boosting their transparency and traceability, hence regaining consumer trust. Blockchain technology may be used to construct food supply chain systems that are more transparent, traceable, and sustainable [32]. Distributed ledger technologies improve transparency and traceability in the agricultural sector's information flow. The technology possesses the following three major capabilities: The primary offerings are as follows: (a) ensuring the authenticity of the product by tracing its provenance and recording all transactions; (b) enabling secure, effortless, and real-time payments; and (c) facilitating better production and marketing decisions through accurate data monitoring and storage. Additionally, food

products would be traceable along the supply chain using the blockchain's unique IDs. Food waste may be prevented with information about growth conditions and expiration dates, and the immutable record of items and transactions can help avoid fraud and foodborne disease [33].

Moreover, blockchain technology may be used to enhance the following functions in food supply chains [34]:

- Track the flow of goods along with the supply chain
- Logistics tracking, e.g., orders, receipts, and shipping alerts
- Attributing certifications and characteristics to products
- Connecting items to their serial numbers or digital tags
- Sharing vital information across the product's assembly, distribution, and maintenance

As stated above, another important factor is the utilization of IoT devices for monitoring environmental or other critical factor metrics to ensure the quality of food products. However, these devices are not built with security mechanisms and are easy to exploit through the different communication protocols that they use to connect to third-party entities, such as other devices or the cloud. In order to be able to create an end-to-end system capable of providing unaltered information, scientists must come up with ways of securing them or developing new robust and resilient systems. Nowadays, typical IoT devices utilize several different kinds of sensors that are easy to be tempered from malicious actors. TinyML is an emerging technology that can operate in constrained hardware and provide intelligent results by running machine learning (ML) locally on edge. Additionally, since there is now the ability to run complex models locally, Anomaly detection systems can be developed to detect and report when abnormalities are discovered across the supply chain. These abnormalities could be a result of a spoiled food product, faulty machine operation, or attempts to tamper with monitoring devices.

Developing secure and robust systems for supporting critical operations, such as supply chain monitoring, is of crucial importance. The use of blockchain technology is one step forward in the right direction, as it ensures the security of the system upon which end nodes interact. The secure operation of the end nodes of the systems through the integration of proper security mechanisms is the second step we are required to take. It will ensure (to the extent that this is feasible) the normal operation of the end nodes and the validity of the data input for the system as a whole. Systems are as secure at their least secure node, and in order to develop fully secure systems, we need to improve security for all their parts. It is essential for the supply chain domain to provide both a secure blockchain-based backbone and a lightweight security mechanism for edge devices.

The contribution of the present paper is two-folded:

- It introduces a blockchain-based system that can be employed to store data across the food supply chain, from farm to grocery. The system ensures that data tampering is infeasible and delivers end-to-end transparency for all actors in the food supply chain.
- It proposes a security mechanism, based upon the emerging technology of TinyML, that can be integrated as a security control to the edge devices used for monitoring purposes. This mechanism is based on a lightweight anomaly detection approach for the monitored data and is capable of identifying cases where malicious actors attempt to exploit or tamper with the devices.

Combining these two complementary mechanisms increases the citizens' trust concerning data presented to them regarding consumed food products.

The rest of this paper is organized as follows. Section 2 presents previous work regarding blockchain-based systems utilized in the food sector. Section 3 provides a brief overview of the main requirements of the food industry. Section 4 describes the three distinct subdomains of the food industry, agriculture, livestock, and fishery. Section 5 introduces the Blockchain technology. Section 6 introduces the technology of TinyML, its main advantages and requirements, and TinyML-based systems regarding agriculture, machine failure prediction and device's security. Section 7 describes the overall concept, challenges and thoughts

behind the system proposed in this work Section 8 analyzes the blockchain-based system and Section 9 presents an example of a system capable of identifying anomalies regarding the monitoring devices required across the food supply chain. Finally, Section 10 concludes with an analytical overview and results from the experiments conducted and presents future plans. Figure 1 depicts the organization of the sections and the overall thoughts behind the paper. It starts with introducing challenges and issues met across the food supply chain, presents food industry's key components and subdomains, introduces the two emerging technologies from which the blockchain-based system and the anomaly detection device are inspired and then presents them and finally concludes with comprehensive analysis and presentation of the results.

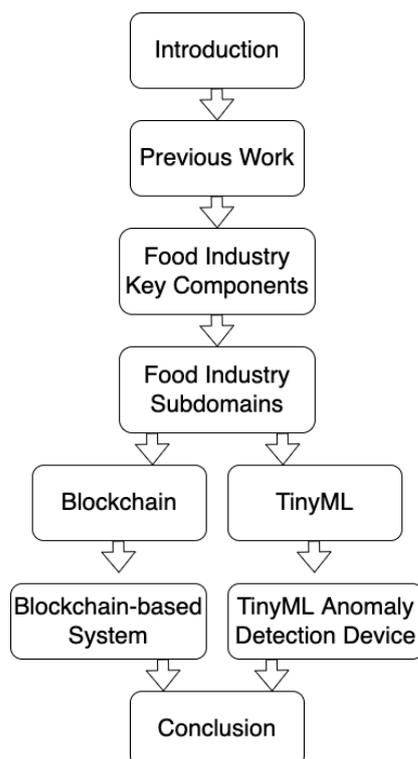


Figure 1. Sections' organization overview.

2. Related Work

According to the literature, the usage of blockchain technology in applications linked to quality assurance and transparency in the food sector has increased significantly in recent years. All of the efforts outlined are not mature enough or may not completely document how the blockchain is used, nor do they address specific issues or restrictions. Conversely, the sheer volume of scholarly publications over a short period reveals a definite trend toward integrating blockchain technology into existing food sector procedures. This trend is primarily due to the compatibility of the characteristics offered by blockchain systems with the issues confronting the particular industry. The following paragraphs provide an overview of various blockchain-based systems for the food supply chain.

To address China's rising food safety concern, a team presented a supply chain traceability system [35] built on blockchain and RFID (radio-frequency identification) technologies. The system can be used to collect data and manage information for all stakeholders, using a "from farm to fork" approach. The use of RFID tags, which are typically found on product packaging, enables the presentation of numerous agri-food product features to the consumer, such as the product's name, variety, origin, fertilization state, and pesticide usage. The system collects, circulates, and shares data using RFID technology, while blockchain technology ensures the integrity of shared information. The system is suggested to be applied to the primary food industry areas of fruits, vegetables, and meats.

The authors of work [36] provided an end-to-end solution for a blockchain-based agri-food supply chain. They have presented comprehensive details such as traceability and delivery regarding the cases explored on the proposed system in consideration. Additionally, they have thoroughly researched and evaluated the efficiency of smart contracts to ensure that the offered solution is both accurate and efficient. The reputation system is intended to sustain the agri-food supply chain's authenticity and product quality standards. Furthermore, since these transactions are based on blockchain technology, they maintain the immutability and authenticity of the transactions. The system in consideration requires a particular quantity of gas to deploy and execute smart contracts, as demonstrated by the simulations provided. Regarding authors' future plans, they intend to implement methods such as refunds into the trade of agri-food items. Moreover, since the reputation system archives reviews from end-users that may be skewed or fraudulent, an additional system capable of detecting fraudulent reviews is intended to be added.

Another team introduced KRanTi [37], a blockchain-based system for the Agriculture food supply chain (AFSC) to assist in resolving production tracking and efficiency issues, as well as making the system more resilient and transparent among users. The system makes use of Ethereum to track transactions between stakeholders and to ensure consistency by maintaining a record of the score granted to the former stakeholder. Additionally, KRanTi offers farmers a special credit-based program that enables them to build funds for superior agriculture-related items. The authors provide tests, compare, and analyze various information such as bandwidth, gas usage, and data storage cost. Additionally, some limitations are mentioned, mainly regarding the overall cost, and one of their plans is the implementation of an artificial intelligence (AI) system to forecast system abnormalities.

A research team was tasked with strengthening public trust in the food supply system. Authors built their system on cutting-edge technologies such as blockchain and IoT while taking the hazard analysis and critical control points (HACCP) methodical approach seriously. The system is based on BigchainDB, a distributed database system that resembles a blockchain, and utilizes a variety of sensor and networking technologies to efficiently gather and transfer the essential data. According to preset access control rules, all supply chain participants can interact with the system by adding, retrieving, or editing data stored in the database. RFID tags are used to label products, which are then immediately associated with a virtual identity. This permits the identification and retrieval of information about each product throughout its existence in the supply chain [38].

In this work [39], a unique architecture that leverages IoT and blockchain technologies to increase transparency throughout the food supply chain is presented. Each food product is assigned a unique identity via the use of an RFID tag. Each action associated with this particular shipment is logged to a blockchain system via sensors deployed at all crucial points across the supply chain, resulting in a tamper-proof digital history. Consumers and retailers can access the public ledger at any time to receive product information. All of this critical information can be used to update the shelf life and conduct targeted recalls. Although only one sensor was included in the suggested system, other sensors such as moisture and light sensors might be included depending on the packed food product. Additionally, the authors did a security analysis, which revealed that the validation of a fabricated block becomes even more challenging with a more significant number of nodes and numerous consensus stages, which can be enhanced by improving hardware security.

World Wide Fund for Nature, a non-profit organization, has embarked on a blockchain supply chain project to establish a transparent and traceable environment for the fresh and frozen tuna supply chains [40]. The pilot was explicitly designed for tuna captured in a longline fishery in Fiji. RFID and QR codes were utilized to collect data at various points along the supply chain. Each fish that lands on a fishing vessel can be traced by attaching a tag to the fish prior to its placement in the hold. This one-of-a-kind tag could be attached to the fish and automatically registered at several types of equipment located on the vessel, at the dock, and in the processing plant. Internet access was necessary to transmit and record the tagged fish data as digital assets on the blockchain. As fish are tagged, a dedicated

mobile application records vital data on a mobile device, which digitally certifies the record. Once internet connectivity is established, the software immediately uploads recorded data to the proper servers, where it is then stored in the blockchain. When fishers return to the port, each tagged piece of fish is checked and then delivered to a processing plant. The tag remains attached to the fish throughout the process to ensure the fish's history is not lost or altered.

Provenance [41] collaborated with fishermen to develop a "first-mile" registration system. The use of blockchain and smart monitoring to supervise the fishing activity of fishers who meet particular social sustainability requirements was pioneered. Fishers could issue their catch as a new blockchain asset via an SMS message. Each object is subsequently assigned a unique permanent ID. When tangible transactions between fishermen and retailers occur, they are also recorded in the blockchain. The item credited to the fishers is linked to the suppliers, and the prior owner's information is also maintained for backward tracing purposes. Additionally, Provenance presented applications for customers that enable them to obtain necessary information about the goods. Smart stickers equipped with NFC are employed, and when scanned, the consumer may assess the product's transaction history from the sea to the store. Additionally, item monitoring might be extended to dining establishments, informing patrons of accessible information about items and ingredients. Provenance's objective is to provide a solution for data interoperability and item tracking in a highly robust yet accessible format.

The work [42] presents a comprehensive concept of a blockchain-based agrifood supply chain traceability system in this, along with a prototype implementation. The implementation of blockchain technology reduces the requirement for supply chain participants to rely on a single organization needed to handle supply chain operations and preserve traceability data. Additionally, this fully distributed strategy eliminates the limitations of scalability as well as a single point of failure. The suggested solution enables the automation of supply chain management procedures and the secure and persistent storage of traceability information. Additionally, the ability to add rules at runtime enables the flexible development of product-specific quality control procedures. Ultimately, the system offers an overview of the many stages of harvesting, processing, and distribution through which quantities of product pass, allowing for the reconstruction of each batch's complete lifecycle and the acquisition of origin details.

Additionally, a blockchain-based system was proposed for tracing the origin of chicken products. The technique was deployed in Tien Giang province, Vietnam, on chicken farms. Numerous companies took part, including poultry farms, veterinary business agencies, and shops. The suggested system was written in PHP, and in addition to the usage of Blockchain technology, QR codes were included to allow consumers to search for information about chicken products stored in the system. Farmers and stakeholders were optimistic about participating in the experiment, and the early findings were encouraging [43].

The authors of the study [44] present FoodSQRBlock, a framework based on blockchain technology that digitizes food production data and makes it easily accessible, traceable, and verifiable by consumers and suppliers through the use of QR codes to integrate the information. Additionally, they used Google Cloud Platform to simulate a real-world food production scenario, employing milk and pumpkins as representations of products from real farms in the United Kingdom. Experiments demonstrate the practicality and scalability of implementing FoodSQRBlock in the cloud.

Additional blockchain-based systems for the food supply chain are discussed in the work [45], together with the subdomains into which they are incorporated, the degree of implementation, the blockchain system chosen, and the type of blockchain access. Table 2 showcases various blockchain-based systems proposed by the scientific community, among with the subdomain they are utilized in, the food industry requirements they are capable to enhance, and finally, their implemented technologies.

Table 2. Blockchain-based Systems.

Reference	Fishery	Livestock	Agriculture	Transparency	Traceability	Sustainability	Technologies
Tian et al. [35]			X	X	X		Blockchain, RFID
Shahid et al. [36]			X	X	X		Blockchain, IPFS
Patel et al. [37]			X	X	X		Blockchain, 5G network, IPFS
Tian [38]			X	X	X		Blockchain, IoT, RFID, BigchainDB
Mondal et al. [39]		X	X	X	X		Blockchain, RFID, IoT
WWF [40]	X			X	X	X	Blockchain, RFID, IPFS, NFC
Provenance [41]	X			X	X	X	Blockchain, NFC, QR-codes, RFID
Marchese et al. [42]			X	X	X		Blockchain
Huynh et al. [43]		X		X	X		Blockchain, QR-codes
Dey et al. [44]			X	X	X		Blockchain, QR-codes, Cloud

3. Food Supply Chain

The main requirements of the food industry as identified by the scientific community and the industry are traceability, transparency, and sustainability. Emerging technologies such as the IoT and blockchain could act as key actors regarding the aforementioned requirements. Food traceability may be aided by blockchain technology. While traditional methods of tracing invoices and shipping papers took several days, the adoption of blockchain-enabled it to be accomplished in a matter of seconds. Additionally, the technology has the potential to increase transparency throughout the food supply chain. This might be accomplished by printing information directly on the package and increasing customer transparency. Additionally, computerized recording and tracing systems may contribute to sustainability by minimizing food waste or by incorporating consumer-facing quality indicators such as working conditions or environmental needs [46]. A brief description of the requirements as stated above follows.

3.1. Traceability

Traceability is defined by the International Organization for Standardization in Codex Alimentarius as the ability to trace an entity's past, usage, or location using documented identifications [47].

Aung and Chang [48] proposed the essential properties and primary attributes that a traceability system must possess: first and foremost, the system must be capable of identifying any ingredient or component of the product; secondly, one of the most critical aspects is the accumulation of intelligence about the product's flow and transfer; and

thirdly, the system must be capable of determining which product is associated with which transfer. Salampasis et al. [49] presented the same parameters as above but added two additional criteria: cost efficiency and user-friendliness.

Agricultural traceability systems are critical for ensuring the safety of the food [50]. Since the European Union established regulations on food traceability, numerous platforms for implementing and supporting traceability in the food chains have been developed [51–53].

A comprehensive agriculture traceability system would include critical information regarding food ingredients, food sources, processing, distribution, storage conditions, and each component of the finished product. A traceability system is effective when it includes quantitative and qualitative data on the final food product and its source [54]. Additionally, the seafood sector has sought traceability for decades and has created and deployed many methods to track a product's transit through the supply chain in collaboration with regulatory bodies and non-governmental organizations (NGOs) [40]. The uses of traceability in the food supply chain have been extensively discussed in the literature [55–57].

Food traceability via blockchain is growing rapidly in the worldwide agrifood business. The potential to track food goods throughout their entire lifespan, from origin to every node along the way to the consumer, bolsters trust, efficiency, and safety. With a quick and simple QR code scan with their smartphone, consumers would be able to track any food product from “farm to fork”.

3.2. Transparency

Transparency is a hot topic these days, particularly among customers, as a result of outbreaks of foodborne illness, food adulteration, and fraud [32]. It refers to the communication and equal access of all stakeholders to all information and knowledge pertaining to the product in the absence of loss, blockage, or distortion [58,59]. Thus, transparency ensures that all product information is accessible to all stakeholders, including the customer, allowing for more informed judgments.

Transparency in the supply chain compels businesses to select how transparent they choose to be. Businesses must first obtain insight into their internal rules and regulations before increasing transparency for consumers and partners. This greater visibility may assist in mitigating supply chain risks to employees, the company's manufacturing skills, and ultimately customers. It is also critical for the subsequent phases of the growth of sustainable supply chains, which involve increasing information exchange, deeper collaboration with partners and competitors. To achieve meaningful and high levels of transparency, simple audits cannot be enough. Businesses are required to innovate and expand their toolkits by introducing new approaches. Technology investments and emerging technology implementations are not enough. To reap the full benefits of transparency, a mindset shift is required. It can start with teaching supply chain partners about the need for openness, the benefits regarding efficiency and collaboration, and the generation of new commercial possibilities capable of developing new market trends with safer food products [60]. There is great scientific interest in transparency with studies that also include the latest challenges such as the COVID-19 pandemic [61], fundamental changes [62], and reviews that connect transparency with sustainability [63].

Blockchain technology significantly improves the capacity to rapidly identify probable sources of contamination in order to effectively prevent, contain, and rectify epidemics. Transparency in terms of blockchain food traceability may help to confirming and identifying the origin of food, as well as increasing brand confidence. Additional benefits include fraud prevention and the capacity to more effectively address outbreaks through preventative measures that assist in reducing food testing costs and increasing margins [64].

3.3. Sustainability

Nearly 30% of total food production is wasted, which may be prevented with proper operations, resulting in a more sustainable environment with safer food and improved food waste prevention [65]. It is observed that public awareness of the environmental and health risks associated with food production and consumption has prompted the food sector to change its mindset and regulations by introducing safer and sustainable operations and technologies [66]. Only recently, the European Union [67] has announced the commencement of an initiative aimed at strengthening consumers' participation in establishing a more sustainable economy. All sectors must be concerned with sustainability and prioritize environmental stewardship, which encompasses all facets of sustainability: people, planet, and profit. This means that organizations have significant challenges justifying decisions on sustainability and resilience initiatives, practices, and policies that demand significant resources and effort [68]. To further complicate matters, the interruptions caused by COVID-19 forced enterprises to go beyond conventional environmental and social issues and handle supply chain perseverance of environmental, health, and economic difficulties [69,70]. Additionally, the existing food system suffers from an increase in food waste as a result of the growth in food services and delivery platforms, exacerbated by the COVID-19 pandemic's uncertainty, resulting in environmental impact [71]. To conclude, durable, non-hazardous materials must be used to construct products, and buyers must have access to information about the food's origins and the sustainability of the procedures utilized to produce and transport it [59,72]. Additional information is presented in the works of Rana et al. [73] and Hervani et al. [74].

4. Food Industry Sub-Domains

Food businesses can be categorized into three distinct subdomains; agriculture, livestock, and fishery.

4.1. Agriculture

Numerous methods of worldwide benchmark standards have been adopted by businesses, including GAP (good agricultural practice), GHP (good handling practice), GMP (good manufacturing practice), and HACCP. However, there are still several unresolved concerns with food quality and safety across the agrifood supply chain that might create severe problems [75]. There is a critical need to develop tight rules in conjunction with laws and trade agreements to ensure the safety of agricultural products. Although there are recognized traceability concerns with low-quality and inexpensive food commodities, a more severe issue is the inclusion of prohibited substances, spoilage, or even pathogenic bacteria in food. Another serious concern found by experts is intermediaries' opportunistic conduct. Intensive agricultural techniques, along with human's over use of phytochemicals, have resulted in a degradation of soil health. Due to the unabated use of herbicides, weed resistance developed, forcing farmers to use even more herbicides to combat it. As a result, an industry has developed around a genetically altered crop that poses a major threat to human health. Plant scientists are much concerned with the frequent use of toxic herbicides and the continuous application of pesticides that resulted in the deposition of chemical residues inside fruits, vegetables, and crops. Toxic residues impact the nutritional quality, taste, shelf time of fruits, vegetables, or crops. After consumption, some of the pesticides, especially chlorine derivatives, get accumulated inside fat tissues and severally affect the food chain and, of course, human health and the environment. EU residents are expressing a preference for organic foods. Eurostat [76] issued a survey in 2005 revealing that about 4% of total agricultural land in the EU-25 was dedicated to organic food production, with the most considerable proportions in Austria (11%), Italy (8.4%), the Czech Republic, and Greece (both 7.2 percent). This led to an increase in the manufacturing of organic foods in order to meet the increased demand. The components used in organic goods are subject to several controls and requirements. Even with these constraints, compliance with genuine

standards is still contingent on the integrity of human actors. Figure 2 depicts the market shares of specific organic food products in different European countries [77].

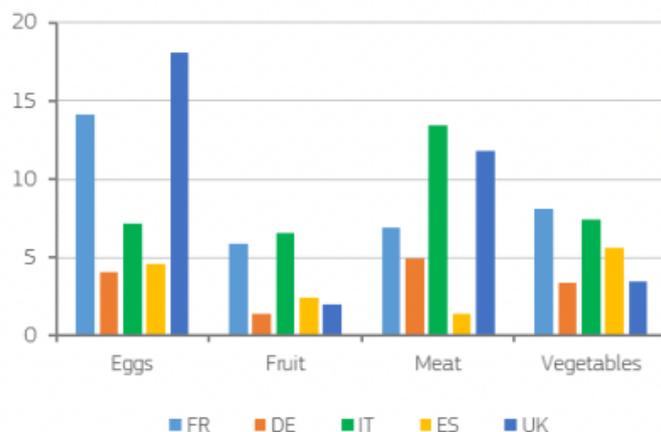


Figure 2. Growth in organic retail sales in volume, annual growth rate 2012–2017 (%). Source: Euromonitor International (2017), Fresh Food 2017.

4.2. Livestock

In 2013, claims surfaced in Europe of meat adulteration goods, including horse DNA discovered in frozen beef burgers [3]. Consumers have a strong desire for assurances about the quality and safety of farmed animal products. This expanding requirement is essentially a result of the frequency with which food safety incidents and cases are extensively publicized. Animal health and food safety are inextricably linked, with any danger to or adjustment of animal health having an effect on food safety [78]. Environmental contaminants, and some pathogenic microbes can infect animals, posing a danger to human health through meat and other products from such animals. On the other hand, agricultural techniques that allow for pasture-based ruminant feeding have a favorable brand image. Pasture feeding promotes animal well-being and adds value to the final product. This is another reason why building an authentication system capable of authenticating the animals' diets is critical. In conclusion, verification of livestock is also necessary for the species' origin, production technique, and processing technologies [79]. Traceable records are a requirement under European regulation 178/2002 for all food-related enterprises. As with any document, the aforementioned documents are easily forged. This demonstrates the crucial necessity for the development of new solid ways for securing the critical information transmitted via the paper-based traceability system. Additionally, the diet and feedstuffs ingested by animals have an effect on the quality of animal-derived meals. It is self-evident that there is a critical need for developing new analytical methods for characterizing foodstuffs, which will ultimately result in the authentication of the activities involved in feeding animals [79].

4.3. Fishery

The consumption of seafood products has risen dramatically over the last fifty years. Additionally, fish and fishery products were among the world's most traded food commodities in 2012. These products account for 10% of agricultural output and 1% of the global commercial trade-in value. According to "The State of World Fisheries and Aquaculture" [80], a research conducted by Food and Agriculture Organization (FAO), total fisheries product output reached a peak of around 179 million metric tons in 2018. The majority of those products were consumed by humans, and a small portion of them was utilized to make fishmeal and fish oil. Seafood items are part of a complicated supply chain system that frequently crosses several national boundaries, including movements into areas with lax or non-existent traceability standards. Around 50% of traded fish captures are processed (i.e., fillets and parts), removing their physical traits and making identification

more difficult. Mislabeling has also been found as a significant factor in the reduction of fish [79]. According to pertinent research, up to 50% of fisheries goods are mislabeled in restaurants and retailers [81,82]. Additionally, contamination and other issues such as inadequate conservation conditions or excessive storage time at the source or throughout the commercial value chain can occur with fish products both for capture and aquaculture. The traceability of the fishing and aquaculture company value chain enables the identification of problematic product lots and could help with the procedure of recalling [50].

4.4. General Remarks

The ability of microorganisms to grow and live within a food product is determined by the content and environment of the food, the processing parameters employed, and the storage circumstances utilized during the food's shelf life. The phrase "intrinsic factors" refers to the food matrix's features. Extrinsic variables refer to the properties of the immediate surroundings, particularly during processing and storage. The food matrix and ambient conditions undergo several changes during storage, all of which may contribute to product development. The parameters in consideration are pH, Water Activity, Eh, Antimicrobial Components, Biological Structures, Temperature, Relative Humidity, Gaseous Environment, Presence of Other Microorganisms, Stress Adaptation and Sub-lethal Injury [25]. To determine whether any of these features has an effect on product development, several types of sensors must be deployed and exploited across the supply chain. It is not possible to obtain measurements for each of the parameters listed above using sensors. We discovered that by exploring the market for various types of sensors, we can obtain data for Water Activity, Temperature, Relative Humidity, and Gaseous Environment. These readings would be examined and the necessary actors would be notified. They may then be further processed using ML techniques and integrated into the blockchain system. Table 3 showcases the two general European Commission Regulations regarding Agriculture, Livestock and Fishery across the food supply chain.

Table 3. General European Regulations regarding Agriculture, Livestock and Fishery.

Agriculture	Livestock	Fishery	Reference	Regulation
X	X	X	ANNEX I [83]	(EC) No 852/2004
	X	X	ANNEX II [84]	(EC) No 853/2004
	X		ANNEX III CHAPTER I–VI, IX–XIII [84]	(EC) No 853/2004
		X	ANNEX III CHAPTER VII–VIII [84]	(EC) No 853/2004
	X	X	ANNEX III CHAPTER XIV–XV [84]	(EC) No 853/2004

5. Blockchain

Blockchain is an approach for setting up decentralized systems that are based on a consensus process that enables the trustful exchange of data between entities [85]. According to the fundamental concept, such systems are public, which means that anybody may interact with those by submitting a transaction or viewing past ones. Because the data stored on blockchain systems are immutable, at least according to the design, such systems are employed in cases where the authenticity of the information shared across all nodes is required. The primary advantage of the technology is that it eliminates the need for a trusted third party, which is required in the majority of client-server-based systems. Centralized systems are also susceptible to the single point of failure effect, as a failure of the central nodes may result in the system's complete availability. Additionally, centralized

systems are vulnerable to malevolent activity by individuals who control central nodes, such as fraud, corruption, data manipulation, and information fabrication [86].

Blockchain systems can be categorized regarding the mechanisms utilized to operate. A short overview of the three different blockchain variants follows:

- Public blockchain systems are based on a completely decentralized ledger system that is not restricted in any way. Users have the ability to do mining, examine records, and validate transactions. The system’s primary advantages are high security, openness and transparency.
- Private blockchain systems present an alternative approach where a secure network is set-up and only qualified users are allowed to connect. It is far smaller than a public blockchain network, it bases its security on the assumption of the proper behavior of the majority of the nodes and that results in faster transactions times.
- Hybrid blockchain is a blend of public and private blockchains that makes use of their primary characteristics, in order to offer a solution for cases in which non public or private blockchain systems provide a satisfactory solution.

Table 4 briefly presents advantages and disadvantages of the Blockchain technology as analyzed in the works of Banerjee et al. [87] and Torossi et al. [88].

Table 4. Blockchain’s Pros and Cons.

Advantages	Disadvantages
No requirement for human operators to maintain and operate the transactions.	Blockchains must work and communicate with other ERP blockchain systems.
Impossible to alter data that has been recorded.	A blockchain database must store data indefinitely. This unrestricted storage of data results in high cost.
Data is available publicly	Data are validated by miners. There is a required time before data are available
Certification of the tamper-proof storage of large volumes of data is allowed.	No global regulatory framework for blockchain.

5.1. Smart Contracts

A smart contract is a self-executing contract in which the terms of the buyer–seller agreement are written directly into lines of code. The code, as well as the agreements it contains, are distributed across a decentralized blockchain network. Transactions are trackable and irreversible, and the code controls their execution.

Simple logical statements are written into code on a blockchain to make smart contracts work. When predetermined conditions are met and verified, the actions are carried out by a network of computers. These actions could include but are not limited to transferring funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. When the transaction is complete, the blockchain is updated. This means that the transaction cannot be changed, and the results are only visible to those granted permission.

There can be as many stipulations as needed in a smart contract to satisfy the participants that the task will be completed satisfactorily. Participants must agree on how transactions and data are represented on the blockchain, as well as the rules that will govern the terms.

A brief description of the main advantages of the exploitation of smart contacts follows:

- Speed, efficiency, and accuracy—When a condition is met, the contract is immediately executed. Because smart contracts are digital and automated, there is no paperwork to deal with and no time wasted correcting errors that can occur when filling out documents by hand.

- Trust and transparency—There is no need to worry about information being tampered with for personal gain because no third party is involved, and encrypted transaction records are shared among participants.
- Security—Due to the fact that blockchain transaction records are encrypted, they are extremely difficult to hack. Furthermore, because each record on a distributed ledger is linked to the previous and subsequent records, hackers would have to change the entire chain to change a single record.

5.2. Blockchain Benefits in Food Supply Chain

The ability of blockchain to track ownership records and resist tampering can be used to address urgent issues in the current food system, such as food fraud, safety recalls, supply chain inefficiency, and food traceability. Blockchain can help bring transparency to the supply chain by making the data collected at each step accessible to everyone in the network. Everything about a food item can be recorded on the blockchain, from production to sale, to eliminate food fraud and recalls.

Food traceability has been a hot topic in the past years, especially in light of recent advancements in blockchain technology. Because of the concept of transient food, the food industry is vulnerable when it comes to making mistakes that could potentially impact human lives negatively. When foodborne infections threaten overall health, the first step in determining the main driver is to locate the source of contamination, as there is no capacity to bear vulnerability.

As a result, food supply chain traceability is critical. Because some involved parties are still tracking information on paper, the current communication framework within the food ecosystem makes traceability a time-consuming task. The structure of blockchain ensures that each actor in the food value chain generates and securely shares data points, resulting in a system that is both accountable and traceable. Large amounts of data with labels that clarify ownership can be recorded quickly and without changes. As a result, the entire journey of a food item from farm to table can be tracked in real-time.

Furthermore, blockchain can be utilized to increase the efficiency of transactions in the food supply chain. It could eliminate inaccuracies caused by traditional paper-based records by preserving every digital record of the transaction. In the event of a food recall or investigation, the process could be completed quickly and efficiently thanks to blockchain's end-to-end traceability. Also, moving the data very quickly is conceivable. When the information is validated, it is reproduced in different nodes of the network to deal with its security.

6. The Technology of TinyML

TinyML, a new technology that is the result of all the efforts and research conducted over the last decades from the scientific community to reduce the size of ML and Deep Learning (DL) algorithms, and bring machine intelligence to constrained hardware. A system that utilizes TinyML is a low-cost, highly efficient device, capable of running complicated models locally and extracting intelligent results in real-time without the need of connecting to external entities.

TinyML is a very rapidly evolving field that is attracting the attention of researchers. The technology makes use of methodical hardware and software design to enable the deployment of ML models and DL networks on constrained resource devices. By using this new domain, developers could build new services and solutions that do not require complex technology and address common challenges associated with IoT devices, such as latency and bandwidth constraints. Devices connected to the Internet of Things will be used to collect, assess, and extract data. Because this information is not shared with other entities, the devices are more secure and unaffected by known malicious network attacks, such as distributed denial-of-service (DDoS) and rogue access point attacks.

Furthermore, the technology required to perform the tasks, microcontrollers (MCUs), is claimed to be extremely energy efficient and low-power. It is often less than a milliwatt

in power consumption and is capable of delivering intelligence in a brief period of time. TinyML may be the field capable of building and designing new devices that operate as a safeguard and enhance an application's or other device's security mechanism. In our test example, a food supply chain, TinyML might deliver unique insights particular to each use case rather than relying on hash functions, predefined thresholds, and simple program logic that could ultimately disclose the anomalous or malicious activity. Notifying the proper actor of a possible machine failure, machine misuse, firmware modification, or change in environmental measurements is vital, and delay or communication disruptions are not tolerated. These gadgets will analyze and alert in real-time across the supply chain without requiring data transfer, enabling a new age of autonomous devices powered entirely by batteries while running complex neural networks (NNs) locally.

6.1. Optimization and Compression Methods

Neural networks contain a large number of parameters with high redundancy inside the models, requiring more computing power and memory than required, a power that is available from high-end graphics processing units (GPUs) or the cloud. As mentioned before, the technology into consideration is utilized for fitting machine learning models and NNs onto low-energy hardware with limited computational resources. The models must be optimized and compressed to enable the aforementioned model inference.

The most common methods utilized for compressing ML models are quantization and pruning. An alternative solution is the exploitation of all in one solutions, frameworks, that are utilized for model training, optimization and MCU deployment. A brief description of the techniques used for optimization follows:

- Quantization is the process by which network variables that are generally stored in 32-bit representations are transformed to 8-bit or lower representations in order to fit on restricted hardware. Associated work on this approach may be found in [89–91].
- Pruning is a strategy in which researchers aim to eliminate connections or neurons that are not critical to the final outcome. This is performed by excluding individuals whose weights fall below a predetermined threshold [92,93].
- Frameworks may be described as a comprehensive solution that can be used not just for model compression but also for training and deployment. TensorFlow Lite for Microcontrollers [94] and Edge Impulse's online platform [95] are two of the most popular options that function differently, as the former requires coding knowledge while the latter is more user-friendly and available as a web application.

6.2. Related Work

The scientific community has already offered several TinyML-based solutions in domains such as healthcare [96–98] and automotive [99–101]. Given that this article discusses developing methods for enhancing food supply chain security, solutions related to agricultural and machine security are briefly discussed.

6.2.1. Agriculture

The paper [102] describes the design of sparse, deep tiny neural networks (DTNNs) and their automatic conversion to an STM32 microcontroller-optimized C-library using the X-CUBE-AI toolchain. The experiments proved that it is possible to deploy a DTNN for atmospheric pressure forecasting in an economical and cost-effective system with a FLASH and RAM occupancy of 45.5 KByte and 480 Byte, respectively. Finally, the system was implemented in a real-world setting, achieving the same prediction quality as a cloud-based deep neural network (DNN) model, but with the benefit of processing all relevant data local to environmental sensors, eliminating raw data transmission to the cloud.

With the increasing complexity of applications and the incorporation of ML and AI techniques into the software development lifecycle, according to the authors of work [103] Azure DevOps is the most critical framework that many organizations are rapidly adopting to reduce the cost of product development and improve customer success. As part of

their work, they presented a unique DevOps framework for developing intelligent TinyML dairy agricultural sensors and the benefits of DevOps in developing high-quality products cost-effectively and serving small-scale farmers.

Another team [104] investigated the possibility of developing a framework for deploying artificial intelligence models in constrained compute environments that would enable remote rural areas and small farmers to participate in the data revolution, contribute to the digital economy, and empower the world through data in order to create a sustainable food supply for our collective future. This work suggested the possibility of democratizing AI for everyone in order to assist and help with the establishment of a sustainable food future.

6.2.2. Machine Failure Prediction and Security

When produced components of industrial machinery fail in the field, the consequences might be severe. Rather than incurring maintenance and replacement costs, an anomaly detection AI may be used to continuously check machine health and alert operators to any malfunctions. This enables the detection of abnormalities prior to their being serious enough to warn machine operators or resulting in a full system breakdown. Work [105] investigates machine learning on an embedded device in order to identify abnormalities using advanced low-power neural networks in this thesis. The authors leverage the cutting-edge TinyML framework to facilitate the creation and deployment of Edge AI. Deep learning can now be performed on the same low-power computer systems that collect sensor data in the field using TinyML. Using a battery-powered embedded device with no network connection, they used this deep learning technique to identify physical abnormalities as they occur. For their experiments a Kenmore top-load washing machine equipped with an Arduino Nano 33BLE development board was tested. The authors exploited the accelerometer sensor on the Arduino to capture normal data from a balanced laundry load and abnormal data from an unbalanced laundry load while they are washed in the machine. Afterwards, two alternative neural network models using normal data were trained: autoencoder and variational autoencoder. These neural networks are used to identify accelerometer irregularities such as imbalanced washer loads. After developing the model, it was inferenced onto the Arduino Nano 33BLE board using TensorFlow Lite. Using the autoencoder approach, the board identifies and signals imbalanced washing machine loads with 92 percent accuracy, 90 percent precision, and 99 percent recall. Finally, according to the authors the TinyML anomaly detector with autoencoder model has a battery life of 20 h when powered by 5 V lithium batteries.

Due to limited computing capabilities and the inapplicability of standard security protocols, both wired and wireless communication channels used by IoT devices face significant security difficulties and challenges in the evolving cyber security landscape. The work [106] discusses numerous security difficulties and challenges, as well as layer-by-layer security procedures that are applicable to IoT devices. Additionally, the author developed a TinyML framework based on the Tensorflow module that is integrated with the CTI platform for predicting potential threat propagation to smart devices using a Naive Bayes supervised machine learning classifier. The final solution predicts threat with an accuracy of 96.8 percent and 96.3 percent for the training and test datasets, respectively.

7. Concept

In the present paper, we propose an end-to-end approach that can significantly increase the security of the supply chain monitoring systems and, consequently, render those more trustworthy for the end consumer. Modern food supply chain systems tend to be complex and consist of more than one information system (controlled by different entities) that lacks compatibility and trust guarantees. The challenge of designing a global system that will be trusted by all entities across the supply chain and present to the consumer information about food products in the most secure way is the basis of the presented system has been designed. The main axes along which the system was designed are:

- Most of the human actors in the supply chain must control their identity and be responsible for the data input they provide to the system. This will reduce the capability of any actor to report fake data to the system, as it will be required for several other actors to collude with him to achieve that.
- It is of high significance that information stored in the system is immutable. In such a large industry is highly probable that someone may attempt to tamper with data to maximize financial gains, even if that would trigger food safety complications. The presented system can be deployed to any ethereum virtual machine (EVM) compatible blockchain network and provides the required integrity guarantees for data produced along the path of the food supply chain.
- A vital part of the supply chain monitoring systems is a network of monitoring devices deployed along the supply chain and collect data about the process or the food ingredients/products. Those devices are highly correlated with an attack vector related to improper handling of those, either by mistake or intentionally. As part of this work, we present that it is currently feasible to equip such devices with anomaly detection security mechanisms that can make them more robust and resilient to improper handling.

In Section 8, we present the blockchain-based system that enables the secure information storage and handling of food supply chain-related data. In Section 9, we provide a proof of concept implementation to highlight that it is feasible to integrate anomaly detection mechanisms into monitoring devices to increase their security.

8. Blockchain Based System

The concept is based on the idea of representing food ingredients as tokens. A new token is minted for any new batch of ingredient that is produced. The ownership of such tokens is closely monitored and recorded. Apart from token transfers, the system allows for token splits and token packaging into a final food product.

Let's assume that we aim at monitoring a food supply chain based on agricultural products. In the proposed scenario, five main actors may be identified. First of all, is the farmer, who has the ability to create a token, where a token represents an ingredient in the real world. After the production, the ingredients have to move to the factory. Therefore, another actor responsible for the transportation is present. During the transportation, the farmer has to transfer the token, and the transport actor has to receive the token. Then, when it is delivered to the factory, again the same process occurs, where the transport actor transfers the token to the factory and the factory receives it. The last actor on this chain is the grocery store, where again, has to receive the final product, which is a collection of tokens in our system. The final user of this system, which is not related to the above chain, but can and has to be able to view it, is the consumer. The consumer, by using the mobile phone, can scan a QR code on the final product, which will create a view of all the transactions and the actors involved from the farmer to the grocery store. The entire process is depicted in Figure 3.

All of the above actors and actions are described in the following paragraphs, where an overview of the backend and the interface of the proposed system are analyzed.

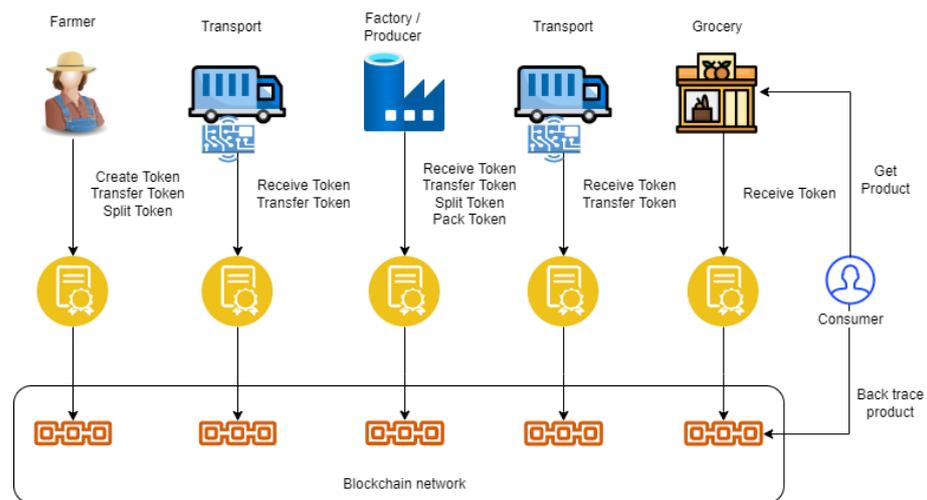


Figure 3. System actors and smart contract interaction.

8.1. Smart Contracts

The core of the system consists of two smart contracts. The former is responsible for the governance of the users and the latter is responsible to maintain all the information on the chain. The first contract, acts as the supervisor and handles the access rights and the administrative roles, for each user on the system. It actually connect the address of the user with his rights. The administrator, can set and update for each user the access rights with regards to the following actions for each different ingredient:

- Mint: with this access right, each user has the right to create a token which represents an ingredient
- Transfer: allows user to transfer a token to other actors of the system
- Receive: it allows user to receive a token after the transfer has been invoked.
- Split: since a minted ingredient can have quantity on it, there are cases, where the user will have to transfer or use a portion of it, thus using split can create a new token with different quantity
- Pack: lock the tokens that participate in the creation of a final product. For example a fruit salad, containing apples and strawberries, could be a final product, where apples and strawberries are the minted tokens.

The core of the system consists of two smart contracts. The former is responsible for the governance of the users, and the latter is responsible for maintaining all the information on the chain. The first contract acts as the supervisor and handles the access rights and the administrative roles for each user on the system. It actually connects the address of the user with his rights. The administrator can set and update each user's access rights with regard to the following actions for each different ingredient:

- Mint: with this access right, each user has the right to create a token that represents an ingredient
- Transfer: allows the user to transfer a token to other actors of the system
- Receive: it allows the user to receive a token after the transfer has been invoked.
- Split: since a minted ingredient can have quantity on it, there are cases where the user will have to transfer or use a portion of it; thus, using split can create a new token with a different quantity
- Pack: lock the tokens that participate in the creation of a final product. For example, a fruit salad containing apples and strawberries could be a final product, where apples and strawberries are the minted tokens.

The second contract implements the actions mentioned above and is responsible for tracking and maintaining all the data and the changes in the system. There are two primary data structures; the first describes all the properties of a token (ingredient), for example, the

quantity, the owner, and the current holder; the second holds all the necessary attributes to maintain the information of the final food products. Furthermore, the implementation of this smart contract utilizes the functionality of mapping to keep the relations between the minted ingredients and the users who used to own them. Thus, the implementation of the functions required is the following. For each action, there is a private function to check the user access rights based on the management contract and contains the software logic required for this action. On the other hand, a public function is exposed to the blockchain network, which can be called and perform the proper actions by using the necessary private functions.

A token is minted by calling the mint token function, which takes two arguments, the ingredient ID and the quantity. Given that the account calling the function possesses the corresponding permissions, the token is created, while the auxiliary mapping that holds data about token ownership is updated.

A second action is the ability to exchange tokens between the users. In order to achieve this, the user has to call the transfer function, which will first check if the caller has the access rights to transfer a token, and if the receiver has the access rights to receive that token. If all the checks are validated, the transfer happens, and the aforementioned mapping is updated with the new changes. The final step in this action is the receiving process, which again checks if the user can receive a token, and if this is true, the mappings are therefore updated with the changes.

Another functionality required in the system is the ability to split tokens to create portions of them. Hence, the split function is responsible do that. It has two arguments, the token ID and the quantity. Again, there is the process of validating the user's access rights and the ability to split the token based on the requested new quantity. The result of this function is the generation of a new token with the requested quantity, which is inserted in the mapping. The master token of subtracting the quantity is updated with the new remaining quantity.

The most crucial action in this contract is the pack function, which combines the requested tokens in order to create the final product. Once this function is called and all the required checks are valid, the tokens are consumed, and a new data structure is created. This new structure contains the tokens that compose the product and the owner, which is the company that produces the end product in most cases. All these data are stored in a new mapping, and there is a new hash generated to represent that product.

Finally, another function, the view pack, has view access rights and can be executed by anyone on the network; it offers the functionality of tracing all activity regarding the tokens that constitute the final product, along with the users that made the actions. This is mainly to be used by the end-user, which is the consumer that will purchase the food product. In this way, the system can provide him full traceability for the product in a secure and trustful way.

8.2. Interacting with the System

In order to enable users to control their identity and interact with the system, it is required for them to manage a blockchain account (a pair of cryptographic keys along with an address) through the use of a wallet. During the tests that were conducted, Metamask [107–109] was used as a wallet to connect all the actors. Metamask is an open source software wallet, which supports many reference platforms, and is a versatile application since it can be used as a browser extension or through a mobile application.

In the following Figure 4, Metamask acts as the connector to the various components and actors, as the user interacts with the system by initializing a Web3 [110] object on the front-end. This object can then be used to access the smart contracts on the blockchain back-end. Whenever the user has to use a feature that will alter the state (information stored) of any of the contracts described in the previous section, Web3 will initialize a transaction, in which Metamask will use the user's private key to sign the transaction.

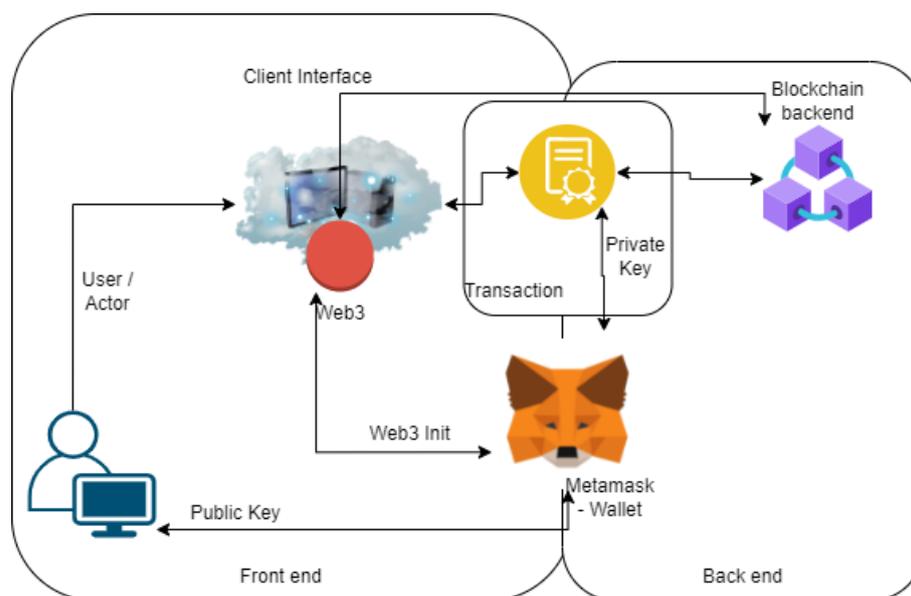


Figure 4. Schematic representation of the user interacting with the system.

9. Anomaly Detection Mechanism

The majority of security systems based on IoT devices cannot be recognized as smart solutions capable of identifying outliers tailored for specific use cases. Those systems are based on programming logic and are built with predefined thresholds that can have different results when utilized in unrelated environments. Additionally, the effort of having intelligence to conventional IoT devices seems to be high-priced, considering that the aforementioned devices only operate as a bridge to transport the information to the cloud, where the processing of data takes place. Tailored and quality results require machine learning algorithms and models, a procedure that due to its high computational cost, can only take place in the cloud and not in constrained hardware such as a typical IoT device. Despite the high operational costs, more challenges arise, such as the security issues when transmitting this data, bandwidth and latency issues for the extraction of the result, storage issues, and finally the requirement for internet collection or other communication protocols.

In the context of food supply chain monitoring systems, it is required to be able to detect the abnormal operation of IoT monitoring devices. In this Section we are presenting a series of experiments that aim at embedding anomaly detection capabilities in such devices. The anomaly detection-based system is proposed to be embedded in a device placed inside a truck refrigerator to measure temperature and humidity, in order to detect if the device is removed or placed in another location such as a portable fridge. The device itself must be trained during a number of trips and while the temperature is set as defined from ISO regulations for specific goods. The system will identify anomalies regarding environmental changes such as the temperature or if the track stops. It will then proceed on with labelling monitoring information as suspicious before being sent to the blockchain based system. A simple example to be given is if the driver decides to remove the device and place it in a fridge he found while delivering the goods to a customer. The reasoning behind this act is to lower the cooling capability of the freezer to reduce fuel costs. The sensors will identify the difference while monitoring temperature and humidity but will also recognize that there is no movement for an unusual period of time.

In the following paragraphs, a TinyML-based system is presented. The device, algorithms, and generally the methodology are subject to change, regarding different use cases, and are used as an example to showcase the feasibility of developing hardware capable of protecting the integrity of a system, like the one presented in this work.

9.1. The Device

A device suited for this purpose should meet a number of criteria. To begin, the most critical component is a development board that is entirely compatible with TinyML technology. Following that, the board must be configured to accept various types of sensors or have them pre-installed. Furthermore, the gadget must be capable of data transmission to the blockchain system. After conducting market research for existing solutions, we concluded that the Arduino Nano 33 BLE Sense development board [111] meets all of our requirements. The board is fully compatible with TinyML; it has all necessary sensors, including temperature, humidity, an accelerometer, and a gyroscope, as well as a communication chip capable of sending data to the blockchain. Furthermore, some additional information about the board can be provided as it is based on the Nordic Semiconductor nRF52840, which features a 64-MHz 32-bit ARM®Cortex™-M4 CPU, 256KB SRAM, 1MB of flash memory and operates at 3.3 V. All this in a form factor of 45×18 mm. Figure 5 depicts the anomaly detection device in a 3D-printed case.



Figure 5. The anomaly detection device.

9.2. The Dataset

It is necessary to generate a dataset of entries classified as normal data. To achieve this, the unit must be installed in the refrigerator of a truck and monitored throughout each journey using the same equipment. For our test case, we prepared a dataset using laboratory simulations. We simulated multiple such journeys over varying distances in order to obtain a range of timings and values.

9.3. Building the Model

Regarding the framework of our choice, we opted to employ Edge Impulse for model training and inference. Edge Impulse is a platform for embedding machine learning models into MCUs. It enables users to capture raw data from connected devices, analyze it, and upload it to the platform as a dataset.

The framework has pre-trained machine learning blocks that may be fully customized to meet the scope of the system. Additionally, the system provides a live testing operation guaranteeing that the model operates as expected while monitoring in real-time. Within the aforementioned structure, a new impulse was created and the time series data block was utilized for manipulating the data received.

Following that, the spectral analysis block was chosen due to its strong flexibility to sensor measurements of the parameters relevant to our use case. We also used the anomaly detection block which makes use of the K-means algorithm. Finally, the impulse was transformed to efficient source code that was prepared for deployment on the Arduino Nano 33 Sense.

9.4. System Evaluation

For the assessment of the model the False Negative (FNR) and False Positive rates (FPR) are calculated to understand the number of occasions the system failed to recognize an anomaly and the times that the system misinterpreted a normal value to an aberrant one. Additionally we utilized recall to quantify the proportion of anomalies found, precision to identify the number of anomalies that were indeed valid, and lastly F1 score to estimate the overall performance of the model. We evaluated our models independently for outliers identification in temperature, humidity and movement. For the temperature test scenario the trials revealed 11% FNR and 16% FPR. The evaluation measure of recall was 0.86, 0.88 for precision and 0.85 for the F1-Score. For the second scenario, regarding humidity, the model achieved 22% FNR and 7% FPR. The score of the evaluation metric of precision was 0.94, the score for recall was 0.77, and finally the F1-Score was 0.85. The final test case, where movement was tested, the model performed 13% FNR and 24%FPR. The evaluation metrics of precision was 0.81, recall 0.85 and F1-Score was 0.83. Figure 6 depicts a visualization of the trained and classified data, during a simulation test. The experiments demonstrated the feasibility of building a device capable of executing machine learning locally and integrating anomaly detection techniques into monitoring devices to improve their security. Further experiments in refrigeration trucks are planned in the future to assess the device’s overall performance in real-world scenarios. Table 5 showcases the experimental results for the three machine learning models, regarding temperature, humidity and movement.

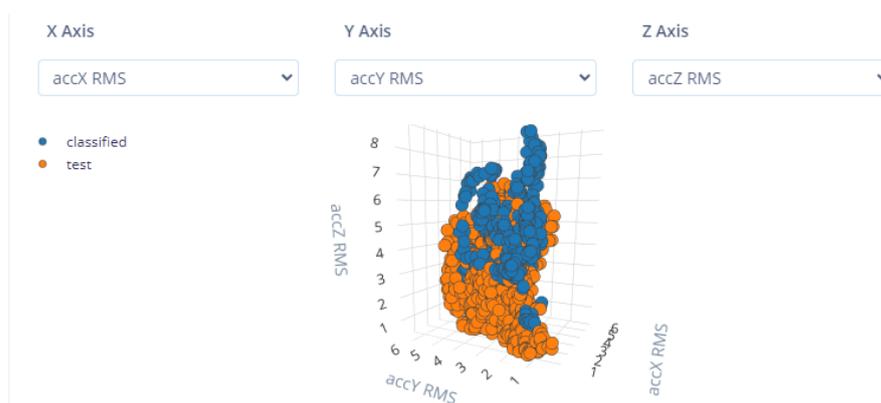


Figure 6. Visualization of trained and classified data.

Table 5. Simulation testing results

Test Case	False Negative Rate	False Positive Rate	Precision	Recall	F1-Score
Temperature	11%	16%	0.88	0.86	0.85
Humidity	22%	7%	0.94	0.77	0.85
Movement	13%	24%	0.81	0.85	0.83

10. Conclusions

One of the most important issues facing consumers today is the origin of the foods and food-related products they consume, as a consequence of many food scares and the globalization of food markets, which has led to food mobility across countries and continents. Complexity and a lack of transparency define food supply networks. Customers’ demands highlight the crucial need for creative approaches for validating and certifying food’s origin, characteristics, and information. This paper discusses an end-to-end approach to secure food supply chain systems and contributes to meeting regulatory standards for transparency and traceability.

The system is based on a blockchain-based back-end that ensures data integrity, automation of workflows, and interoperability between monitoring systems of different

vendors. A tokens-based scheme enables the detailed monitoring of food ingredients handling, transferring, or storing and allows for presenting such data for a specific food end product that reaches the consumer. Additionally, the prospect of developing a security system that utilizes TinyML's fledgling technology to function as a safeguard for monitoring devices is studied. This approach is capable of identifying anomalies that occur when malicious actors try to exploit or tamper with devices that are destined to report data to the aforementioned system. It has been proven that it is feasible to embed an anomaly detection mechanism into monitoring devices of limited resources with satisfactory accuracy results.

To our knowledge, this is one of the first efforts, if not the first, that integrates two emerging technologies, blockchain and TinyML, with the goal of increasing food safety across the food supply chain. This work contributes to two areas: the transparency and traceability of food goods, which are increasingly requested by customers today, and security, as the anomaly detection device works as a deterrent to malicious actors.

Regarding future work, it is expected to test the tokens scheme developed in a broader set of supply chain applications, apart from the agricultural food industry, to revise or extend it accordingly to serve the needs of other domains as well. As the data collected may be of high importance, supply chain actors may be reluctant to share those with the public. A more versatile approach to providing privacy protection features is going to be developed on top of the current scheme through which users will be able to control the access to the data they store in the system. We also plan to apply the TinyML anomaly detection feature to a real-world scenario, in which actors of the supply chain will attempt to use the monitoring devices in their favor to validate that the methodology is appropriate.

Currently, a proof of concept implementation of the presented system has been developed in a laboratory environment. The next step is to apply the proposed system in a more realistic setup in collaboration with the food industry. This will enable us to validate the functional requirements for the system better and also assess any performance issues that may come up in order to fine-tune the system.

The final phase is to evaluate the system through user studies conducted with invited actors. Some of the critical points that need to be extracted from those studies are the users' perceptions of the system's interface and overall usability, their thoughts on how the system improved key components of the food supply chain, such as traceability, transparency, and sustainability, their perspectives of the mobile application, and finally, their overall thoughts and propositions for new system additions.

The present paper has introduced a novel approach in order to ensure end-to-end security for food supply chain monitoring systems. It presents the combination of blockchain technology and TinyML to enhance food supply chain security. While we have presented the concept, the design, and a proof of concept implementation, there is much room for the further development and validation of the proposed system.

Author Contributions: This work was developed by the authors as follows: Conceptualization, A.K. (Aikaterini Kampa); Data curation, V.T. and A.G.; Funding acquisition, A.K. (Athanasios Kakarountas) and G.S.; Investigation, V.T., A.G. and A.K. (Aikaterini Kampa); Methodology, V.T. and A.G.; Project administration, G.S.; Resources, V.T., A.G. and A.K. (Aikaterini Kampa); Software, V.T. and A.G.; Supervision, G.S. and A.K. (Athanasios Kakarountas); Validation, V.T. and A.G.; Visualization, V.T. and A.G.; Writing—original draft, V.T., A.G. and G.S.; Writing—review and editing, V.T., A.G. and G.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work has received funding by the project "ParICT_CENG: Enhancing ICT research infrastructure in Central Greece to enable processing of Big data from sensor stream, multimedia content, and complex mathematical modeling and simulations" (MIS 5047244) which is implemented under the Action "Reinforcement of the Research and Innovation Infrastructure", funded by the Operational Programme "Competitiveness, Entrepreneurship and Innovation" (NSRF 2014–2020) and co-financed by Greece and the European Union (European Regional Development Fund).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CDC	Centers for Disease Control and Prevention
IoT	Internet of things
TinyML	Tiny Machine Learning
ML	Machine Learning
DL	Deep Learning
RFID	Radio-Frequency Identification
AFSC	Agriculture food supply chain
AI	Artificial Intelligence
HACCP	Hazard Analysis and Critical Control Points
NGOs	non-governmental organizations
GAP	good agricultural practice
GHP	good handling practice
GMP	good manufacturing practice
FAO	Food and Agriculture Organization
DDoS	Distributed Denial-of-Service
GPU	Graphics Processing Unit
MCUs	Microcontroller Units
NN	Neural Network
DTNNs	Deep Tiny Neural Networks
DNN	Deep Neural Network
EVM	Ethereum Virtual Machine
FNR	False Negative rate
FPR	False Positive rate

References

- Scallan, E.; Hoekstra, R.M.; Angulo, F.J.; Tauxe, R.V.; Widdowson, M.-A.; Roy, S.L.; Jones, J.L.; Griffin, P.M. Foodborne Illness Acquired in the United States—Major Pathogens. *Emerg. Infect. Dis.* **2011**, *17*, 7–15. [[CrossRef](#)]
- Scharff, R.L. State Estimates for the Annual Cost of Foodborne Illness. *J. Food Prot.* **2015**, *78*, 1064–1071. [[CrossRef](#)] [[PubMed](#)]
- Boyacı, İ.H.; Temiz, H.T.; Uysal, R.S.; Velioglu, H.M.; Yadegari, R.J.; Rishkan, M.M. A Novel Method for Discrimination of Beef and Horsemeat Using Raman Spectroscopy. *Food Chem.* **2014**, *148*, 37–41. [[CrossRef](#)]
- Gourama, H. Foodborne pathogens. In *Food Safety Engineering*; Demirci, A., Feng, H., Krishnamurthy, K., Eds.; Food Engineering Series; Springer International Publishing: Cham, Switzerland, 2020; pp. 25–49. [[CrossRef](#)]
- Gaul, L.K.; Farag, N.H.; Shim, T.; Kingsley, M.A.; Silk, B.J.; Hyytia-Trees, E. Hospital-Acquired Listeriosis Outbreak Caused by Contaminated Diced Celery—Texas, 2010. *Clin. Infect. Dis.* **2013**, *56*, 20–26. [[CrossRef](#)] [[PubMed](#)]
- Buchholz, U.; Bernard, H.; Werber, D.; Böhmer, M.M.; Renschmidt, C.; Wilking, H.; Deleré, Y.; an der Heiden, M.; Adlhoch, C.; Dreesman, J.; et al. German Outbreak of Escherichia Coli O104:H4 Associated with Sprouts. *N. Engl. J. Med.* **2011**, *365*, 1763–1770. [[CrossRef](#)] [[PubMed](#)]
- Multistate Outbreak of Listeriosis Linked to Whole Cantaloupes from Jensen Farms, Colorado | Listeria | CDC. Available online: <https://www.cdc.gov/listeria/outbreaks/cantaloupes-jensen-farms/index.html> (accessed on 14 March 2022).
- Wholesome Soy Products, Inc. Sprouts and Investigation of Human Listeriosis Cases. Available online: <https://www.cdc.gov/listeria/outbreaks/bean-sprouts-11-14/index.html> (accessed on 14 March 2022).
- Davis, K.R.; Dunn, A.C.; Burnett, C.; McCullough, L.; Dimond, M.; Wagner, J.; Smith, L.; Carter, A.; Willardson, S.; Nakashima, A.K. Campylobacter Jejuni Infections Associated with Raw Milk Consumption—Utah, 2014. *Morb. Mortal. Wkly. Rep.* **2016**, *65*, 301–305. [[CrossRef](#)] [[PubMed](#)]
- Enteritidis Infections Linked to Bean Sprouts | November 2014 | Salmonella | CDC. Available online: <https://www.cdc.gov/salmonella/enteritidis-11-14/index.html> (accessed on 14 March 2022).
- Outbreak of Salmonella Infections Linked to Pre-Cut Melons | Outbreak of Salmonella Infections Linked to Pre-Cut Melon | April 2019 | Salmonella | CDC. Available online: <https://www.cdc.gov/salmonella/carrau-04-19/index.html> (accessed on 14 March 2022).
- Tseng, M.-L.; Ha, H.M.; Tran, T.P.T.; Bui, T.-D.; Lim, M.K.; Lin, C.-W.; Helmi Ali, M. Data-Driven on Sustainable Food Supply Chain: A Comparison on Halal and Non-Halal Food System. *J. Ind. Prod. Eng.* **2022**, 1–28. [[CrossRef](#)]
- Fung, F.; Wang, H.-S.; Menon, S. Food Safety in the 21st Century. *Biomed. J.* **2018**, *41*, 88–95. [[CrossRef](#)]

14. Nayak, R.; Waterson, P. Global Food Safety as a Complex Adaptive System: Key Concepts and Future Prospects. *Trends Food Sci. Technol.* **2019**, *91*, 409–425. [CrossRef]
15. Kaur, H. Modelling Internet of Things Driven Sustainable Food Security System. *Benchmarking* **2019**, *28*, 1740–1760. [CrossRef]
16. Thyberg, K.L.; Tonjes, D.J. Drivers of Food Waste and Their Implications for Sustainable Policy Development. *Resour. Conserv. Recycl.* **2016**, *106*, 110–123. [CrossRef]
17. Théolier, J.; Barrere, V.; Charlebois, S.; Benrejeb Godefroy, S. Risk Analysis Approach Applied to Consumers' Behaviour toward Fraud in Food Products. *Trends Food Sci. Technol.* **2021**, *107*, 480–490. [CrossRef]
18. Liu, W.; Shao, X.-F.; Wu, C.-H.; Qiao, P. A Systematic Literature Review on Applications of Information and Communication Technologies and Blockchain Technologies for Precision Agriculture Development. *J. Clean. Prod.* **2021**, *298*, 126763. [CrossRef]
19. Dixon, B.R.; Fayer, R.; Santín, M.; Hill, D.E.; Dubey, J.P. Protozoan parasites: *Cryptosporidium*, *Giardia*, *Cyclospora*, and *Toxoplasma*. *Rapid Detect. Identif. Quantif. Foodborne Pathog.* **2011**, 349–370. [CrossRef]
20. Kelly, S. New approaches to determining the origin of food. In *Food Chain Integrity*; Woodhead Publishing: Sawston, UK, 2011.
21. Andersson, A.; Ronner, U.; Granum, P.E. What Problems Does the Food Industry Have with the Spore-Forming Pathogens *Bacillus Cereus* and *Clostridium Perfringens*? *Int. J. Food Microbiol.* **1995**, *28*, 145–155. [CrossRef]
22. Commission Regulation (EC) No 2073/2005. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R2073&from=EN> (accessed on 14 March 2022).
23. Schaffner, D.W.; Brown, L.G.; Ripley, D.; Reimann, D.; Kockavy, N.; Blade, H.; Nicholas, D. Quantitative Data Analysis to Determine Best Food Cooling Practices in U.S. Restaurants. *J. Food Prot.* **2015**, *78*, 778–783. [CrossRef] [PubMed]
24. Taormina, P.J.; Dorsa, W.J. Growth Potential of *Clostridium Perfringens* during Cooling of Cooked Meats. *J. Food Prot.* **2004**, *67*, 1537–1547. [CrossRef]
25. Rolfe, C.; Daryaei, H. Intrinsic and extrinsic factors affecting microbial growth in food systems. In *Food Safety Engineering*; Demirci, A., Feng, H., Krishnamurthy, K., Eds.; Food Engineering Series; Springer International Publishing: Cham, Switzerland, 2020; pp. 3–24. [CrossRef]
26. Bucknavage, M.; Campbell, J.A. Good manufacturing practices and other programs in support of the food safety system. In *Food Safety Engineering*; Demirci, A., Feng, H., Krishnamurthy, K., Eds.; Food Engineering Series; Springer International Publishing: Cham, Switzerland, 2020; pp. 159–173. [CrossRef]
27. Ho, K.-L.G.; Sandoval, A. Sanitation Standard Operating Procedures (SSOPs). In *Food Safety Engineering*; Demirci, A., Feng, H., Krishnamurthy, K., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 175–190. [CrossRef]
28. LaBorde, L.F. The hazard analysis risk-based preventive controls. In *Food Safety Engineering*; Demirci, A., Feng, H., Krishnamurthy, K., Eds.; Food Engineering Series; Springer: Cham, Switzerland, 2020; pp. 205–226. [CrossRef]
29. Kennedy, A.; Stitzinger, J.; Burke, T. Food traceability. In *Food Safety Engineering*; Demirci, A., Feng, H., Krishnamurthy, K., Eds.; Food Engineering Series; Springer International Publishing: Cham, Switzerland, 2020; pp. 227–245. [CrossRef]
30. Martino, K.; Stone, W.; Ozadali, F. Product recalls as part of the last line of food safety defense. In *Food Safety Engineering*; Demirci, A., Feng, H., Krishnamurthy, K., Eds.; Food Engineering Series; Springer International Publishing: Cham, Switzerland, 2020; pp. 247–263. [CrossRef]
31. Lin, J.; Shen, Z.; Zhang, A.; Chai, Y. Blockchain and IoT based food traceability for smart agriculture. In Proceedings of the ICCSE'18 3rd International Conference on Crowd Science and Engineering, Singapore, Singapore, 28–31 July 2018; pp. 1–6. [CrossRef]
32. Astill, J.; Dara, R.A.; Campbell, M.; Farber, J.M.; Fraser, E.D.G.; Sharif, S.; Yada, R.Y. Transparency in Food Supply Chains: A Review of Enabling Technology Solutions. *Trends Food Sci. Technol.* **2019**, *91*, 240–247. [CrossRef]
33. Ahmed, S.; ten Broek, N. Blockchain Could Boost Food Security. *Nature* **2017**, *550*, 43. [CrossRef]
34. Ray, P.; Harsh, H.O.; Daniel, A.; Ray, A. Incorporating Block Chain Technology in Food Supply Chain. *Int. J. Manag. Stud.* **2019**, *6*, 115. [CrossRef]
35. Tian, F. An agri-food supply chain traceability system for china based on RFID & blockchain technology. In Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016; pp. 1–6. [CrossRef]
36. Shahid, A.; Almogren, A.; Javaid, N.; Al-Zahrani, F.A.; Zuair, M.; Alam, M. Blockchain-Based Agri-Food Supply Chain: A Complete Solution. *IEEE Access* **2020**, *8*, 69230–69243. [CrossRef]
37. Patel, N.; Shukla, A.; Tanwar, S.; Singh, D. KRanTi: Blockchain-Based Farmer's Credit Scheme for Agriculture-Food Supply Chain. *Trans. Emerg. Telecommun. Technol.* **2021**, e4286. [CrossRef]
38. Tian, F. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things. In Proceedings of the 2017 International Conference on Service Systems and Service Management, Dalian, China, 16–18 June 2017; pp. 1–6. [CrossRef]
39. Mondal, S.; Wijewardena, K.P.; Karuppuswami, S.; Kriti, N.; Kumar, D.; Chahal, P. Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain. *IEEE Internet Things J.* **2019**, *6*, 5803–5813. [CrossRef]
40. Blockchain: Transforming Seafood Supply Chain Traceability. Available online: <https://www.wwf.org.nz/?15961/Blockchain-Transforming-Seafood-Supply-Chain-Traceability> (accessed on 12 March 2022).
41. From Shore to Plate: Tracking Tuna on the Blockchain. Available online: <https://www.provenance.org/tracking-tuna-on-the-blockchain> (accessed on 12 March 2022).

42. Marchese, A.; Tomarchio, O. An agri-food supply chain traceability management system based on hyperledger fabric blockchain. In Proceedings of the 23rd International Conference on Enterprise Information Systems (ICEIS2021), Prague, Czech Republic, 26–28 April 2021; pp. 648–658.
43. Huynh, T.S.; Nguyen, L.A. Developing Blockchain-Based System for Tracking the Origin of Chicken Products. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 90–96.
44. Dey, S.; Saha, S.; Singh, A.K.; McDonald-Maier, K. FoodSQRBlock: Digitizing Food Production and the Supply Chain with Blockchain and QR Code in the Cloud. *Sustainability* **2021**, *13*, 3486. [\[CrossRef\]](#)
45. Tsoukas, V.; Gkogkidis, A.; Kampa, A.; Spathoulas, G.; Kakarountas, A. Blockchain technology in food supply chain: A state of the art. In Proceedings of the 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Preveza, Greece, 24–26 September 2021; pp. 1–8. [\[CrossRef\]](#)
46. Creydt, M.; Fischer, M. Blockchain and More—Algorithm Driven Food Traceability. *Food Control* **2019**, *105*, 45–51. [\[CrossRef\]](#)
47. FAO Traceability/Product Tracing in Codex. Available online: http://www.fao.org/waicent/faoinfo/food-safety-quality/cd_hygiene/cnt/cnt_en/sec_3/docs_3.6/Traceability.pdf (accessed on 12 March 2022).
48. Aung, M.M.; Chang, Y. Traceability in a Food Supply Chain: Safety and Quality Perspectives. *Food Control* **2014**, *39*, 172–184. [\[CrossRef\]](#)
49. Salampasis, M.; Tektonidis, D.; Kalogianni, E.P. TraceALL: A Semantic Web Framework for Food Traceability Systems. *J. Syst. Inf. Technol.* **2012**, *14*, 302–317. [\[CrossRef\]](#)
50. Oliveira, J.; Lima, J.E.; da Silva, D.; Kuprych, V.; Faria, P.M.; Teixeira, C.; Ferreira Cruz, E.; Rosado da Cruz, A.M. Traceability System for Quality Monitoring in the Fishery and Aquaculture Value Chain. *J. Agric. Food Res.* **2021**, *5*, 100169. [\[CrossRef\]](#)
51. Bevilacqua, M.; Ciarapica, F.E.; Giacchetta, G. Business Process Reengineering of a Supply Chain and a Traceability System: A Case Study. *J. Food Eng.* **2009**, *93*, 13–22. [\[CrossRef\]](#)
52. Biswas, K.; Muthukkumarasamy, V.; Lum, W. Blockchain based wine supply chain traceability system. In Proceedings of the Future Technologies Conference (FTC), Vancouver, BC, Canada, 29–30 November 2017.
53. Narrod, C.; Roy, D.; Okello, J.; Avendaño, B.; Rich, K.; Thorat, A. Public–Private Partnerships and Collective Action in High Value Fruit and Vegetable Supply Chains. *Food Policy* **2009**, *34*, 8–15. [\[CrossRef\]](#)
54. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. Blockchain in Agriculture Traceability Systems: A Review. *Appl. Sci.* **2020**, *10*, 4113. [\[CrossRef\]](#)
55. Bosona, T.; Gebresenbet, G. Food Traceability as an Integral Part of Logistics Management in Food and Agricultural Supply Chain. *Food Control* **2013**, *33*, 32–48. [\[CrossRef\]](#)
56. Dabbene, F.; Gay, P.; Tortia, C. Traceability Issues in Food Supply Chain Management: A Review. *Biosyst. Eng.* **2014**, *120*, 65–80. [\[CrossRef\]](#)
57. Badia-Melis, R.; Mishra, P.; Ruiz-García, L. Food Traceability: New Trends and Recent Advances. A Review. *Food Control* **2015**, *57*, 393–401. [\[CrossRef\]](#)
58. Hofstede, G.J.; Spaans, L.; Schepers, H.; Trienekens, J.H.; Beulens, A.J.M. *Hide or Confide: The Dilemma of Transparency*; Reed Business Information: New York, NY, USA, 2004.
59. Wognum, P.M.; Bremmers, H.; Trienekens, J.H.; van der Vorst, J.G.A.J.; Bloemhof, J.M. Systems for Sustainability and Transparency of Food Supply Chains—Current Status and Challenges. *Adv. Eng. Informatics* **2011**, *25*, 65–76. [\[CrossRef\]](#)
60. Kraft, T.; Zheng, Y. How Supply Chain Transparency Boosts Business Value. *MIT Sloan Manag. Rev.* **2021**, *63*, 34–40.
61. Montecchi, M.; Plangger, K.; West, D.C. Supply Chain Transparency: A Bibliometric Review and Research Agenda. *Int. J. Prod. Econ.* **2021**, *238*, 108152. [\[CrossRef\]](#)
62. Medina, G.; Thomé, K. Transparency in Global Agribusiness: Transforming Brazil’s Soybean Supply Chain Based on Companies’ Accountability. *Logistics* **2021**, *5*, 58. [\[CrossRef\]](#)
63. Schäfer, N. Making Transparency Transparent: A Systematic Literature Review to Define and Frame Supply Chain Transparency in the Context of Sustainability. *Manag. Rev. Q.* **2022**, 1–26 [\[CrossRef\]](#)
64. Blockchain Food Traceability. Available online: <https://openlink.com/en/insights/articles/blockchain-food-traceability-can-revolutionize-the-industry/> (accessed on 14 March 2022).
65. Shafiee-Jood, M.; Cai, X. Reducing Food Loss and Waste to Enhance Food Security and Environmental Sustainability. *Environ. Sci. Technol.* **2016**, *50*, 8432–8443. [\[CrossRef\]](#) [\[PubMed\]](#)
66. Cavaliere, A.; Ricci, E.C.; Solesin, M.; Banterle, A. Can Health and Environmental Concerns Meet in Food Choices? *Sustainability* **2014**, *6*, 9494–9509. [\[CrossRef\]](#)
67. European Commission Consumer Policy—Strengthening the Role of Consumers in the Green Transition. Available online: <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12467-Empowering-the-consumer-for-the-green-transition> (accessed on 12 March 2022).
68. Ivanov, D. Viable Supply Chain Model: Integrating Agility, Resilience and Sustainability Perspectives—Lessons from and Thinking beyond the COVID-19 Pandemic. *Ann. Oper. Res.* **2020**, 1–21 [\[CrossRef\]](#) [\[PubMed\]](#)
69. Dolgui, A.; Ivanov, D. Exploring Supply Chain Structural Dynamics: New Disruptive Technologies and Disruption Risks. *Int. J. Prod. Econ.* **2020**, *229*, 107886. [\[CrossRef\]](#)
70. Nandi, S.; Sarkis, J.; Hervani, A.A.; Helms, M.M. Redesigning Supply Chains Using Blockchain-Enabled Circular Economy and COVID-19 Experiences. *Sustain. Prod. Consum.* **2021**, *27*, 10–22. [\[CrossRef\]](#)

71. Tseng, M.-L.; Lim, M.K.; Helmi Ali, M.; Christianti, G.; Juladacha, P. Assessing the Sustainable Food System in Thailand under Uncertainties: Governance, Distribution and Storage Drive Technological Innovation. *J. Ind. Prod. Eng.* **2022**, *39*, 1–18. [CrossRef]
72. Sustainability in the Food Industry: Progress and Next Steps. Available online: https://insights.figlobal.com/sites/figlobal.com/files/uploads/2018/04/Whitepaper-Sustainability-in-the-food-industry-progress-and-next-steps-including-case-study-on-Symrise_-Solvay_-Diana-Food-and-ABC_FINAL-1.pdf (accessed on 12 March 2022).
73. Rana, R.L.; Tricase, C.; De Cesare, L. Blockchain Technology for a Sustainable Agri-Food Supply Chain. *Br. Food J.* **2021**, *123*, 3471–3485. [CrossRef]
74. Hervani, A.A.; Nandi, S.; Helms, M.M.; Sarkis, J. A Performance Measurement Framework for Socially Sustainable and Resilient Supply Chains Using Environmental Goods Valuation Methods. *Sustain. Prod. Consum.* **2022**, *30*, 31–52. [CrossRef]
75. GHP and HACCP | Food Safety and Quality | Food and Agriculture Organization of the United Nations. Available online: <https://www.fao.org/food-safety/food-control-systems/supply-chains-and-consumers/ghp-and-haccp/en/> (accessed on 12 March 2022).
76. Organic Area Accounted for 4% of the Total Utilised Agricultural Area in the EU25 in 2005. Available online: <https://ec.europa.eu/eurostat/web/products-euro-indicators/-5-12062007-bp> (accessed on 12 March 2022).
77. Organic Farming in the EU. Available online: https://ec.europa.eu/info/sites/default/files/food-farming-fisheries/farming/documents/market-brief-organic-farming-in-the-eu_mar2019_en.pdf (accessed on 14 March 2022).
78. Hoorfar, J.; Jordan, K.; Butler, F.; Prugger, R. *Food Chain Integrity: A Holistic Approach to Food Traceability, Safety, Quality, and Authenticity*; Woodhead Pub. Ltd: Oxford, UK; Philadelphia, PA, USA, 2011.
79. Montet, D.; Ray, R.C. *Food Traceability and Authenticity: Analytical Techniques*; CRC Press: Boca Raton, FL, USA, 2017. [CrossRef]
80. FAO. *The State of World Fisheries and Aquaculture, (SOFA)*; Technical Report, FAO: Rome, Italy, 2020.
81. Oceana Oceana Canada Report Uncovers Widespread Seafood Fraud Across Country. Available online: <https://www.oceana.ca/en/press-center/press-releases/oceana-canada-report-uncovers-widespread-seafood-fraud-across-country> (accessed on 12 March 2022).
82. Sotelo, C.G.; Velasco, A.; Perez-Martin, R.I.; Kappel, K.; Schröder, U.; Verrez-Bagnis, V.; Jérôme, M.; Mendes, R.; Silva, H.; Mariani, S.; et al. Tuna Labels Matter in Europe: Mislabelling Rates in Different Tuna Products. *PLoS ONE* **2018**, *13*, e0196641. [CrossRef]
83. Regulation (EC) No 852/2004 of The European Parliament And Of The Council. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0852&from=EN> (accessed on 14 March 2022).
84. Regulation (EC) No 853/2004 of The European Parliament And Of The Council. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0853&from=EN> (accessed on 14 March 2022).
85. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [CrossRef]
86. Perboli, G.; Musso, S.; Rosano, M. Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases. *IEEE Access* **2018**, *6*, 62018–62028. [CrossRef]
87. Banerjee, A. Chapter Three—Blockchain technology: Supply chain insights from ERP. In *Advances in Computers*; Raj, P., Deka, G.C., Eds.; Blockchain Technology: Platforms, Tools and Use Cases; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 69–98. [CrossRef]
88. Dos Santos, R.B.; Torrisi, N.M.; Yamada, E.R.K.; Pantoni, R.P. IGR Token-Raw Material and Ingredient Certification of Recipe Based Foods Using Smart Contracts. *Informatics* **2019**, *6*, 11. [CrossRef]
89. Dettmers, T. 8-Bit Approximations for Parallelism in Deep Learning. *arXiv* **2016**, arXiv:1511.04561.
90. Gholami, A.; Kim, S.; Dong, Z.; Yao, Z.; Mahoney, M.W.; Keutzer, K. A Survey of Quantization Methods for Efficient Neural Network Inference. *arXiv* **2021**, arXiv:2103.13630.
91. Park, E.; Yoo, S.; Vajda, P. Value-Aware Quantization for Training and Inference of Neural Networks. *arXiv* **2018**, arXiv:1804.07802.
92. Mozer, M.C.; Smolensky, P. Skeletonization: A Technique for trimming the fat from a network via relevance assessment. In *Advances in Neural Information Processing Systems 1*; Morgan Kaufmann Publishers Inc.: San Francisco, CA, USA, 1989; pp. 107–115.
93. Hagiwara, M. Removal of hidden units and weights for back propagation networks. In Proceedings of the 1993 International Conference on Neural Networks (IJCNN-93-Nagoya, Japan), Nagoya, Japan, 25–29 October 1993; Volume 1, pp. 351–354. [CrossRef]
94. David, R.; Duke, J.; Jain, A.; Reddi, V.J.; Jeffries, N.; Li, J.; Kreeger, N.; Nappier, I.; Natraj, M.; Regev, S.; et al. TensorFlow Lite Micro: Embedded Machine Learning on TinyML Systems. *arXiv* **2021**, arXiv:2010.08678.
95. Edge Impulse. Available online: <https://www.edgeimpulse.com/> (accessed on 14 March 2022).
96. Bian, S.; Lukowicz, P. Capacitive sensing based on-board hand gesture recognition with TinyML. In Proceedings of the 2021 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Virtual USA, 21–26 September 2021; pp. 4–5.
97. Fedorov, I.; Stamenovic, M.; Jensen, C.; Yang, L.-C.; Mandell, A.; Gan, Y.; Mattina, M.; Whatmough, P.N. TinyLSTMs: Efficient Neural Speech Enhancement for Hearing Aids. *Interspeech* **2020**, *2020*, 4054–4058. [CrossRef]
98. T’Jonck, K.; Kancharla, C.R.; Vankeirsbilck, J.; Hallez, H.; Boydens, J.; Pang, B. Real-time activity tracking using TinyML to support elderly care. In Proceedings of the 2021 XXX International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 15–17 September 2021; pp. 1–6. [CrossRef]

99. Roshan, A.N.; Gokulapriyan, B.; Siddarth, C.; Kokil, P. Adaptive traffic control with TinyML. In Proceedings of the 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 11 May 2021; pp. 451–455. [CrossRef]
100. Andrade, P.; Silva, I.; Signoretti, G.; Silva, M.; Dias, J.; Marques, L.; Costa, D.G. An unsupervised TinyML approach applied for pavement anomalies detection under the internet of intelligent vehicles. In Proceedings of the 2021 IEEE International Workshop on Metrology for Industry 4.0 IoT (MetroInd4.0 IoT), Rome, Italy, 7–9 June 2021; pp. 642–647. [CrossRef]
101. Lahade, S.V.; Namuduri, S.; Upadhyay, H.; Bhansali, S. Alcohol Sensor Calibration on the Edge Using Tiny Machine Learning (Tiny-ML) Hardware. *Meet. Abstr.* **2020**, *MA2020-01*, 1848. [CrossRef]
102. Alongi, F.; Ghielmetti, N.; Pau, D.; Terraneo, F.; Fornaciari, W. Tiny neural networks for environmental predictions: An integrated approach with Miosix. In Proceedings of the 2020 IEEE International Conference on Smart Computing (SMARTCOMP), Bologna, Italy, 14–17 September 2020; pp 350–355. [CrossRef]
103. Vuppapapati, C.; Ilapakurti, A.; Chillara, K.; Kedari, S.; Mamidi, V. Automating tiny ML intelligent sensors DevOPS using Microsoft Azure. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020; pp 2375–2384. [CrossRef]
104. Crossing the Artificial Intelligence (AI) Chasm, Albeit Using Constrained IoT Edges and Tiny ML, for Creating a Sustainable Food Future. Available online: <https://www.springerprofessional.de/en/crossing-the-artificial-intelligence-ai-chasm-albeit-using-const/18435296> (accessed on 14 March 2022).
105. Lord, M. TinyML, Anomaly Detection. Available online: <https://scholarworks.calstate.edu/concern/theses/8336h7115?locale=en> (accessed on 14 March 2022).
106. Dutta, A.; Kant, S. Implementation of cyber threat intelligence platform on Internet of Things (IoT) using TinyML approach for deceiving cyber invasion. In Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Port Louis, Mauritius, 7–8 October 2021; pp 1–6. [CrossRef]
107. Metamask. Available online: <https://metamask.io/> (accessed on 12 March 2022).
108. Lee, W.-M. Using the MetaMask chrome extension. In *Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript*; Lee, W.-M., Ed.; Apress: Berkeley, CA, USA, 2019; pp. 93–126. [CrossRef]
109. Rewatkar, H.R.; Agarwal, D.; Khandelwal, A.; Upadhyay, S. Decentralized voting application using blockchain. In Proceedings of the 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 18–19 June 2021; pp. 735–739. [CrossRef]
110. Web3JS Etherreum JavaScript API. Available online: <https://web3js.readthedocs.io/en/v1.7.1/> (accessed on 12 March 2022).
111. Arduino Nano 33 Datasheet. Available online: <https://docs.arduino.cc/resources/datasheets/ABX00031-datasheet.pdf> (accessed on 12 March 2022).