An IoT-Sensor with Security Capabilities for acting on a Blockchain architecture-Based Food Traceability System

Eng. Carlos Andrés González Amarillo

Universidad del Cauca

Faculty of Electronics and Telecommunications Engineering
Master Program in Telematics Engineering
Line of Research in e-environment
Popayán, Jun 2021

Carlos Andrés González Amarillo

An IoT-Sensor with Security Capabilities for acting on a Blockchain architecture-Based Food Traceability System

Dissertation Submitted to the Faculty of Electronics and Telecommunications Engineering of the Universidad del Cauca, Colombia. For the acquisition of the academic degree:

Magíster en:
Ingeniería Telemática

Advisor:
Ph.D. Juan Carlos Corrales Muñoz

Co-Advisors:
Ph.D. Gustavo Adolfo Ramirez González
Ph.D. Miguel Angel Mendoza Moreno

Popayán
2021

(MEANWHILE YOU CAN, TRY IT.)

La experiencia es, sin ninguna duda, el primer producto surgido de nuestro entendimiento al elaborar éste la materia bruta de las impresiones sensibles. Por ello mismo es la primera enseñanza y constituye, en su desarrollo, una fuente tan inogatable de informaciones nuevas, que nunca faltará la concatenación entre todos los nuevos conocimientos que se produzcan en el futuro y que puedan reunirse sobre esta base. Sin embargo, nuestro entendimiento no se reduce al único terreno de la experiencia. Aunque ésta nos dice qué es lo que existe, no nos dice que tenga que ser necesariamente así y no de otra forma. Precisamente por eso no nos da la verdadera universalidad, y la razón, tan deseosa de este tipo de conocimientos, más que satisfecha, queda incitada por la experiencia.

IMMANUEL KANT

Acknowledgements

I would like to thank doctors Gustavo Adolfo Ramirez, Miguel Angel Mendoza, and Juan Carlos Corrales. Without them, this master thesis never has been possible. Thanks to all resources that were provided by (GIT) Telematics Research Group, for making possible my research. Moreover, thanks to COLCIENCIAS and The Gobernación de Boyacá for my PhD scholarship.

Structured abstract

Background: Food Traceability Systems (FTS) has found on IoT a powerful tool for guaranteeing the track of products or raw materials in any production stage, because it is highly interoperable, scalable, open, and ubiquitous. IoT has become an adaptable technology to any context for collecting and transmitting data, whether to analyze or to inform the stakeholders. Moreover, its main purpose is to keep the customer informed about the innocuity and quality of the product with transparent data. FTS has security mechanisms for production processes, with different security levels that give high or low reliability according to the technology used. Those low levels extend the opportunities to commit fraud or to ignore security issues on IoT-based production chain. The reasons above allow concluding that, until today, there is an information system in the FTS, but it is not a completely secure system. For this reason, it is necessary to search and sort these security issues. Since emerging technologies as Blockchain can solve the majority of security problems present on IoT ecosystems through Blockchain-IoT BIoT architectures.

Aims: This thesis aims to design and development a BIoT-Sensor (BIoTS) that provides data transparency and integrity in the storage and transmission information process without needing an intermediary device (Hub) in the transport layer within IoT architecture. This new BIoTS has the specific capabilities to act as a primary source of reliability and certification in FTS based on the BIoT architecture. Moreover, it will have the capacity to participate as a Miner within the Blockchain network.

Methods: To achieve the objective of this thesis, we used the methodology of scientific documentary research and the technological development process. First, we present the summary of the bibliometric analysis that provides a scientific overview of the information technology-based STFs (The complete bibliometric analysis is attached in the appendix). In the scientific research methodology stage, we identify the main research areas, research gaps, and research opportunities that lead to the research question and the formal statement of objectives. In the solution approach stage, we present the description of the Blockchain architecture and a conventional IoT sensor; in this process, we identify the security requirements of both parts to match the architectures and achieve a new device called BIoTS. Finally, we present a method of hardware development, validation, and evaluation regarding the security of the Blockchain-based BIoTS device in an IoT ecosystem.

Results: Through this process, we have defined the IoT ecosystem's necessities in terms of security and the implications that have the development of new (BIoTS) (Blockchain-IoT-Sensor-of-Traceability-Systems) inside of FTS. We analyze BIoTS behavior to guarantee the traceability of products transparently throughout the supply chain and, second, guarantee the traceability of data in food security matters. The BIoTS modules that adapt to the Blockchain architecture (cryptography and consensus algorithms) were developed on an FPGA (Field-Programmable Gate Array). The peripheral modules were implemented with analog electronics and embedded devices. The BIoTS, thanks to its architectural elements, is a hardware device capable of participating as a miner in a Blockchain network.

Conclusions: New BIoTS designed can solve some high, intermediate, and low-level security issues into the FTS. The sensor designed its novel and integrate two disruptive technologies (Blockchain and IoT) for solving security issues on food safety. In this case, BIoTS was designed for the agriculture domain, where the security issues in the supply chain are frequent and affect the health of many people. The BIoTS device maintained a continuous, unmediated connection to the Blockchain network hosted at the proposed Blockchain-IoT architecture application layer. 110 bytes of data were transmitted at a transaction rate per second of 0.99 and with a maximum latency of 0.10 seconds.

Keywords: Food Traceability System, IoT, Blockchain, IoT Security, Food Safety.

Resumen Estructurado

Antecedentes: Los sistemas de trazabilidad de alimentos (FTS, siglas en inglés) han encontrado en el internet de las cosas (IoT), una poderosa herramienta para garantizar el seguimiento de los productos o a las materias primas en cualquier etapa de producción, porque es altamente interoperable, escalable, abierta y ubicua. IoT se ha convertido en una tecnología adaptable a cualquier contexto para recopilar y transmitir datos, ya sea para analizarlos o para informar a los interesados. Además, su principal objetivo es mantener al cliente informado sobre la inocuidad y la calidad del producto con datos transparentes.

Los FTS cuentan con mecanismos o elementos de seguridad para los procesos de producción, con diferentes niveles de seguridad que dan una alta o baja fiabilidad según la tecnología utilizada. Esos bajos niveles amplían las oportunidades de cometer fraude o de ignorar los problemas de seguridad en la cadena de producción basada en IoT. Las razones anteriores permiten concluir que, hasta hoy, existe un sistema de información en los FTS, pero no son un sistema completamente seguro. Por esta razón, es necesario buscar y resolver estos problemas de seguridad. Ya que las tecnologías emergentes como Blockchain pueden resolver la mayoría de los problemas de seguridad presentes en los ecosistemas de IoT a través de las arquitecturas Blockchain-IoT BIoT.

Objetivos: Esta diseratación tiene como objetivo diseñar y construir un dispositivo BIoT-Sensor (BIoTS) que proporcione integridad y transparencia de datos en el proceso de almacenamiento y transmisión de información sin necesidad de un dispositivo intermediario (Hub) en la capa de transporte de la arquitectura IoT. Este nuevo BIoTS tiene las capacidades específicas para actuar como fuente primaria de fiabilidad y certificación en FTS basado en la arquitectura BIoT. Además, tendrá la capacidad de garantizar la participación como Miner en una red Blockchain.

Metodos: Para lograr el objetivo de esta tesis, utilizamos la metodología de la investigación científica documental y el proceso de desarrollo tecnológico. Primero, presentamos el resumen del análisis bibliométrico que brinda un panorama científico de los FTS basados en tecnologías de la información (En anexo se presenta el análisis bibliométrico completo). En la etapa de la metodología de la investigación científica, identificamos las

principales áreas de investigación, las brechas y la oportunidad de investigación que dan lugar a la pregunta de investigación y al planteamiento formal de los objetivos. En la etapa del planteamiento de la solución, presentamos la descripción de la arquitectura de Blockchain y de un sensor IoT convencional; en este proceso, identificamos los requisitos de seguridad de ambas partes para hacer coincidir las arquitecturas y lograr un nuevo dispositivo llamado BIoTS. Finalmente, presentamos un proceso de desarrollo hardware, validación y evaluación en términos de seguridad del dispositivo BIoTS basado en Blockchain en un ecosistema IoT.

Resultados: En el proceso de diseño e implementación del BIoTS, hemos definido las necesidades de los ecosistemas de IoT en términos de seguridad y las implicaciones que tiene el desarrollo de nuevos (BIoTS) (Blockchain-IoT-Sensor-for-Traceability-Systems) dentro del FTS. El nuevo BIoTS se adapta a la arquitectura del FTS para garantizar la trazabilidad de los productos de forma transparente a lo largo de la cadena de suministro y garantiza la trazabilidad de los datos en materia de seguridad alimentaria. Los módulos de BIoTS que se adaptan a la arquitectura de Blockchain (algoritmos de criptografía y consenso) fueron desarrollados en una FPGA (Field-Programmable Gate Array). Los módulos periféricos fueron implementados con electrónica análoga y dispositivos embebidos. BIoTS, gracias a sus elementos arquitectónicos, es un dispositivo hardware capaz de participar como miner en una red Blockchain.

Conclusiones: El nuevo BIoTS diseñado puede resolver algunos problemas de seguridad de alto, medio y bajo nivel en los FTS. El diseño del sensor es novedoso porque integrada dos tecnologías disruptivas (Blockchain-IoT) para resolver problemas de seguridad en la informacíon y la comunicación y además en la seguridad alimentaria. En este caso, el BIoTS se diseñó para el dominio de la agricultura, donde los problemas de seguridad en la cadena de suministro son frecuentes y afectan la calidad y por lo tanto, la salud de las personas. El dispositivo BIoTS mantuvo una conexión continua y sin intermediarios con la red Blockchain alojada en la capa de aplicación de la arquitectura Blockchain-IoT propuesta. Fueron transmitidos 110 bytes de datos, a una tasa de transacción por segundo de 0,99 y con una latencia máxima de 0,10 segundos.

Keywords: Sistemas de trazabilidad alimentaria, Internet de las cosas (IoT), Blockchain, Seguridad IoT, Seguridad alimentaria.

Content

List of Figures

List of Tables

1. Introduction

Traceability is defined as the ability to track the movement of food through specific stages of production, transformation, and distribution [4]. Food Traceability Systems (FTS) consider production processes in two abstract forms. Value Chain (VC) refers to a product's earned quality or economic value when it changes at each stage of the process [5]. This value is perceived by the customer and therefore is specifically designed for that purpose. Second, Supply Chain (SC) has the unique purpose of assuring safe and quality products with external stakeholders such as the government, private entities, suppliers, or trade agreements evaluators. In this chain, the product may or may not suffer transformations by chain actors [4, 6].

FTS enables us to locate, record, and trace products in the manufacture, processing, and distribution through platforms that offer access to users [7], for instance, Internet of Things platforms [8]. Such platforms promote quality in production, facilitate the identification of problems, and improve communication capacity between stakeholders.

Internet of Things (IoT) can be defined as a technological paradigm based on Internet connectivity, where the correlated computing devices, objects, animals, or people, are identified by Unique Identification (UID). These devices are set to satisfy necessities through some actions or to provide specific information for decision making in the activities directed to services supplied by digital or mechanic machines [9, 10].

IoT has become an adaptable technology to any context for collecting and transmitting data, whether to analyze or to inform the stakeholders [11, 12]. SC has found in IoT a powerful tool for guaranteeing the track of products or raw materials in any production stage because it is highly interoperable, scalable, open, and ubiquitous. Moreover, its primary purpose is to keep the customer informed about the harmlessness and quality of the product with transparent data [13, 14].

Data integrity is a critical security issue within IoT ecosystems. To improve the communication process between peer devices, it might focus on solving data management from several technological schemes (fog or edge computing), but the transparency of the information recorded is not always guaranteed. A current IoT system contains multiples devices with embedded sensors characterized by low power, reduced memory capacity,

and limited processing capabilities. These features allow identifying the origin of significant security problems. Nevertheless, any solution concerning IoT devices' security capabilities is designed from the software that governs the data management, generally in the management layer of the system. For this reason, new challenges arise today in the management of informatic security in communication systems. Food security demands new concepts of trust, and Blockchain is an obvious choice for further development in this regard.

Blockchain technology can be defined as a phenomenon from three viewpoints; social, economic, and technological. Social, because the information transparency concept is assured through cryptography; economic because the cooperation in a business process imposes the idea of crypto-currency and breaks the scheme of the common currency [15–17]. Finally, technological because it also breaks the centralized systems concept and imposes distributed systems as a solution to the critical issues of access and security [18–20].

Blockchain-IoT (BIoT) can be implemented on an SC in two ways. First, from software usage, it allows management of the network resources to share the information and reach the participation of the actors of the SC through the smart contracts [21, 22]. The second way involves the sensor's hardware development to improve the storage and device's processing capabilities to act as an active role in the mining process on the blockchain architecture [16, 20, 22].

2. Chapter 1
Research Proposal

This chapter contains the formal presentation of the dissertation. Identifying the problem and the analysis of its context gives rise to the research question that will support the contribution of the research work. The review of the scientific literature provides the roadmap for searching gaps in the proposed solutions and supports the objectives of the dissertation. Conceptual elements to understand the problem, the context, and the purpose of the research are described from the point of view of scientific research methodology.

2.1. Statement of the problem

The act of assuring safety along the SC has involved defining concepts such as backward-traceability, referring to the geographic origin and sanitary status of the products or raw materials used in the production; forward-traceability, meaning the destination the product will have; and internal-traceability, that relates to the processes of cultivation. Internal-traceability is generally used in agriculture for phytosanitary, hygiene, and safety evaluation of production [4].

The Short Supply Chain (SSC) refers to short production chains where industrialization or extensive farming does not intervene; in the context of Colombia, as a developing country, it does not have the technological maturity level to implement FTS for safeguarding the foodstuff production because the information and communication technologies in the country do not have any influence in the agricultural production [23]. This situation makes some countries consider the deployment of cost-effective paths that improve the competitive level as a food producer as in [24, 25]. To that effect, Colombia's agricultural production can be seen as a cluster of specific products sorted by region and intended for local consumption. Generally, the SSC concept can support the traceability systems' design for small producers and conduct good practices for mitigating environmental impacts and ensuring the food product's safety and quality. As the SC are processes based on the Internet of Things (IoT) systems, the SSC can adopt the same techniques, but according to new social, economic or socials approaches [26–29].

In all cases where are implemented IoT-based FTS, the sensors are the basis of the system. The sensors should ensure the data transparency on the communication process, from the data collection to the same transmission. Nevertheless, security issues on IoT systems are primarily due to the disability of sensors for providing security on an information system.

Theoretically, data transparency on IoT-based FTS is defined as the impossibility to corrupt data or reduce information transmission error of active devices (sensors) that intervene on capturing variables [13, 14]. Transparency of the communication processes in SCs is a critical aspect that now concentrates engineering efforts to overcome issues and challenges regarding data security. The SC generally is an IoT-based scheme due to the deployment of architectures through the behavior of networks, devices, sensors, and actuators. Nowadays, these systems assess transparency, privacy, integrity, and redundancy of communication and information. However, unfortunately, on practice, IoT ecosystems do not fully guarantee such measures [30, 31].

FTS has security mechanisms for production processes, with different security levels that give high or low reliability according to the technology used [32, 33]. Those low levels extend the opportunities to commit fraud or to ignore security issues on IoT-based production chain [34, 35]. The reasons above allow concluding that, until today, there is an information system in the FTS, but it is not a completely secure system. For this reason, it is necessary to search and sort these security issues.

According to the most frequent security vulnerabilities in [36] were identified and classified IoT security issues. After summarizing the IoT-Systems' security threats, some works rank these threats as challenges in the security field and propose a hierarchy of security issues: i) Low-level security issues highlight the insecure initialization, insecure physical interface, or jamming adversaries. ii) Intermediate-level security issues highlight the insecurity of network connectivity between devices, authentication, non-secure communication on end-to-end transport-level security, and privacy violation on cloud-based IoT. iii) High-level security issues highlight Constrained Application Protocol (CoAP) security with the internet, insecure interfaces, insecure Software/firmware, and middleware security.

Since emerging technologies as Blockchain can solve the majority of security problems present on IoT ecosystems, this proposal will focus on solving some intermediate-level-security issues concerning the reliability of end-to-end data transmitted on the IoT network [37]. In this sense, it is an opportunity to enhance the approach of the new Blockchain-IoT (BIoT) concept [38]. An IoT-Sensor designed according to the security requirements of Blockchain guarantees the data transparency transmitted from the sensor to the stakeholders that take part in the Blockchain-IoT-based system.

IoT devises management, control, and security for data protection, a field with open challenges and opportunities to apply new information techniques and security technologies. Diverse works predict the potential use of smart contracts (Blockchain) in the supply chain using Hubs-IoT [16–18]. However, the Intermediate-level security issues caused by specific hardware devices depend on how they act in the cloud as a mining actor in the Blockchain architecture without needing an intermediary device (Hub) in the fog or edge layer. [20–22]. Currently, the related works in the area do not reflect the existence of approaches to improve IoT devices' specific capabilities to act as main sources of reliability and certification in FTS based on the BIoT architecture.

The BIoT application of the SSC concept represents an appropriate technological solution to small agriculture that guarantees data transparency, stakeholders' participation and provides a decentralized e-commerce platform for consumers of the safety and quality food products. Therefore, this proposal focuses on the development of an investigative process aimed to harmonize a hardware-based BIoT solution for FTS, answering the following research question:

How to transmit data from an IoT sensor to the Blockchain network in a transparent way within a short supply chain?

2.2. Motivation

Today, significant safety issues of food have a relation with the harmlessness gained throughout the supply chain. Only through some technologies and techniques used on IoT systems can guarantee total transparency of data and quality products. Almost most of them lack reliability according to standards of quality. The principal reason is that major IoT devices (Sensors) existing in the IoT ecosystems do not have security features.

One of the issues that motivate this master proposal is improving the data security of the food traceability systems based on IoT ecosystems through Blockchain implementation. Transparency of the information record guarantees the quality and safety of products that make part of the productive process. For this reason, this information must be covered through technologies that allow knowing the product sheet, which means that the data also is traceable along the supply chain and transmitted reliably to stakeholders.

In the above context, in this master's thesis, we identified the Sensor as a critical element in the IoT-based FTS. For this reason, we focus on the design of new capabilities to the Sensor for acting as an element that provides security and transparency in the collection

and transmitting of data. FTS, based on Blockchain-IoT architecture, can solve significant security problems and avoid security attacks inside the system.

2.3. Objectives

2.3.1. General Objective

To supply, in a transparent way and without intermediaries, sensed data to the Blockchain network through the implementation of specific security capacities in a BIoT network's sensor within a short supply chain.

2.3.2. Specific Objectives

- To identify the Blockchain architecture security requirements needed to a transparent communication between an IoT sensor and a Blockchain network.
- To propose additional storage and processing units to an IoT sensor needed for its integration with a Blockchain architecture.
- To design an IoT sensor that contains the proposed storage and processing units.
- To verify the transparency of data transmitted from the designed IoT sensor to a Blockchain network without deploying intermediaries.

2.4. Contributions

The present master proposal aims to achieve the following contributions:

- An IoT-Sensor able to participate as a miner on blockchain archituecture.
- A Blockchain-IoT solution for solving security issues on traceability systems (Food Traceability Systems).
- The first approach to traceability platform based on the IoT concept. The assessment of sensors and actuators into Traceability Systems, one research paper titled "An IoT-Based Traceability System for Greenhouse Seedling Crops" Volume 6, Special Issue 2018, and indexed in the JCR Q1. We present the original paper in Appendix A.
- The core of this master thesis shows a general description of Blockchain-IoT Sensor for Traceability Systems (BIoTS) in a scientific paper titled: "Blockchain-IoT Sensor

(BIoTS): A solution to IoT-Ecosystems Security Issues" The article was accepted in the journal Sensors, indexed in the JCR Q1. It will be published in the next few days. We present the original paper in Appendix A.

- Bibliometric Analysis made for searching gaps and research opportunities in food safety from the information and communications technologies. This work is presented in an original and extended paper titled: "Visualizing a global panorama of the food traceability systems through science mapping: Gaps and research opportunities." This paper is now evaluating in a scientific journal for possible publishing. We present the original paper in Appendix A.

2.5. Contents of the Dissertation

This dissertation is divided into five chapters, which we describe as follows:

Chapter 1. Research Proposal:
In this chapter, we present the research proposal according to the guidelines required by the program. We offer the problem statement, the motivation, the objectives, the scientific contributions of the research, and the dissertation content summary.

Chapter 2. Bibliometric Analysis:
In this chapter, we present a summary of the Bibliometric Analysis of Food Traceability Systems in the 2001-2019 period. This analysis allows us to identify referents works, authors, techniques, and technologies used on traceability Systems. Moreover, we identify the gaps and research opportunities, and it gives us the contributions opportunity in the research field.

Chapter 3. Real World Problem:
This chapter describes the Blockchain-IoT architecture for identifying basic hardware and software requirements to deploy communication processes on the IoT network with Blockchain technology. We present IoT security issues and challenges, and we contextualize the motivation scenario with the solution in an overview of Security on The IoT-based Food Traceability Systems. We describe the security issues and how BIoTS is a potential solution.

Chapter 4. Proposal Development:
This chapter presents the design of BIoTS-Sensor architecture able to participate in BlockchainIoT-based traceability systems. Build on FPGA all modules present on the new BIoTS device according to requirements of Blockchain architecture. We describe

the Blockchain and IoT Systems architecture (Including the sensors) for identifying security and hardware requirements to match both technologies, and we can design a specific solution at the hardware level. Besides, we present the IoT Sensor (BIoTS) evaluation into the network intended for a Blockchain-IoT architecture-based that allows defining the behavior and assess the integrity of transmitting and recorded data.

Chapter 5. Conclusion and Future Works:
Finally, in this chapter, we present the ins and outs of our IoT Sensor (BIoTS) able to act directly on a Blockchain-IoT architecture. This performance considering individual aspects relating to Food Traceability Systems, and propose different future works that could increase the impact of our BIoTS device.

3. Chapter 2
Conceptual Framework and Related Works

In this chapter, we introduce some theoretical concepts and some technologies descriptions to understand this thesis's purpose. The first part (Background) of this chapter contains ideas and their descriptions as Food Traceability Systems, Internet of Things (IoT), security on IoT ecosystems, and Blockchain. The second part (State of the Art) contains the summary of the bibliometric analysis made to find research opportunities according to gaps and generalized issues found in our investigation area of interest.

3.1. Background

To offer a general context from the concepts and technological background for developing this thesis, we present an available description of the main ideas surrounding the Food Traceability Systems definition Based on Blockchain-IoT architecture.

3.1.1. Food Traceability

The global food trade has changed due to outbreaks of diseases transmitted from animals to humans, such as bird flu, swine flu, or mad cow disease. Consequently, food safety has become a priority for many countries, citizens, and the food industry [39]. Moreover, the challenge in agricultural traceability is to limit the use of chemicals in crops and promote agricultural quality and safety for consumers and value chain actors [40].

The main aim of traceability is to identify the origin of foods, the manufacturing process, the ingredients used, and most notably, discover the responsible party or parties whenever a product is in some way faulty [41]. Traceability systems enable us to locate, record, and trace products in the manufacture, processing, and distribution through platforms that offer access to users [7], for instance, Internet of Things platforms [8]. Such platforms promote quality in production, facilitate the identification of problems, and improve communication capacity between customers.

The countries that have established a standard for trading in agri-food products continue to extend the global production network based on ensuring food quality and safety [42,43]. The technological relationship between food production processes and informatics technology systems is overcoming connectivity problems. This is especially so when information may be accessed from virtually anywhere [44–46]. Traceability systems are characterized by operation in real-time and protect processes against risks and establish a priority throughout the value chain. These technological processes assure the necessary alerts in the process for reducing operating costs [46–48]. These systems can be effective, efficient, and profitable; for instance, they can reduce product losses, improve the identification process, and help all logistic processes and distribution operations. Nevertheless, there are still security issues to overcome [42, 43, 49].

3.1.2. Internet of Things (IoT)

Internet of Things (IoT) can be defined as a technological paradigm based on Internet connectivity, where the correlated computing devices, objects, animals, or people, are identified by Unique Identification (UID). These devices are set to satisfy necessities through some actions or to provide specific information for decision making in the efforts directed to services supplied by digital or mechanic machines [9, 10].

The supply-chain and value-chain established by the diagrams of the record-making, tracing, and tracking of food as a global trading network have a strong relationship with consumers and are growing new technological paradigms [42, 44, 49]. For instance, the IoT paradigm accommodates the majority of resources available to human service, in this case, to prevent diseases. The novelty in platforms such as these is the remote access to information in real-time. In this way, countries' populations are protected against diseases communicable by animals or poisoning products [45, 46, 48, 50]. New challenges arise today in the management of informatics security in communication systems. Food security demands new concepts of trust, and Blockchain is an obvious choice for further development.

3.1.3. Security on IoT ecosystems

The security of IoT ecosystems determines the quality of data linked to the communications and physical layer. An example of a physical layer is the hardware-implemented. Data quality can be affected due to various adverse factors such as radio interference, which can damage the connection for sending or receiving data [51, 52]. The mechanism of initializing or setting IoT devices guarantees the privacy of network services [53, 54].

The physical security of IoT devices depends on software access through physical interfaces. Another impacting factor on the usage of IoT devices is the energy consumption and management caused by battery duration on several scenarios where the distance, tasks, or functions are of high performance [55].

IoT architecture requires identifying the hardware devices on the network to guarantee data transmission with linked nodes. These nodes, many times, are routers or hubs managements. Nevertheless, security issues related to the transport layer need identification and to be matched to other platforms to send packets that can result in denial-of-service, and this is a genuine threat on IoT [56].

On IoT management systems, it is vital to authenticate the IoT devices to avoid security vulnerabilities. Recording of users and devices on an integrated platform help to minimize communication failures or attacks of security [57, 58]. The systems based on cryptography are an integral solution for security problems of network authentication and connection [59, 60].

Data transparency is a critical security issue within IoT ecosystems. To improve the communication process between peer devices, it might focus on solving data management from several technological schemes (fog or edge computing), but not always the transparency of information recorded is guaranteed. A current IoT system contains various devices with embedded sensors characterized by low power, reduced memory capacity, and limited processing capabilities. These features allow identifying the origin of significant security problems. Nevertheless, any solution concerning IoT devices' security capabilities is designed from the software that governs the management data, generally in the management layer of the system.

3.1.4. Blockchain

A blockchain record book consists of two types of records: individual records and blocks. The first block consists of a header and data that correspond to transactions within a set time. The block's timestamp is used to help create an alphanumeric string called hash [18, 61].

Once the first block has been created, each subsequent block in the book uses the hash of the previous block to calculate its hash [16, 62]. Before a new block can be added to the chain, its authenticity must be verified by a computational process called validation or consensus. At this point in the blockchain process, most network nodes must accept that the new block's hash has been correctly confirmed. The consensus ensures that all copies of the distributed book share the same status [16].

Once a block has been added, it can be referenced in subsequent blocks, but it cannot be changed. If someone tries to exchange a block, the hashes of the previous and next blocks will also change and interrupt the shared status of the ledger [16]. When consensus is no longer possible, other network equipment proves that a problem has occurred, and new blocks are not added to the chain until the issue is resolved. Typically, the block that causes the error will be discarded, and the consensus process will be repeated [61, 63].

Blockchain arrives at food traceability systems to resolve falsification of food products and raw material to manufacture. The authenticity that requires producers, researchers, consumers, and all other supply chain actors can be given through a tool where the involvement is secure. The distribution of security control to the stakeholders is generalized [16, 18, 62]. This technology will allow us to understand any product's origin or identify and address contamination sources in food products. This technology's principal aim is to avoid manipulating stored data of a food production process and alert consumers [62, 63].

The classification made by OWASP IoT Top 10 picks up the possible challenges that Blockchain technology can solve. Applying smart Blockchain-based contracts to IoT services represents an effective way to guarantee information security for maintaining data uncorrupted and providing data traceability. Nevertheless, some threats would be overcome from hardware usage and can provide higher capacities to Blockchain-based IoT systems.

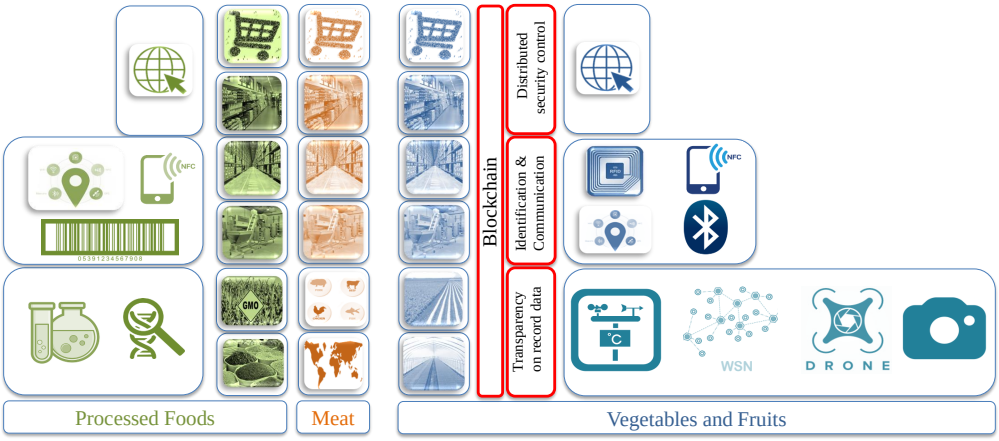


Figure 3-1.: Techniques and Technologies of the food traceability systems.

Fig. **3-1** shows an abstraction of techniques and technologies used by the food traceability systems on three action fields; processed foods, meat and vegetables, and fruits. The green column has six stages; two initial phases represent chemical and biological techniques as PCR, HPLC, and spectrometry for ADN isolating. These techniques and

technologies allow identifying diseases and viruses. Two initial stages on the Blue column mean the wireless sensor network (WSN), cameras, drone, and weather stations. The red column corresponds to meat traceability; this field uses all scientific techniques and technologies to track and trace meat products. The third and fourth stages in all columns indicate the technologies that allow sensing or trace the raw materials, processed products, or fresh products(RFID, Barcode, NFC). Finally, the last stage means the connection between the products and customers. Today such a platform is the internet.

The three red boxes in Fig. **3-1** indicate the way as Blockchain technology influences each stage of the agriculture supply chain. The transparency on a record data resource is promoted through information stored in the blockchain blocks on the network from the sensors. This resource modifies the identification and communication form between devices. It helps overcome the possible security problems on the IoT system, described in the next section, providing a context of a security solution with Blockchain on IoT ecosystems. Finally, data management's capacity through distributed networks of data guarantees the data traceability and ensures the transparency of the information [36, 64].

3.2. Related Work

This section presents a part of the scientific evolution analysis of the food traceability area through the keywords used in its historical development of the last 19 years. Food safety problems are becoming more strategic and further promoting the research for solving from the technical overview. For this reason, it is critical to identify areas, sub-areas, and fields that can to suffer evolutions or to decline, that emerging or disappear, and an excellent way to evaluate it can be through science mapping.

This science mapping lists a series of scientific community responses in several academic areas - techniques, technologies, and methods. Moreover, it includes the gaps and research opportunities that offer many areas identified as critical, particularly for proposing keys to the future of food quality and safety, an element that none review work contains. The analysis allows us to identify the impact on the scientific productivity of the field, discover the dynamics of relevant published research, and find the most prominent areas as they vary with time. The primary source of information used in this analysis is the Web of Science bibliographic database, employing SciMAT as a software tool to make the science-mapping. The Bibliometric review was carried out with a dataset of 2,289 documents published over the (2001-2019) period. The study provides a perspective according to the strategic map, evolutionary map, and main strategic clusters identified for future research.

A scientific Journal evaluates this bibliometric analysis as a global panorama of food safety from a technological viewpoint. The analysis is divided into four sub-periods. Hereunder, we describe part of the last sub-period summarizes the main topics identified as a future trend, the critical gaps, and research opportunities that made this proposal possible. The second part of this section presents the proposed solutions in works related to security issues on Blockchain-IoT ecosystems.

The evaluation of incident topics in food traceability was structured as follows. The study period of 19 years (2001-2019) was divided into four sub-periods, organized according to the incidents of highest impact related to outbreaks and epidemics in humans by consuming food products of animal origin and the poisoning of vegetables (Agriculture). Moreover, were identified the techniques and technologies used on the FTS.

The bibliometric analysis identifies the areas, subareas, and highlighted topics to guide the present research. The study was made with 2289 bibliometric references and divided as we can observe in Fig. **3-2**. Fig. **3-3** shows the paper amount per area that was reading in looking up of gaps for researching. Moreover, table. **3-2** shows results related to Blockchain-IoT and Supply chains (Traceability Systems) on diverse domain fields. Web os Science (WoS), Scopus, Elsevier, and IEEE was used as a database of bibliometric references.

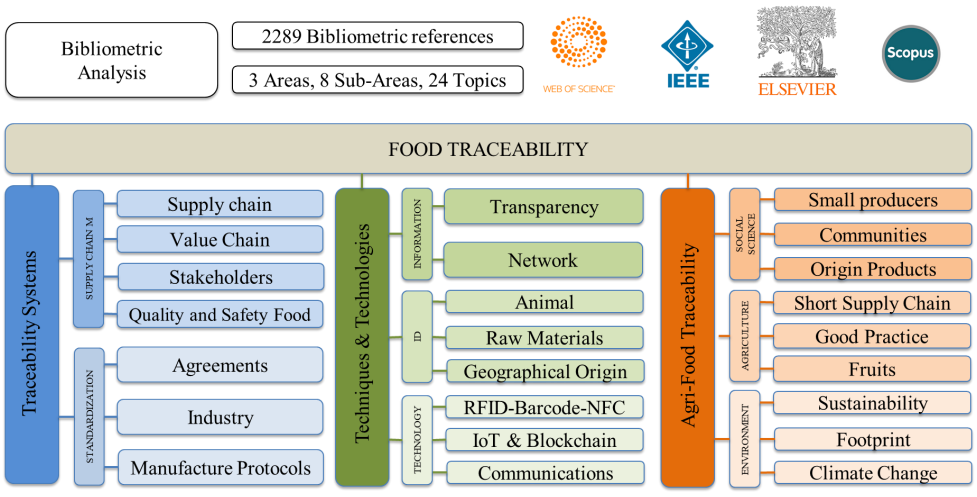


Figure 3-2.: Bibliometric Analysis Areas.

Table. **3-1** shows the possible directions of research that give; as a result, science mapping, and these directions are determined mainly for the gaps found in the content of documents on this review. The scientific need of the technology and theories applications can be perceived from the issues identified in each studied area. Once the strategic papers per area and sub-period were read, eight clusters were selected, which correspond

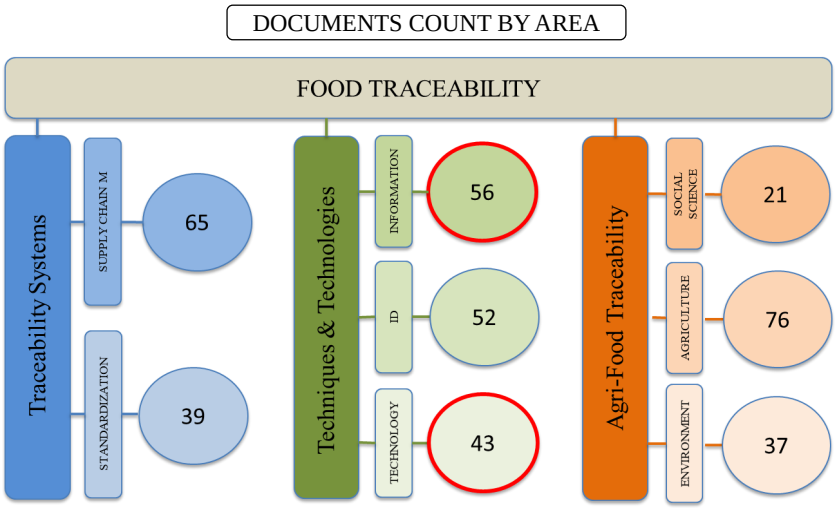


Figure 3-3.: Documents Count by Area of Bibliometric Analysis.

to sub-areas that will summarize the gaps and direct the researcher to new opportunities of inquiry.

The first area found was IDENTIFICATION; despite existing techniques and technologies advanced for food identification, these systems do not reach the level of developing countries or places where supply chains' applications are precarious. Therefore, any food production systems that desire to acquire a food traceability system based on genetic tester's chemical characterization to guarantee products' safety and quality will have a problem to overcome. Mainly due to the equipment cost and the scientific knowledge in the domine of some technologies.

The second area identified was INFORMATION. In most study cases, the information systems analyzed are simulated or proposed as a framework with technologies and resources that are not yet available or are going through a development process. Nevertheless, the internet and sensors make easy the implementations of particular cases where the deployment is not complex. Furthermore, the only countries with actual capacities for applying robust systems are developed countries as EEUU, China, or some European countries. It must be taken into account that traceability should be complemented with other strategies for managing the food quality, such as GAP (Good Agricultural Practices), GMP (Good Manufacturing Practices), and HACCP (Hazard Analysis Critical Control Points); because traceability is a mean of monitoring, it is not a mechanism to eliminate physical, chemical and microbiological risks in food. The traceability informs us of where the product is obtained; it has the details of its production, handling, and distribution; but there is no guarantee that it is harmless.

Area	Gap	Research opportunity
Identification	Lack of preventive measures for identifying the origin of the products without backward-traceability technological tools.	To focus on backward-traceability techniques for adopting preventive measures in food systems that currently lack storage technology or scientific knowledge.
Information	Lack of transparency in the information submitted to the consumer or the supply chain actors throughout the production process.	To explore the design and deployment of informatic security tools to guarantee a traced product's authenticity and reliability.
Technology	Lack of hardware dispositive associated with several processes within the food traceability chain to assure the record and modify the content of information throughout the supply chain.	To design a framework where the cooperation between dispositive and traceability platforms set the supply chain management structure.
SCM	Lack of financial inclusion mechanisms for short supply chain and the specific products, this field its dominated for modeling and simulations without fault control.	To identify critical products in regions that have the potential for certifying processes and validate technologies to the supply chain management.
Standardization	The industrial standards and existent protocols for food systems and traceability schemes have a complex design with low capacity for short supply chains.	To propose a supply chain or food traceability system based on international standards but according to the particularity of species and amount produced in each country.
Environment	The supply chain and food traceability systems have no yet been designed with an environmental sustainability focus or social impact. With the association of minority groups, ethnic or native communities.	To focus the design of supply chains towards environmental sustainability with trade and social impact that involve cooperative sectors of the peasant, natives or women.
Agriculture	The study cases analyze the extensive agriculture beneath the domain of precision agriculture. Nevertheless, these models have not been applied to focus on e-commerce.	To explore options of e-commerce for not manufactured products to eliminate the cost overrun for the consumer.
Social sciences	The socio-cultural characterization of countries where they have implemented food traceability systems do not guarantee homogeneity in safety and quality of food products.	To characterize producer populations, potential regions, and trade channels for products with the origin denomination, besides to convene for joint production strategies between industrials and researchers.

Table 3-1.: Gaps and Research opportunities.

The third area identified was TECHNOLOGY. When the use of technology is generalized for several applications, principally for food traceability or industrial food systems, technologies as the barcode, QR code, RFID (Radio Frequency Identification), WSN (Wireless Sensor Network), ANN (Artificial Neural Network), to name a few, the software and hardware have a certain match. Still, they do not guarantee compatibility, although the international agreements and standards require it, making it hard to articulate between industries or countries. Additionally, the hardware devices are not yet related within the scheme of food traceability systems and industrial food processes for guaranteeing trust.

The fourth area identified was SCM (Supply Chain Management). Although this area is different from Supply Chain (SC), we can say that one contains the other. SCM includes all logistic processes and industrial production. For this reason, we assume as a challenge the improvement of the SCM.

One of the principal issues found is the lack of a classification of supply chains, where there exist standards and protocols for a short Supply Chain of products that do not need long and complex treatment in the production chain. The industrial standards are made for mass production. Despite the many alternatives to guarantee the consumer's willingness and the harmlessness of products, the security, and quality in the manufacture or handling of food products are not entirely transparent. For this reason, technologies as the blockchain try to assure supply chain safety.

Blockchain arrives at food traceability systems to resolve falsification of food products and raw material to manufacture. The authenticity that producers, researchers, consumers, and all other actors of the supply chain require can be given through a tool where the involvement is massive and where the distribution of security control to the stakeholders is generalized. This technology will allow us to understand the origin of any product or identify and address contamination sources in food products. This technology's principal aim is to avoid the manipulation of stored data of a food production process and alert the consumers.

The fifth area identified was STANDARDIZATION. This area presents issues in how the standards are handled and imposed on countries and industries that desire entry into food trade agreements between countries. The regions, continents, or countries establishing your standards for commercing food products, not all have the same parameters.

Standardization processes are vital because the raw materials are always of biological origin (produced by animals or plants). However, the product must always be similar to meet the consumer's needs and ensure their loyalty. In this sense, traceability is an element that facilitates the standardization of processes in the food industry, establishing mo-

re significant links between producers, processors, and consumers. While the standards and protocols are not universal and installed according to each country's conditions or product, it will have a complex standardization of food and traceability systems.

The sixth area identified was ENVIRONMENT. Many industries do not focus on sustainability practices and propose theories or frameworks to apply the SCM without a sustainable approach. The soil use and climate change are not part of the food traceability scheme stamp to food production.

When carrying out detailed monitoring of the conditions of food production in the field, from the supply of inputs, planting, harvesting or harnessing, post-harvest, storage, and transport; As well as the conditions of processing, distribution, and consumption; allowing to estimate actual costs of production and logistics in the chain; also recognize bottlenecks and propose optimization alternatives. The previous analysis is also a reference for calculating the environmental effects of the functioning of food chains (carbon footprints) and suggest options for improvement.

The seventh area identified was AGRICULTURE. In developing countries as Colombian, this factor is critical in the willingness of people. The lack of establishing short and adjustment supply chains for tropical products and particular aspects in the production do not count with details. However, precision agriculture applications in fields as coffee can serve as an example for guiding other action fields, not including small groups of women or peasants in the agri-food supply chains. In every case, the design of SCM is building for industries, not for small producers.

A way of positioning food products in any country's external or internal trade is visibility, recognition by origin, mark, or biological product features. These positioning ways applied in massive use platforms become an opportunity to boost e-commerce and all its advantages. We find the benefits of avoiding intermediaries, speeding up the business process, promoting transparency, and ensuring product origin.

The last area identified was SOCIAL SCIENCES. In the major countries that apply modern food traceability systems and complex schemes of food safety supervising the commerce and the local production for assessing the need of consumers, considering the social impact of measures economics, of governance and politics around to food systems.

This proposal originates in the INFORMATION and TECHNOLOGY areas identified in the bibliometric analysis because, despite existing communication techniques and technologies to apply in the FTS [65], these systems do not reach the required level of security to guarantee the data transparency recorded by the sensor on the IoT ecosystems [66–68].

This data transparency leads to the product's quality throughout the supply chain and promotes consumers' food safety.

Table. **3-2** shows the summarize of relevant works that serve as a reference to the present proposal. These works present some valuable features to the hardware development proposed into Blockchain-IoT architecture. Despite the many alternatives to guarantee the consumer's willingness and the harmlessness of products, the security and quality in the manufacture or handling of food products are not entirely transparent; for this reason, technologies as the blockchain try to assure supply chain safety [69].

Blockchain arrives at food traceability systems to resolve falsification of food products and raw material to manufacture. The authenticity that producers, researchers, consumers, and all other actors of the supply chain require can be given through a tool where the distribution of security control to the stakeholders is generalized [70]. This technology will allow us to understand the origin of any product or identify and address contamination sources in food products. The principal aim of this technology is to avoid the manipulation of stored data of a food production process and to alert the consumers [71].

A way of positioning food products in any country's external or internal trade is visibility, recognition by origin, mark, or biological product features. These positioning ways applied in massive use platforms become an opportunity to boost e-commerce and all its advantages. We find the benefits of avoiding intermediaries, speeding up the business process, promoting transparency, and ensuring the product origin [64, 72].

Fig. **3-4** shows the graphical abstraction between the timeline, fields of application, and food safety systems evolution. The terms that contain the circles born of each cycle of growth denoting techniques, technologies, and products that stamp the behavior of the world's food systems. Some acronyms that contain the figure are; SCM (Supply Chain Management), VC (Value Chain), ANN (Artificial Neural-Network), WSN (Wireless Sensor-Network), IoT (Internet Of Things), ASC (Agri-Supply Chain), GTIN (Global Trade Item Number), SSCC (Serialized Shipping Container code number), GMO (Genetically Modified Organism), PCR (Polymerase Chain Reaction), HPLC (High Performance Liquid Chromatography).

Author	Title	Description
Feng Tian (2016) [73]	An Agri-food Supply Chain Traceability System for China Based on RFID and Blockchain Technology.	This paper develops a hybrid concept of RFID (Radio-Frequency Identification) and blockchain technology. However, they do not develop the hardware related to the application of these technologies.
Tareq Ahram, et al. (2017) [74]	Blockchain Technology Innovations.	This article describes the Blockchain technology used in the healthcare industry, Health-chain. It does not refer to the use of IoT devices acting directly on Blockchain technology.
Simone Figorilli, et al. (2018) [75]	A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood along the Whole Supply Chain.	This work implements a blockchain architecture in the traceability system of the wood value chain. The sensors are managed apart from the blockchain architecture through an intermediary hub device. The Infotracking system is based on RFID and others IoT devices open source.
Oscar Novo (2018) [76]	Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT.	This paper proposes a new architecture for arbitrating roles and permissions in IoT. This a fully distributed access control system for IoT based on blockchain technology. The architecture is supported by a proof of concept and evaluated in realistic IoT scenarios.
Ali Dorri, et al. (2018) [77]	Blockchain in Internet of Things: Challenges and Solutions.	This paper proposes a hierarchical IoT architecture applied to smart homes, an overlay and cloud storage network that coordinates data transactions with Blockchain, to provide privacy and security.
Pascal Urien (2019) [38]	Blockchain IoT (BIoT): A new direction for solving Internet of Things Security and trust issues.	This paper proposes to insert the sensor data in blockchain transactions. The objects are not logically connected to blockchain platforms. Therefore the controller entities forward all information needed for transaction validation. Here build a Hub device.

Table 3-2.: Reference works.

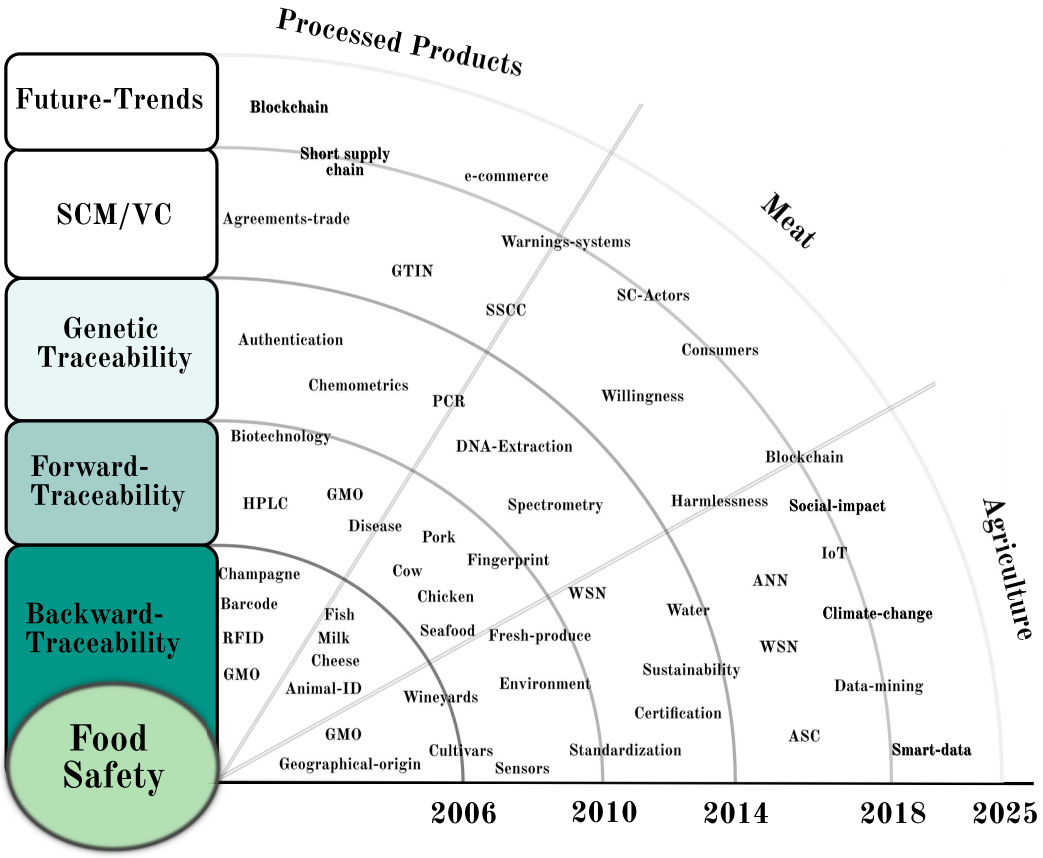


Figure 3-4.: Evolution of food Systems and the food traceability.

3.2.1. Research opportunity

The security threats in IoT ecosystems can be solved through various architectural elements; some of these are hardware, interfaces or apps, software, network components, and firmware. Nevertheless, most security problems have a solution with the blockchain architecture implementation upon the IoT ecosystem. Nonetheless, the sensor will always be the source of mistrust on transferring data to the cloud or storage. Hereunder we describe some solutions found on the review, but none of them proposes to build a hardware device for promoting the transparency of data recorded from the sensor [36].

Fig. **3-5** shows the two possible paths to data streaming, recordkeeping, and share information into an IoT ecosystem. Path 1, in blue, represents a conventional flow of data in IoT. S(n) represents the sensors that are part of the network for capturing variable data. These sensors are connected between them and, at the same time, with a hub manager for transmitting to the cloud or storage. Along path 1, between sensors and hub, and between hub and cloud, most security problems on IoT are related to the streaming data's

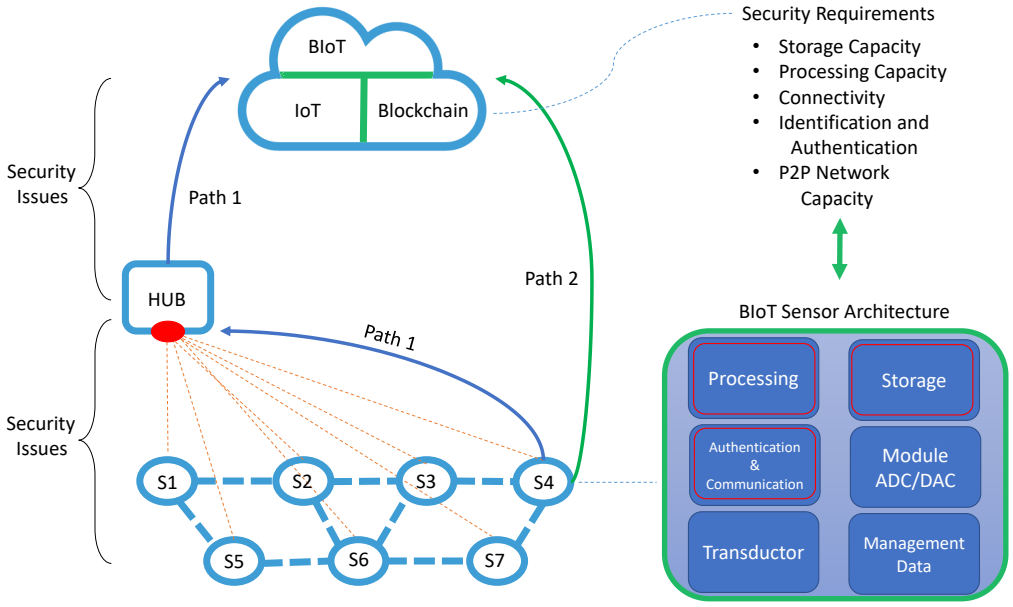


Figure 3-5.: BIoT Architecture.

vulnerability. Path 2 proposes to benefit from the security requirements of Blockchain architecture and match them with the IoT sensor architecture to solve most of the security problems related to the transparency of data in the streaming process. In the IoT Device (Sensor) architecture, the three boxes in red correspond to the aspects that ought to be improved for being able to act on the BIoT architecture.

None solution described refers to building hardware with new security capabilities to act on blockchain architecture to promote transparency upon data collected and transmitted by the sensor. The above-referenced works on table. **3-2** , serve to identify the opportunities to apply some techniques and technologies in the IoT device. Only one work [23] developed a hardware device for connecting it with blockchain systems. Nevertheless, this device does not guarantee the reliability of the information according to the blockchain architecture's security requirements for acting as a miner actor. The remaining works use the IoT devices as an independent actor in the blockchain architecture. For this reason, they use a hub for managing the communication process with the sensors.

The works hereunder propose solutions that are insufficient to solve most security problems on IoT ecosystems. However, some techniques are aimed to solve particular security issues but can serve as a reference to develop new hardware capabilities for an IoT device to act on a blockchain-based system.

Security problems like Jamming attacks are considered minor problems. Nevertheless,

the message collisions and errors on the sending of the packages are solved in [78], where they measure the signal to extract the noise, then compare these measures with customize threshold measurements and detect the attack. Other solutions against a jamming attack use cryptographic functions to help correct errors [52]. Others suggest avoiding the jamming attack with encoded packages through a division of the message into blocks or changing channel frequencies for the communication flow to be successful [79].

The security on the physical communication layer through the initialization of IoT platform, many works proposes a framework to protect the system [80]. Other works deploy artificial noise in signals inside communication networks [53, 81]. Sybil attack is a security problem upon the network nodes that use MAC identification values for accessing to IoT platform. These security issues result in denial of access to legitimate devices on the network. Some solutions proposed using strength measurements of signals for detecting and correcting the attack [82]. In static networks, some works suggest using signals with strength measurements for MAC addresses to detect attacks upon Sybil nodes [83–86].

(OWASP) The Open Application Security Project discusses the IoT devices as physical objects into IoT networks with its security through software/firmware access with external interfaces. These features make it vulnerable to different security attacks. Some works propose a Trusted Platform Module (TPM) incorporated into the system regarding physical security improvement on the network. Moreover, some evaluate the attacks upon Wireless Sensor Networks (WSN), where it is suggested to mitigate sleep deprivation and to reduce the energy consumption through framework [87]. Nevertheless, these measures are insufficient to avoid intrusions on the WSN.

Some solutions propose the modification of authentication protocols with cryptography algorithms for detecting malicious nodes in security attacks. Nevertheless, the RPL standard also computed the parent's rank value with other nodes according to the calculated value based on rank [88, 89], and this is considered as a novel solution.

3.3. Conclusions

Ever since 2001, incidents with animal diseases transmitted to humans have opened up possibilities of finding solutions in all areas of human knowledge. This work thus guides researchers and readers in studying the past, evolution, and future of the food traceability field. It presents an analytical panorama of the patterns and trends of the related research topics.

The analysis results show that the production of knowledge across the sub-periods has increased in the field of food traceability. The results reflect the high degree of maturity of the areas and topics related to the field. Most areas have a high development degree, taking into account the social, cultural, and political needs of countries around food's healthiness. Indeed, the constant evolutionary trend exists in the four sub-periods through the concepts, techniques, and technologies used for food traceability systems. The behavior of the transient keywords allows us to identify successes and gaps in the new research opportunities.

Furthermore, we can observe that the supply-chain and the value-chain of any product ensure quality and safety, in addition to establishing the basis of all traceability systems. For this reason, the first step in the challenge toward food safety and quality must be the analysis and study of the actors in the value chain, the human and material variables involved, such as information systems, policies, trading standards, and technical and technological aspects.

The sub-periods strategic maps were analyzed to enable a clearer picture of the patterns and trends of the agri-food areas. The areas appear and disappear, evolve or regress according to the research's maturity in those fields and the preventative strategies for ensuring harmlessness of foods achieved around the world through information systems. The measure of the accuracy of traceability systems is the occurrence of epidemic events.

The supply-chain and value-chain established by the record-making diagrams, tracing and tracking food as a global trading network have a strong relationship with consumers and growing new technological paradigms. For instance, the IoT paradigm accommodates the majority of resources available to human service, in this case, to alleviate, protect, and prevent diseases. The novelty in platforms such as these is the remote access to information in real-time. In this way, countries' populations are protected against diseases communicable by animals or poisoning by agri-chemicals. New challenges arise today in the management of informatics security in communication systems. Food security demands new concepts of trust. Blockchain is an obvious choice for further development in this regard.

Academia, principally researchers, pursues innovative solutions thanks to the high degree of maturity of food traceability areas. However, many private and public organizations worldwide have adopted platforms in which improvements can always be made. In other words, the bibliometric study provides vital information to benefit the platforms devoted to food safety. Furthermore, intelligent systems advance in providing services to the extent that the information promotes the world of business. IoT platforms gather most of the solutions in diagrams such as smart cities, food safety, and trade agreements with

consumer participation.

The keywords represent the most significant element in the topics of each period in the evolution. They show the principal aspects of the development of the food traceability field toward the sub-period of reference. The academic environment has built a stage in which all terms are strongly related to guarantee the systems of food harmlessness. Although all the keywords are essential, the timeline relates quality with information, with the value-chain, and with the supply-chain summarizes one of the food safety commitments.

4. Chapter 3
Research Problem Context

IoT can trace or track food products, store and process critical data for recording the process; nonetheless, it is not entirely safe in terms of transparency of data stored. Blockchain, beyond the crypto-currencies and the business, can certify processes transparently through the data traceability.

The ability to certify the processes into the food supply chains through the data integrity collected of end-to-end connection points and contained in the Blockchain-IoT architecture reveals BIoTS device's aim. End-to-end connection points in the IoT architecture indicate the sensor's path to the cloud service (Vertical). Simultaneously, the path from the first stage in the traceability system to the last stage (Horizontal). See Fig. **4-1**.

Combining two disruptive technologies involves identifying the problems they face in applying in food security and then finding the architectural features that make the coupling possible.

4.1. Food Traceability Systems Blockchain-IoT-based

Fig. **4-1** presents the abstraction of the Blockchain-IoT-based traceability system architecture. The figure is displayed over three axes; x, y, z. On the z-axis are the six conventional stages that a food traceability system has. In this case, each stage is equipped with devices and technologies that make it possible to track the variables involved in the production process. This deployment is done in the perception layer of the architecture. The red dot represents where tracing (backward traceability) or tracking (forward traceability) is intended to be done along the supply chain stages. In the perception layer and along the z-axis, the coverage, type of network, and infrastructure required for traceability are configured. On the x-axis of the figure, we can see the origin and destination of the data generated in the physical layer of the architecture (red dot). The data collected depends mainly on the devices deployed in the sensing layer and the transport layer setting.

The y-axis of the figure shows the infrastructure required to transmit data from its origin to the end-user. Above the perception layer is the transport layer. This layer manages the

system according to the network characteristics and the physical devices, and the communication channel required to secure data transport. Features such as interoperability, energy, storage, processing capacity, and security are evaluated to define levels of scalability, robustness, accessibility, and security. Finally, in this axis, we find the application layer. This layer deploys the public access service to the data managed along the x, y, and z axes. These data move in the three directions in a coordinated manner to reach the end-user and thus certify processes or products. However, some features of IoT devices can be improved to ensure data integrity throughout the process of transporting information across all layers of the architecture.

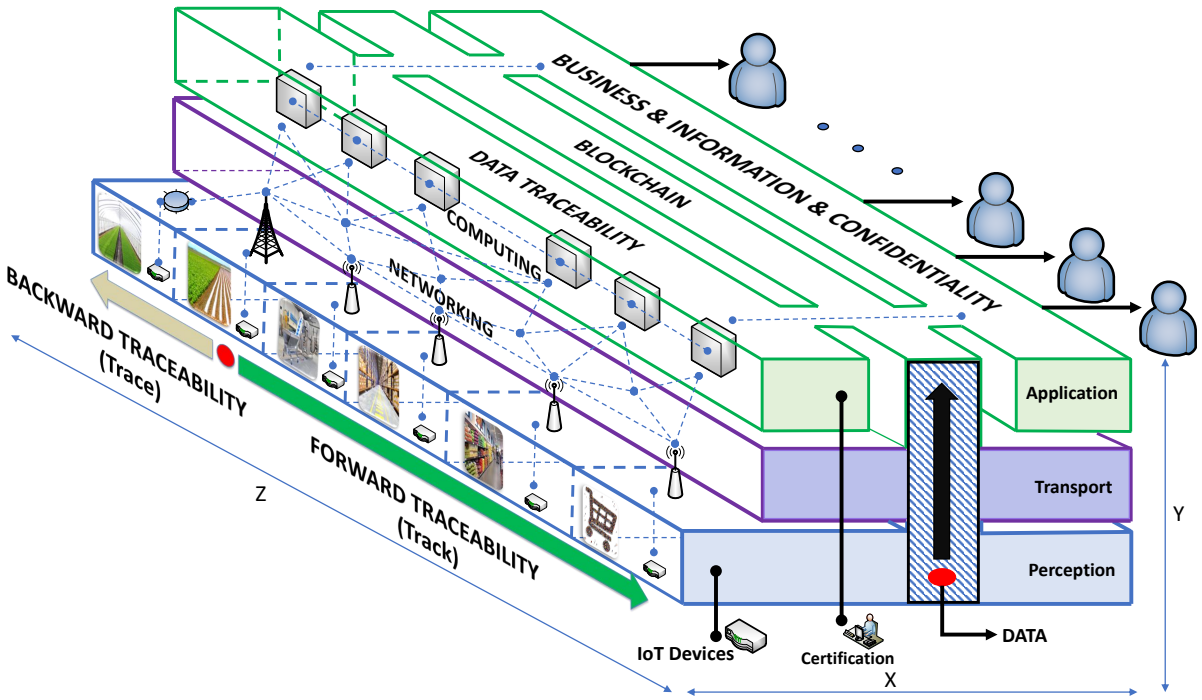


Figure 4-1.: The Blockchain-IoT-based food traceability systems.

Blockchain technology is defined as a disruptive technology that imposes a new paradigm that can connect securely way to the world throughout the network. Blockchain technology can describe as a platform where the transactions and the information recorded are safeguarding through cryptography algorithms in a distributed ledger to all participants of the network [90–92].

All food fields apply some techniques and technologies within reach effective to evaluate food safety. Nevertheless, they are insufficient because all countries do not have capacities to deploy them.

IoT represents an opportunity to apply Blockchain technology as a support to guarantee security in some respects [93, 94]. As we can see, Blockchain technology is called to resolve significant problems of connecting, support, protecting businesses and stakeholders participating in food traceability systems (Supply Chains or Value Chains).

4.1.1. IoT security issues and challenges

Due to the range of services provided by objects, persons, or machines into the IoT networks, it is mandatory to equip both networks and devices with security features.

The standard communication protocols define the rules and security techniques in IoT networks. Fields such as health, financial security, or food safety handle processes with sensitive data that require transparency and integrity in their handling. But the adverse factor is that as long as the IoT network design is done on the Low-Power and Lossy Network (LLN) network scheme, security will have that measure; that is, the device immersed in the IoT network will not have security properties beyond those allowed by its capabilities.

4.1.2. Overview of security issues on IoT

The identification of security issues on IoT is so extensive that it generally is made from the field of application. Also, the field of application imposes safety criteria focused on the user and the system architecture. This hierarchy in the identification of security problems helps to identify comprehensive solutions and technologies.

Due to the technology's capacity with which the build of BIoTS device proposed in this work, it is possible to identify the problems attending the two perspectives (Application and architecture), because of its implementation answers integrally to the IoT security problems. For this reason, this section presents the findings of some security problems keeping a mixed approach between the security requirements of the application field and the IoT architecture.

The scheme in Fig. **4-2** shows a map of security problems in IoT, which identifies in a general way the issues that affect the IoT-based food traceability systems and focused on food safety and quality. This scheme is based on three works that propose taxonomies for identifying security issues on IoT [36, 95–97]. The following list describes the two perspectives from which security issues in IoT ecosystems have been mapped.

- Application Field Perspective: On the left of the scheme, food safety as an application field, establishes the three layers of IoT architecture as a channel to guarantee

data and product traceability in the communication process throughout the IoT system.

- Architecture Perspective: In the upper part, the IoT architecture (Perception, Transport, and Application) establish as the central axis in the identification and classification of security problems.

The implementation of BIoTS aims to solve the security problems described here. Each layer in the IoT architecture has issues that the technology on which BIoTS-based solves. The issues identified here are not part of the security problems faced by Blockchain. However, they are different, and their management depends on specific measures in the application design.

The Datagram Transport Layer Security (DTLS) and Transmission Control Protocol (TCP) communication protocol govern IoT systems' conventional security architecture in standard networks. In the IoT application layer, the Constrained Application Protocol (CoAP) and Hypertext Transfer Protocol (HTTP) communication protocol establish the interchange of information.

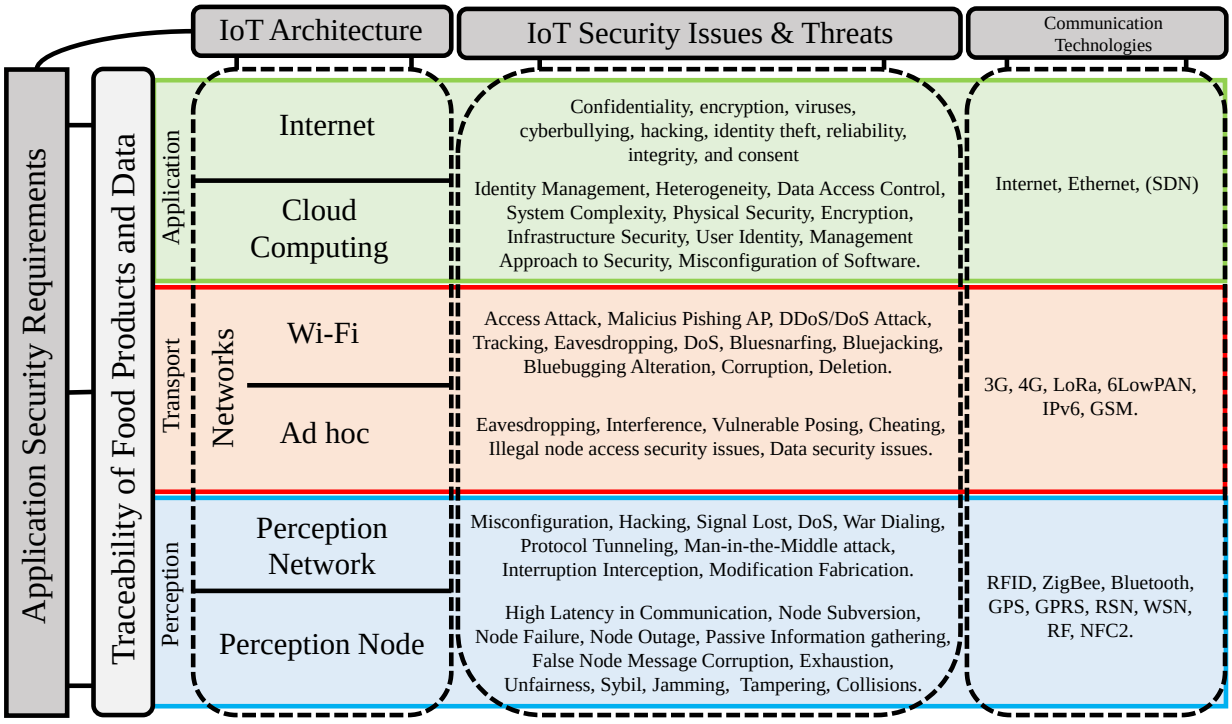


Figure 4-2.: IoT Security Issues and Threats.

1. **Perception Layer**: In this layer, where the devices that interact with the medium are hosted, we list and describe some security issues that BIoTS can solve in two scenarios; a) In sensor nodes and b) In sensor gateways. a) In the sensor nodes case,

to make possible the process of sensing and interconnecting with other nodes, they have these components; a controller, a transmitter (for communication), a memory where the device storage the program (code), a power source, and the hardware that obtains the sensed data. At this level, you are prone to security problems such as; node subversion, node failure, node outage, passive information gathering, false node message corruption, exhaustion, unfairness, Sybil, jamming, tampering, and collisions. b)For sensor gateways, the collection of information on WSN represents a problem because the wireless communication channel involving radio communication and its possible appears problems such as; misconfiguration, hacking, signal loss, DoS, war dialing, protocol tunneling, man-in-the-middle attack, interruption interception, and modification fabrication. As you can see, in both cases, all security problems are aimed at attacking the trust, privacy, and integrity of the transmitted data.

2. **Transport Layer**: To solve some security vulnerabilities associated with the network type, BIoTS acting in a Blockchain-based IoT network. The networks generally used for food traceability systems are two; a) WiFi-centric network and b) Ad-hoc non-centric network. For this reason, BIoTs and your ecosystem pretend to solve some security issues as; a) In a WiFi network, attacks such as access attacks, malicious phishing AP, and DDos/Dos attacks. b) In IoT, an unfocused Ad-hoc network is a Peer-to-Peer network. The traditional problems in this nature's networks have to do with the communication channel's vulnerability—attacks such as Eavesdropping, interference, vulnerable posing, cheating, Man-in-the-Middle (MitM).

3. **Application Layer**: In the food safety scenario, millions of users are expected to access sensitive information on edible products. Data confidentiality and traceability is the anticipated contribution of BIoTS in the network deployed for its operation. The ecosystem is expected to contribute to security issues associated with authentication and access authorization. Besides, process safety management within a supply chain based on certification through Blockchain Smart Contracts is expected.

4.1.3. Summarize of solutions

Afterward, we present some security issues in terms of architecture and information and some works that pretend to solve them. All proposals focus on IoT classify security problems and describe the main security issues in communication within IoT systems [36, 95–97].

All IoT architectures evaluate their security through parameters such as privacy, integrity, and confidentiality of data. As long as IoT networks connect heterogeneous low-capacity devices, data collection will present security problems associated with computer

networks. For this reason, when designing an IoT network, the level of security that the system will have is also intended.

The Transport and Application layers of the IoT architecture described below concentrate most of the proposals to solve information security problems [17, 98]. However, the coverage of these designed measures does not include the end-to-end aspect (to Perception layer) of the vertical and horizontal path described above [38, 90].

The Internet as a connection standard allowed bandwidth management and gave rise to connection management and device communication processes in the IoT network. Concepts such as Machine-to-Machine (M2M), Wireless Sensor Networks (WSN), and Cyber-Physical Systems (CPS) emerged. With them, security problems in the IP protocol grew due to updating security attacks while expanding the fields of action of IoT.

According to the most frequent security vulnerabilities in [36] were identified and classified IoT security issues. Summarizing the security threats of IoT-Systems, some works rank these threats as challenges in the security field and propose a hierarchy of security issues; i) Low-level security issues highlight the insecure initialization, insecure physical interface, or jamming adversaries. ii) Intermediate-level security issues highlight the insecurity of network connectivity between devices, authentication, non-secure communication on end-to-end transport-level security, and privacy violation on cloud-based IoT. iii) High-level security issues highlight CoAP safety with the Internet, insecure interfaces, insecure Software/firmware, and middleware security. Some emerging technologies, like Blockchain, can solve the majority of security problems present on IoT ecosystems, a fact that makes possible a new Blockchain-IoT (BIoT) concept.

Generally, networks based on IoT may suffer identity violation and information privacy issues, such as the services related to cloud, storage, transmission, or processing [99]. Security systems on the Internet about Constrained Application Protocol (CoAP) suffer security attacks from the application layer [37, 100], this fact makes the web, mobile, and cloud interfaces vulnerable as those indicated in (OWASP IoT top 10).

Security problems like Jamming attacks are considered minor problems. Nevertheless, the message collisions and errors on the sending of the packages are solved in [78], where they measure the signal to extract the noise, then compare these measures with customize threshold measurements and detect the attack. Other solutions against a jamming attack use cryptographic functions to help correct errors [52]. Others suggest avoiding the jamming attack with encoded packages through a division of the message into blocks or changing channel frequencies for the communication flow to be successful [79].

Sybil attack is a security problem upon the network nodes that use MAC identification values for accessing to IoT platform. These security issues result in denial of access to legitimate devices on the network. Some solutions proposed using strength measurements of signals for detecting and correcting the attack [82]. In static networks, some works suggest using signals with strength measurements for MAC addresses to detect attacks upon Sybil nodes [83–86].

(OWASP) The Open Application Security Project discusses the IoT devices as physical objects into IoT networks with its security through software/firmware access with external interfaces. These features make it vulnerable to different security attacks. Some works propose a Trusted Platform Module (TPM) incorporated into the system regarding physical security improvement on the network. Moreover, some evaluate the attacks upon Wireless Sensor Networks (WSN), where it is suggested to mitigate sleep deprivation and to reduce the energy consumption through framework [87]. Nevertheless, these measures are insufficient to avoid intrusions on the WSN.

The security threats in IoT ecosystems can be solved through various architectural elements; some of these are hardware, interfaces or apps, software, network components, and firmware.

4.2. Security on The IoT-based Food Traceability Systems

Most sensors in IoT-based Food Traceability systems will have some features as; interoperability, energy, size, position, and communication. These features make possible the ubiquity term and make the procedure a lightweight system to adapt secure form between them to deploy a service in any context.

In the food processing industry, biosensors, capable of identifying pathogens in contaminated products, have gained relevance. For this reason, this proposal attempts to focus on the construction of a sensor-equipped with a technology (Blockchain) capable of guaranteeing data integrity and transparency in the transmission of information.

Table. **4-1** presents the characteristics and configuration of the system by each layer of the IoT architecture, identifying the challenges and threats in security. This table describes the IoT ecosystem's technical and technological features in which BIoTS will perform to ensure product and data traceability.
The works listed in the table above define the roadmap for working in agricultural product traceability security and helps to relate security vulnerabilities, scientific work, and th-

Architecture Layer	Threats in Security	weaknesses	Related Works	Attacks
Application Layer				
Internet	Confidentiality	Energy Consumption, Storage Capacity	[71], [101], [38], [102], [103]	51 Percent, Pishing, Malware
Transport Layer				
Wireless	Rogue access points, Misconfiguration	Hacking, Signal lost	[104], [105], [106], [104], [107]	DoS, War dialing, protocol tunneling;man-in-the-middle
Perception Layer				
Sensor Nodes	DoS, Exhaustion, Unfairness,Sybil	Flooding, Routing Protocols	[108], [109], [110], [111], [104], [112], [113]	Jamming, Tampering, Collisions

Table 4-1.: Security Issues, Threats and technologies.

reats. Technologically and conceptually, we focus on the problem and evaluate alternative solutions [114, 115].

4.3. Conclusions

The security on IoT ecosystems determines the data quality linked to the communications and physical layer. An example of a physical layer is the hardware-implemented. Data quality can be affected due to various adverse factors such as radio interference, which can damage connection for sending or receiving data [51, 52]. The mechanism of initializing or setting IoT devices guarantees the privacy of network services [53, 54]. The physical security on IoT devices depends on software access through physical interfaces. Another impacting factor on the usage of IoT devices is the energy consumption and management caused by battery duration on several scenarios where the distance, tasks, or functions are of high performance [55].

IoT architecture requires identifying the hardware devices on the network to guarantee the transmission of data with linked nodes; these nodes many times are routers or hubs managements. Nevertheless, security issues related to the transport layer need identification and to be matched to other platforms to send packets that can result in Denial-of-Service, and this is a genuine threat on IoT [56].

On IoT management systems, it is key to authenticate the IoT devices to avoid security vulnerabilities. Recording of users and devices on an integrated platform help to minimize communication failures or attacks of security [57,58]. The systems based on cryptography are an integral solution for security problems of network authentication and connection [59, 60].

5. Chapter 4
Proposal Development

This chapter describes the features of BIoTS device architecture and design-implementation of Blockchain-Network, which allows us to define the necessities of functioning to design a Blockchain-IoT system. Then, we make a description of some architectural modules of the system.

Most sensors immerse in the IoT ecosystem, further measure some variables, have some capacities to provide security. Nonetheless, it does not guarantee specific security requirements for low processing, energy, and storage capabilities.

These reduced capacities make the lightweight of the IoT systems and guarantee the ubiquitous characteristic of the system. However, reducing the size of the devices (sensors) present in the IoT ecosystems conflicts with the entire system's security capabilities. For this reason, the leading security solutions presented by scientific research propose solutions on the transport layer or (fog) and on the application layer or (cloud) to manage security. However, the possibility of adapting the sensor hardware to an IoT architecture based on Blockchain to provide the security system has not been studied so far.

Exploring this possibility has technical implications at the level of architecture and resources. For example; the system is no longer light, but there are fields of application (food and health) where the robustness of the system is worth the cost, especially if the integrity and transparency of the information are guaranteed.

5.1. Blockchain Network

This section answers the specific objective one ***[To identify the Blockchain architecture security requirements needed to transparent communication between an IoT sensor and a Blockchain network]***.

BIoTS has as a challenge to adapt all its architectural modules to the functional requirements of Blockchain. In this case, it is necessary to adapt two algorithms at the hardware

level; i) the SHA-256 algorithm responsible for cryptography in the communications process and ii) the Proof of Work (PoW) algorithm responsible for the consensus process in the network.

As its name indicates, Blockchain is a chain of blocks that systematically stores information in a decentralized network. Each node acts as Miner, and these, generate validation through their processing capabilities. The information contained in each block is interconnected with the previous block employing a hash, making it impossible to reverse or modify data in each block. That's where Blockchain's security comes from. Fig. **5-1**

Fig. **5-1** shows the principal modules contained in each Block of the Blockchain. The Block header module contains the hash (identification on the blockchain system) to exchange transactions on the network. Hash and nonce modules make up a firm, part of a public and private key to transactions on the network. The Block version module contains the block number (series of consecutive numbers) throughout the chain of blocks; this module serves as an identifier to know their position in the chain. The Time-Stamp module guarantees the distributed temporal database contained on each Miner in the network. This module assists in the system's security because the proof of work algorithm reads and processes it to reach the consensus. Merkle Root Hash module allows us to know the origin and history of hash blocks; this feature makes it impossible to decipher the hashes' chain for obtaining the address or the contend any block. Nonce module assigns a zeros-chain before of hash in the Block header module; thanks to this feature, each Block into the Blockchain contains a unique transaction ID (Represents other security behavior of Blockchain). Finally, the Previous Header Block module is responsible for saving the previous header hash for adding to the new hash in the new Block, this module serves to form the Merkle root hash module [116].

5.1.1. Building the Blockchain

The BIoTS performance assessment is possible thanks to building a Blockchain network. Network deployment allows knowing the architectures' adaptation in connection and security requirements. A decentralized network deployment requires careful management of databases in the web and mobile applications. Two algorithms are programmed (SHA-256 and Proof of Work), which govern the Blockchain-IoT system. The Blockchain platform construction as a web service is done in Python language. The development cycle for building software Blockchain application is divided into the stages described in Fig. **5-2**.

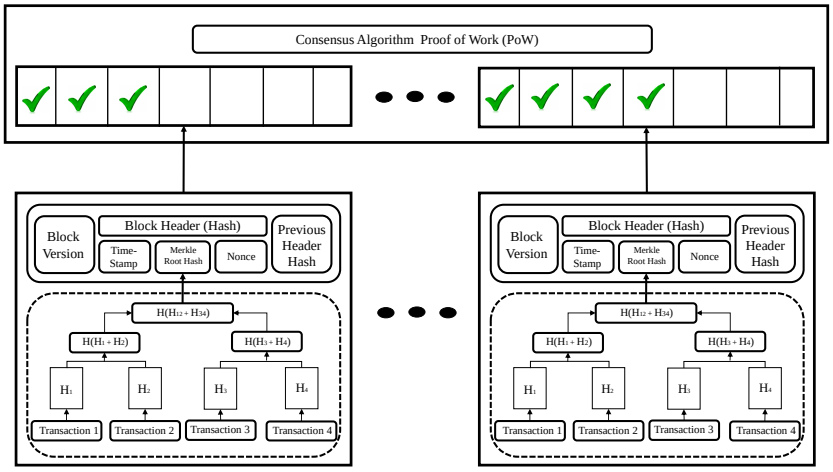


Figure 5-1.: Blockchain system architecture and transaction validation mechanism

Information Gathering and Planning

Build a blockchain network requires find platforms, frameworks, and programming languages. Although Blockchain is popular technology, exist few alternatives to free development. Also, Python allow us building all interoperable ecosystem for deploying the Blockchain Network.

Design Layout and Development

In this stage, we define the website's structure where the information presents to the developer and the users; we organize paths and a hierarchy order of code to navigate the web application. Here, we define backend and frontend elements to start the web service.

Testing, Review and Launch

A blockchain network is considered functional when decentralized nodes and distributed networks can act as miners to validate the information. Besides, the encoding and decoding of information to be protected through cryptography must be checked.

Information Gathering and Evaluation

At this stage, the BIoTS connection to the blockchain network is evaluated. For now, it is enough that the information sent from BIoTS can generate a block or a transaction within the Blockchain-IoT ecosystem.

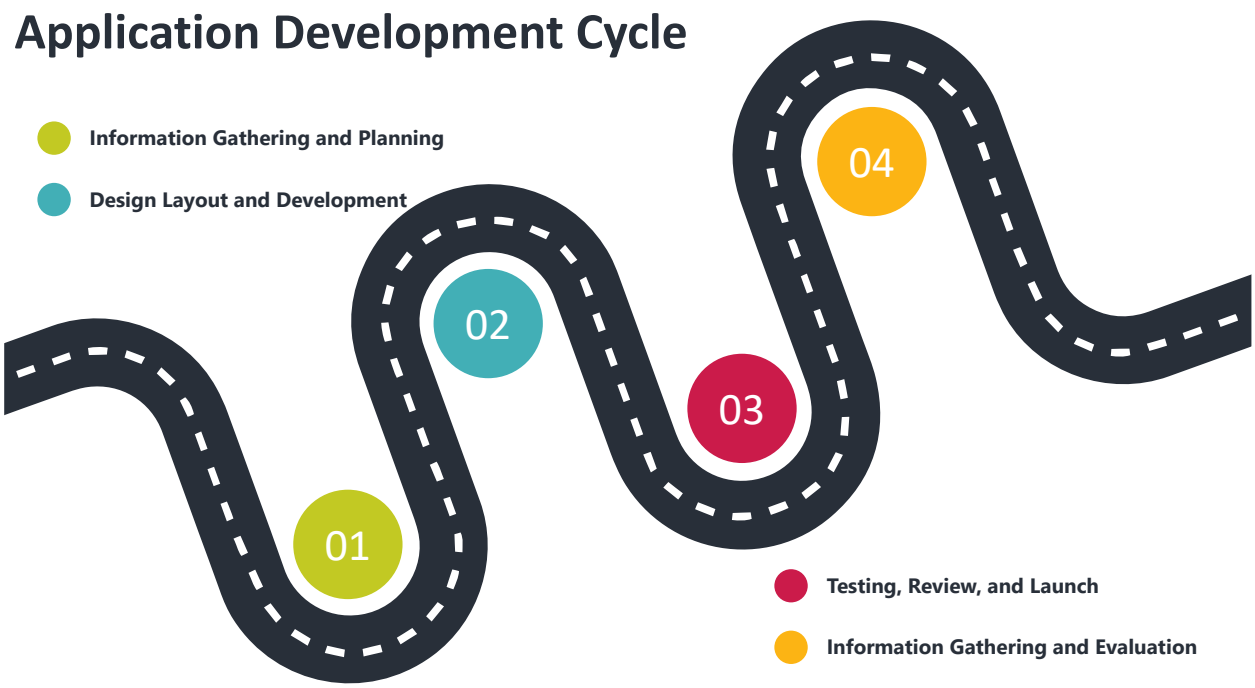


Figure 5-2.: Application development cycle of Blockchain network

Fig. **5-3** describe the software development structure of the Blockchain application. The software architecture deployed to design a functional Blockchain is possible thanks to the interoperable articulation of 4 platforms and Frameworks to associate the services thus: Python, the internal modules of the Blockchain are programmed (SHA-256 Algorithm, PoW Algorithm, Merkle Tree, Nonce, User Registration, Transaction Registration, etc.). Flask is a lightweight web application framework with high scalability properties for web applications. Flask relies on Jinja and Werkzeug to deploy Web services from Python. HTML and CSS are used in the design of the Frontend user environment of Blockchain's web application. Functionally operates relations between the Python algorithms, the databases, the user requirements, and articulating the Blockchain transactions processes. SQLite is an embedded SQL database engine that does not have a separate server process which makes it possible to read and writes directly to ordinary disk files in web or mobile applications.

5.1.2. Web Application Functioning

Fig. **5-4** shows the user's Web environment for access to the Blockchain named BIoTS. In the upper part of the application is distributed the navigation menu for the BIoTS operation. The navigation menu's access buttons are; Home, Blockchain viewer, Make transaction, Mine Blocks, Become a Node and Buy BIoTS. Each access is described as follows:

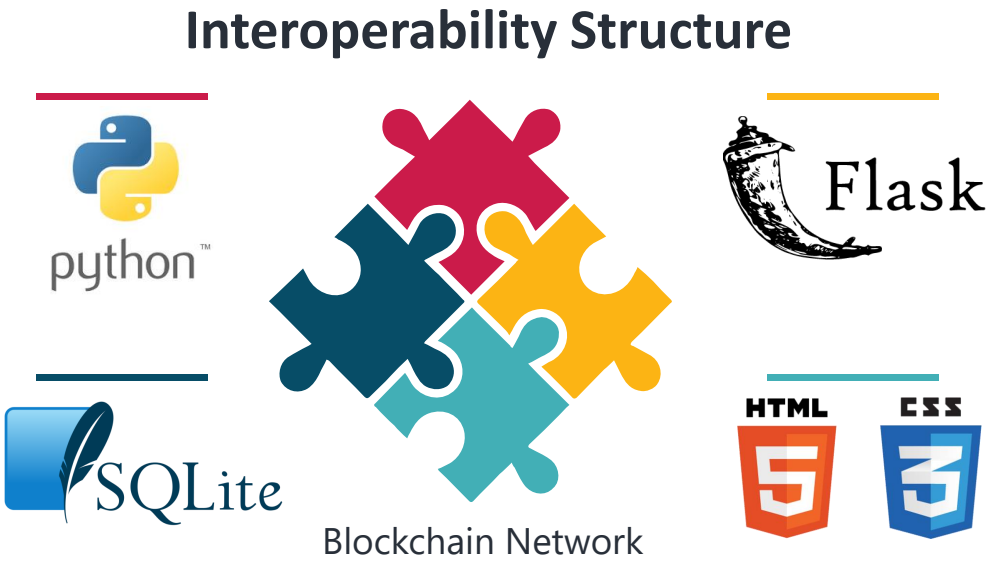


Figure 5-3.: Blockchain Network Interoperability Structure

Blockchain Viewer: Displays the number of blocks in chronological and transactional order that the Blockchain contains. Here is visible only the date and time of the block creation, the previous hash, the hash block identifier, and the block number. In each block, there is a button that displays the historical transactions contained. **Make Transaction:** It displays a set of text boxes where you must register the desired transaction. The data requested are; sender, receiver, and amount. Also, there is an input button to make a transaction. **Mine Blocks:** Displays a table containing information on the mining actors' transactions in the network. Besides, you can see if the system validated the transaction. **Become a Node:** Allows us to convert a network node according to the Blockchain network configuration. In the case of public or private Blockchain, it's select. **Buy BIoTS:** Allows us to buy cryptocurrencies generated by the value of transactions within the network. In case of deploying the system in a public way and for commercial purposes.

As shown in the Fig. **5-5**, the network blocks are the chain of transactions made with the BIoTS participation, both proposing the blocks and mining the data from the other two nodes present in the system. When BIoTS generates a Block, it cannot do it autonomously. To enter the network, BIoTS need to register and start the activity as a miner. That's why a programmed request is generated in solidity from the software through a smart contract. The smart contract is programmed so that a particular action is executed at a specific time. It is possible to have BIOTS generate the block in the network, and the other nodes validate it. This Blockchain network's behavior is due to the configuration of a consortium network. It is a public and private network, given the need to make the sensors act in

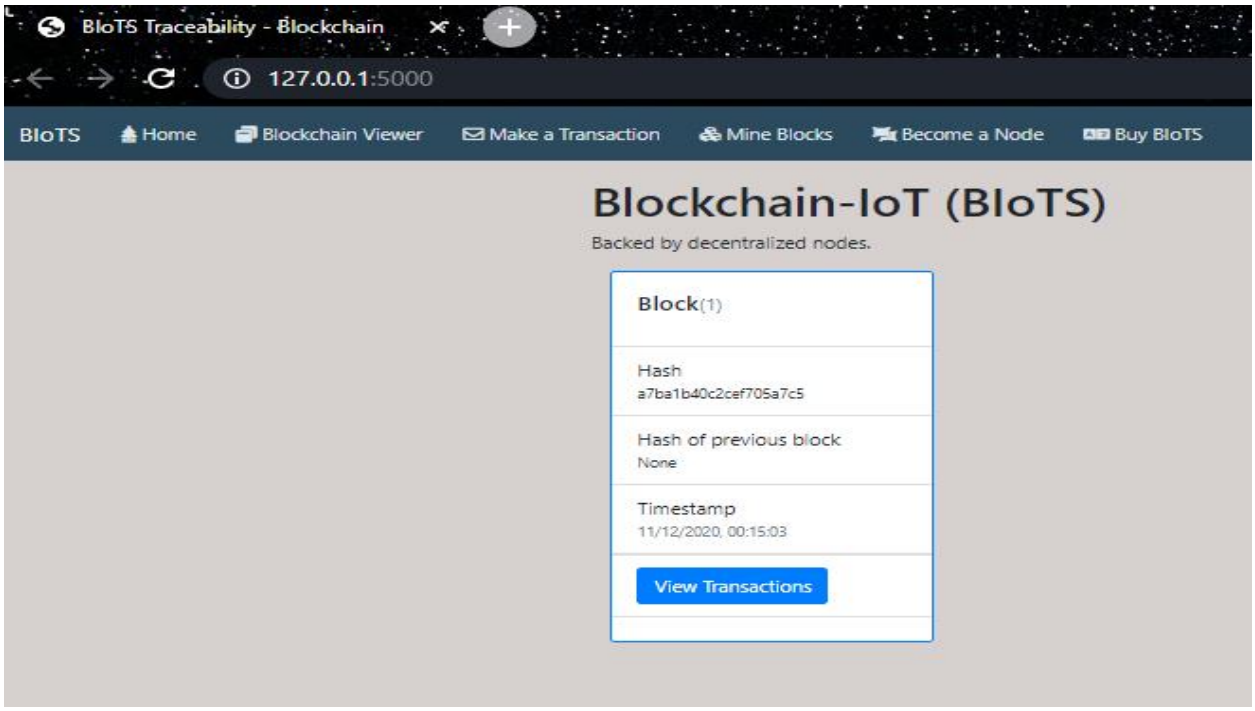


Figure 5-4.: Web application home

a private network. Consumers have access to that information only as observers of the information contained in the blocks.

5.1.3. Smart Contract

Vitalik Buterin conceived the Blockchain as a technology with an enormous capacity beyond Bitcoin. That is why he proposes Ethereum as a blockchain capable of doing much more than transactions. The Ethereum Virtual Machine EVM module in the architecture of the Blockchain Ethereum in Fig. **5-6**, allows processing in a distributed way in all the miners the smart contracts. These smart contracts opened the door to the development of complete Blockchain applications with distributed processing.

A Smart Contract is a program capable of running autonomously and automatically, without the need for intermediaries or third parties to execute it. A Smart Contract is programmed; that is, it will be conducted only when the characteristics marked in it are fulfilled.

The Smart Contracts features are:

- Public: they are stored in the Blockchain, and anyone who is part of it can have access.

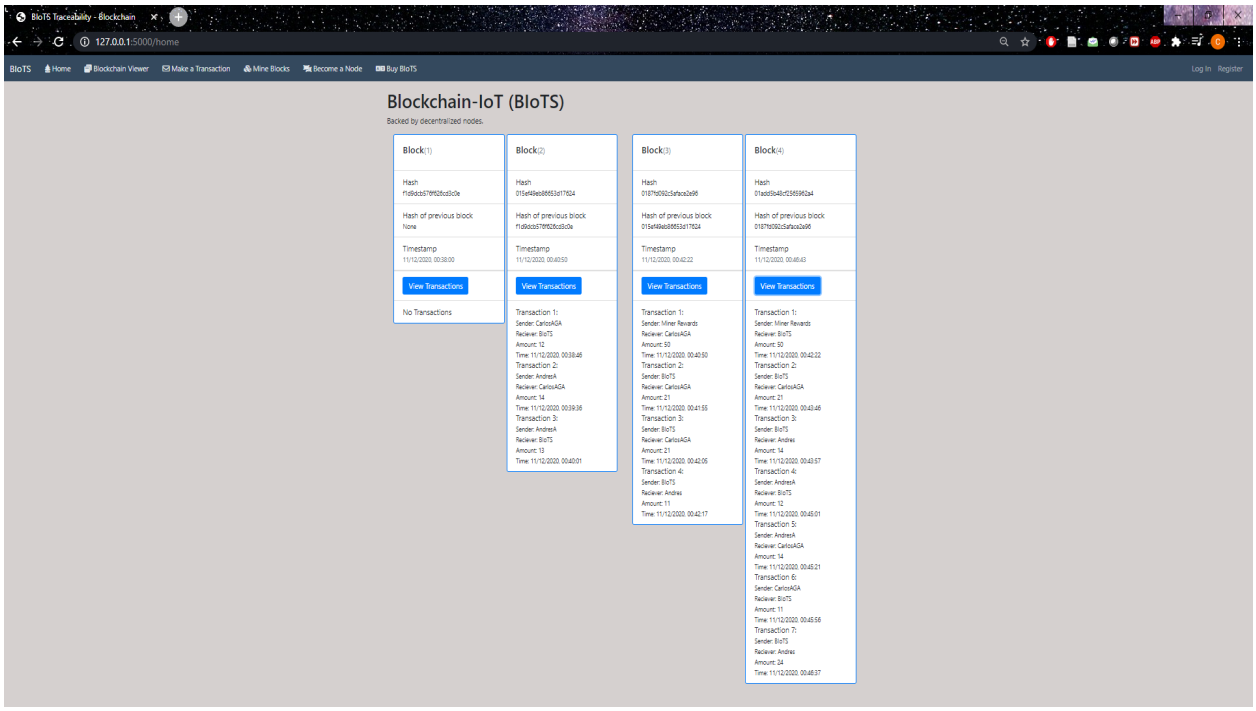


Figure 5-5.: Mining process

- Immutable: they are stored in the Blockchain, so they cannot be changed.
- Configurable: Once you upload the Smart Contract to the Blockchain, only its owner can change certain variables.
- Communicative: the Smart Contract can communicate between them.
- Distributed: the miners are the ones who execute the Smart contracts so that anyone can process them. So eliminates any attempt to absolute control. Any miner can execute it without any permission.

Solidity is a high-level programming language used to implement smart contracts. Decentralized Applications (DApps) are applications created on top of Blockchain and Smart Contracts. This technology feature allows us to implement Blockchain in food traceability.

There are three possible configurations for a Blockchain; public, private, and consortium. The Blockchain designed for this work is a consortium type. With this one, it is possible to make the BIoTS sensors act in the network as miners; that is, they are the only ones capable of validating and processing data. The users can publicly access the information only by way of consultation.

5.2. BIoTS Architecture

This section answers the specific objective two ***[To propose additional storage and processing units to an IoT sensor needed for its integration with a Blockchain architecture]***.

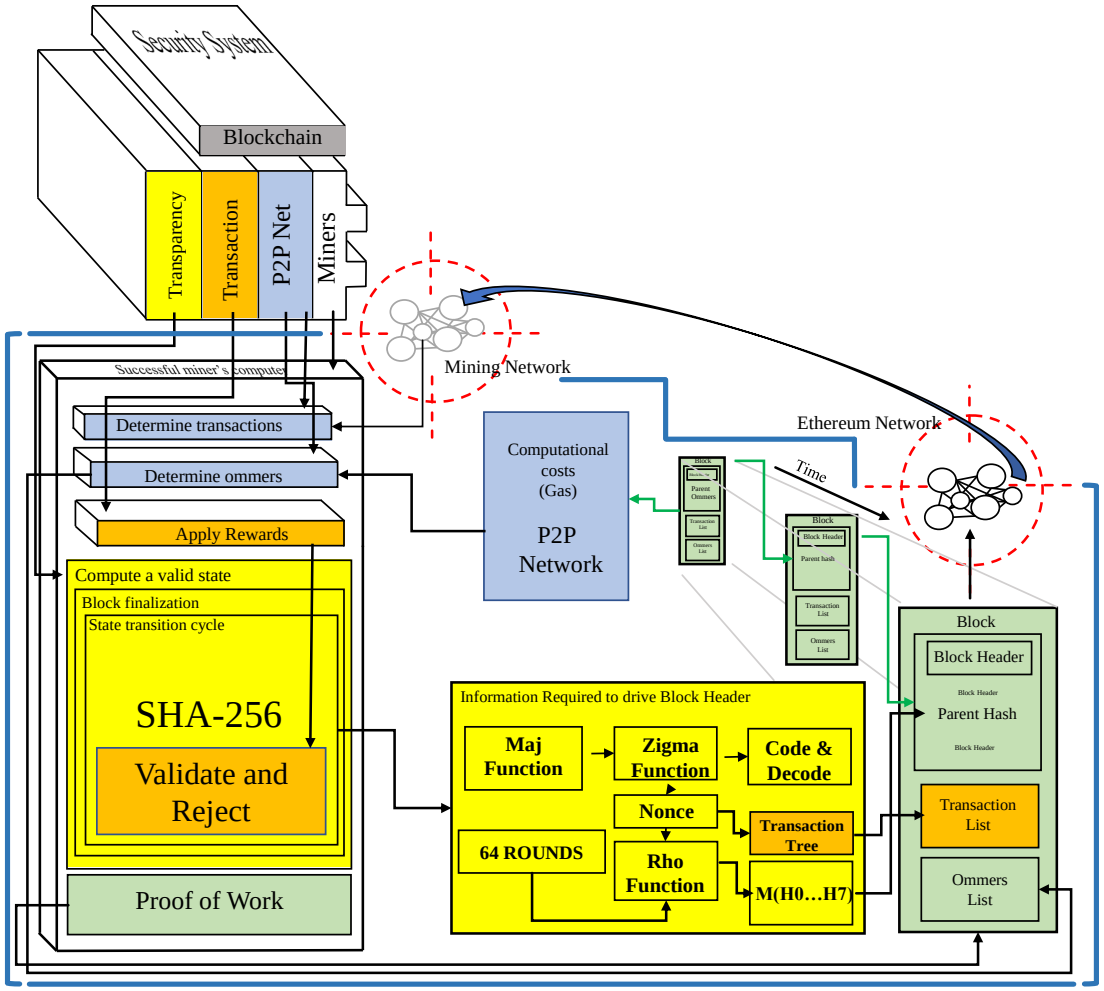
A IoT sensor is an embedded device capable of acquiring information, processing it, analyzing it, storing it, and transmitting it to a repository. It also can coordinate with other networked devices. Under this concept, we describe BIoTS-Sensor architecture features that allow us to define the necessities of functioning to design a Blockchain-IoT system. Then, we make a description of some architectural modules.

Block A in Fig. **5-6** is the architectural approach of an Ethereum's blockchain. This block describes the structural layers that form a security system. For this proposal, we focus on the Miners layer's study and analysis. In this layer, we found the physical devices (Computers) that interact in the Network to make the Blockchain valid. The fundamental elements in this layer are two; storage and processing capacity.

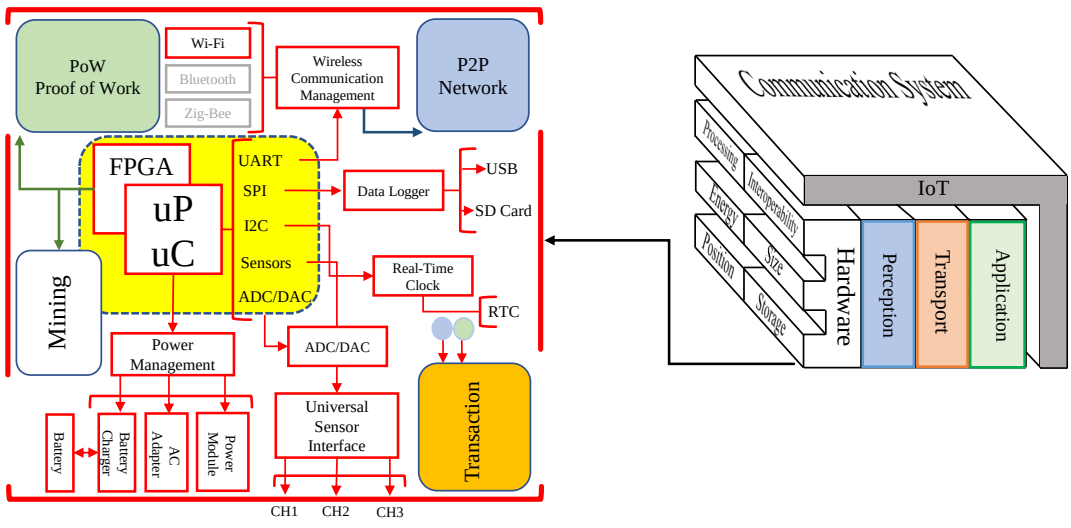
As we can see in Fig. **5-6**, block B represents IoT as a communication system where a service is deployed through some architectural layers (see Fig. **4-1**). In this block B, we focus on designing and improving the hardware capabilities in the perception layer to splice this device with block A's Blockchain software technology. The primary devices features that act in this layer are; i) interoperability, ii) processing, iii) energy, iv) size, v) position, vi) storage capacity, and vii) Security. Moreover, it can evaluate the hardware device quality involved in an IoT ecosystem according to these features. For this reason, they are the ones we take into account to develop the new BIoTS capabilities.

The block B, we can see the module that ought added to the sensor. Each module responds to the need created by the Blockchain system. The modules are related by color; thus, the blue module of the P2P Network is designed to make possible the P2P Network in which the sensor acts as Miner. The green module of the Proof of Work (PoW) algorithm makes transaction validation possible and guarantees the block's information's immutability. The yellow module subject to the Mining process is designed to calculate hashes in the communication's cryptographic function. Finally, the orange module is designed to store the records for each validation through the Merkle tree.

As we can see, the junction of these blocks, the IoT as an oriented communication system, and the Blockchain as a security system, together represent a communication system with a high-security level.



(A)



(B)

Figure 5-6.: Blockchain-IoT Architecture Matching. (A) Blockchain Ethereum Architecture Approach by Lee Thomas based on [1]. (B) IoT-Sensor Architecture.

Thanks to the previous construction of the Blockchain network described in the previous section, we know the hardware, security, and interoperability requirements needed to connect an IoT device and the Blockchain network directly. Fig. **5-6** summarizes the elements adapted through the digital design of the two parts of the architecture (Blockchain and IoT) in the new BIoTS. The agri-food traceability application field, where this solution is thought, means the traceability of both product and information.

Fig. **5-7** shows with path one the conventional data flow in an IoT ecosystem. This path clearly defines some hardware elements deployed and interconnected in the physical sensing layer of the IoT architecture. This data is managed in a hub or breaker device at the transport layer of the architecture. In general, these devices expand the system's capacity and link the sensing layer devices with technologies hosted in the application layer. The application layer receives the data and manages access to it, either for processing or storage. As can be seen, the security vulnerability of the system lies in the boundaries of each layer of the architecture. For this reason, route 2, defined as BIoTS-Paths, aims to eliminate intermediaries (hubs or breakers) for the integral transport of data from the perception layer to the application layer, thus eliminating the boundaries between each layer of the architecture. This path is ensured by the architectural adaptation of IoT devices with Blockchain technology hosted at the application layer.

The architectural adaptation of the IoT device with a Blockchain system contains several challenges in the hardware construction. The two algorithms that will make possible the participation of the IoT device as an active agent (Miner) within the Blockchain network are described below.

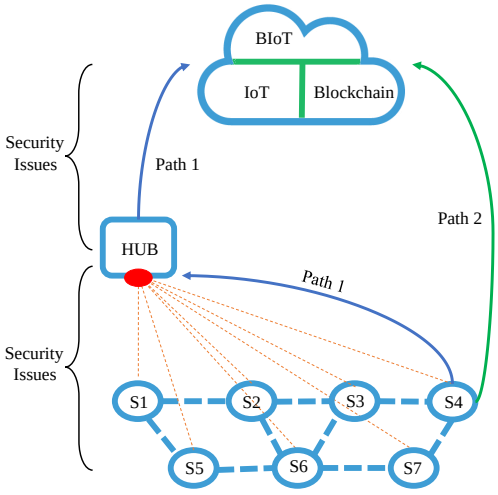


Figure 5-7.: Path 1: conventional data transmission in an IoT system. Path 2: architecture and transmission path proposed by (BIoTS-Paths).

5.2.1. BIoTS Cryptography Algorithm

A hash function can convert an input message with a specific length into an alphanumeric array on the output called a digest. A hash function has the following characteristics [117].

- The reverse process of reconstructing the message from the hash is almost impossible.
- A minor change in the input message completely changes the output.
- The algorithm can compress any extension of the input message for arranging the output. It is impossible to find the same hash for two different input messages.

The SHA-256 algorithm has two modules; i) Message Block schedule and ii) Compression function. Below is a brief description of the modules. In the message Schedule module, an N-bit message gets added with bit 1 followed by zero bits until the following equation 5-1.

$$N + 1 + k = 448 \ mod \ 512 \tag{5-1}$$

It is satisfied, where k indicates the number of zero bits to be added. The value N is then converted to its 64-bit binary representation and further added to the 448-bit intermediate value to get the 512-bit message block. This formed block is further subdivided into sixteen 32-bit word sub-blocks that input the compression function.

Compression function involves 8 registers a, b, c, d, e, f, g, h and 6 logical functions Ch, Maj, Σ0, Σ1, δ0, δ1. There are another set of eight registers H0, H1, H2, H3, H4, H5, and H6, H7, to store 32-bit hash values, which is updated Mtimes if there are M 512-bit message blocks. These registers are initialized with 32-bit constant values obtained by considering only the fractional part of the first eight prime numbers after taking the square root. Logical functions comprise XOR, right rotation, and right shift operations. These complex operations are performed on 32-bit words for 64 rounds.
Following functions are computed on each round, and the registers are updated:

1. Calculate Maj(a,b,c), Ch(e,f,g), Σ0 (a), Σ1(e), δ0(a), δ1(e).
2. Words are prepared for each round using the below equation: For first 16 rounds

   $$W_n = Message_{n_n}^{\ i} \tag{5-2}$$

   where n ranges from 0 to 15 and i indicates number of message blocks. For the other rounds,

   $$W_n = \delta_1(W_{n-2}) + W_{n-7} + \delta_1(W_{n-15}) + W_{n-16} \tag{5-3}$$

3. Six registers b,c,d,f,g,h are updated with the previous registers value i.e., a,b,c,e,f,g respectively after each round of operation. While register a = T1 + T2 and register e = d + T1.

4. T1 and T2 have the following equations:

$$T_1 = h + \Sigma_1(e) + Ch + W_n + K_n \tag{5-4}$$

, K are a set of 64 constant words.

$$T_2 = h + \Sigma_0(a) + Maj \tag{5-5}$$

After 64 rounds of operation, registers H1 to H7 are updated for i ranging from 1 to M as follows:

$$\begin{aligned}
H_0^i &= H_0^{i-}1 + a \\
H_1^i &= H_1^{i-1}1 + b \\
H_2^i &= H_2^{i-2}1 + c \\
H_3^i &= H_3^{i-3}1 + d \\
H_4^i &= H_4^{i-4}1 + e \\
H_5^i &= H_5^{i-5}1 + f \\
H_6^i &= H_6^{i-6}1 + g \\
H_7^i &= H_7^{i-7}1 + h
\end{aligned}$$

Final 256-bit Hash value is obtained by concatenating 32-bit values H_0^M to H_1^M. $Hashdigest = H_0^M H_1^M H_2^M H_3^M H_4^M H_5^M H_6^M H_7^M$.

The mathematical deployment of the SHA-256 algorithm above aids the compression of the algorithm by software, and this, in turn, allows the algorithm to be deployed in hardware. The pseudocode of the SHA-256 Algorithm 1 will enable us to see the successive multiplication and addition operations in the encoding rounds of the W and M functions. This pseudocode allows us to mathematically analyze the process flow to calculate the nonce by the consensus algorithm.

5.2.2. Consensus Algorithm Analysis for BloTS

The consensus algorithm establishes the mining agents' computational effort to solve the mathematical puzzle that validates transactions within a Blockchain network. Consensus algorithms can be categorized into two groups; proof-based consensus and vote-based consensus. In the first case, the node wishing to join the network must demonstrate higher processing and storage capabilities than the rest of the network. In the second, each node in the network is asked to propose or validate a transaction block that will be part

Algorithm 1 SHA-256

for Compression Function **do** Message Schedule module (Eq.: 5-1)
    Words are prepared for each round $\mathbf{M}_{aj}$ (Eq.: 5-2)
    for First 16 rounds $\mathbf{W}_n$ **do** (Eq.: 5-3)
        Six registers b,c,d,f,g,h are updated with the previous registers
        ,K are a set of 64 constant words (Eq.: 5-4, 5-5)
        After 64 rounds of operation $\mathbf{H}_1$ to H_7
        if then $H_7^i = H_7^{i-7}$
            Final 256-bit Hash value is obtained by concatenating 32-bit values
        end if
        Hash digest = H_0^M to H_1^M
    end for
end for

of the validation in the rest of the network. The final decision is made only after considering the majority's results. Thus, some algorithms were analyzed theoretically and based on [2, 3, 118] to select the BIoTS algorithm, some voting-based consensus algorithms; Proof of Vote (PoV), Ripple, Delegated Byzantine Fault Tolerance (DBFT), and Proof of Trust (PoT). Furthermore, two proof-based; Implicit consensus and Proof of Work (PoW).

The most common consensus algorithms in Blockchain (Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT)) limit the BIoTS ecosystem for the following reasons:

- PoS: It is based on the concept of the age of the coin, this age being known as its value multiplied by the period after its creation. In other words, the longer a node has a currency, the more privileges it will obtain in the network. For this reason, the BIoTS ecosystem for food traceability systems does not require concepts of this type.
- DPoS: It is based on the fact that each node in the network can select tokens according to their participation. These selected tokens create new blocks one by one as assigned and get a reward. Throughout the network, the n best witnesses who have participated in the transaction's validation and have obtained the highest number of votes are entitled to the benefit. Blockchain using DPoS is more efficient and saves more energy than PoW and PoS. However, in the BIockchain-IoT ecosystem where BIoTS is deployed, it is not expected to have enough witness nodes to validate the data BIoTS collects. A BIoTS P2P network is expected to operate with consensual data sharing.
- PBFT: Designed to solve transmission problems and improved to avoid exponential

operations. Regarding BIoTS, it is not convenient to use it as it requires a master server to execute the validation throughout all supply chain stages.

Most Blockchain networks are decentralized, with synchronous or asynchronous communication models, and are implemented in networks of nodes where mining agents are processor-based; consensus algorithms' behavior is subject to factors such as; Blockchain type, transaction rate, scalability, adversary tolerance model, experimental setup, latency, throughput, bandwidth, communication model, communication complexity, security attacks, energy consumption, mining, consensus category, consensus finality. Here we analyze some of these.

Table. **5-1** shows some characteristics of the consensus algorithms studied for implementation in the BIoTS device. As can be seen, physical experimentation on hardware to find the performance parameters do not yet exist. However, theoretically, it is possible to establish the suitability of some of them according to the Blockchain network design.

Consensus Algorithm	Blockchain Type	Mining	Consensus Category	Reference	Experiment Setup	Communication Model	Energy Consumption
PoW	Permission-less	Based on computational power	Proof-based	[119]	Real implementation	Asynchronous	538 KWh
Implicit Consensus	Permissioned	Proof based mining	Proof-based	[120]	Theoretically evaluated	Asynchronous	Unknow
PoV	Consortium	Vote-based mining	Vote-based	[121]	Simulation, Single machine	-	Unknow
Ripple	Permissioned	Vote-based mining	Vote-based	[122]	Simulation, Single machine	Asynchronous	Unknow
DBFT	Permissioned	Non-proof of work based mining	Vote-based	[123]	Proposed solution is not validated through experiments	Asynchronous	Unknow
PoT	Permission-based consortium	Probability and vote based mining	Vote-based	[124]	Simulation, Single machine	Asynchronous	Unknow

Table 5-1.: Generic Features Analysis of Consensus Algorithms (based on [2, 3])

After this analysis, it is concluded that some voting-based consensus algorithms can be highly relevant for BIoTS performance in a Blockchain-IoT ecosystem. However, we expect that BIoTS based on PoW and Ethereum can certify processes within a supply chain. The right way to condition the collection and validation of information for Blockchain is through smart contracts. On the other hand, although Blockchain is very popular, some experimental developments of this type need support and tools that are not yet available. In contrast, the Blockchain development community from Ethereum provides many alternatives for support and development.

5.2.3. BIoTS Consensus Algorithm (PoW)

Proof of Work consensus algorithm is a mechanism that allows users or machines to coordinate in a distributed network. This algorithm ensures that all agents in the system can agree on a single truth source, even if some agents fail. In other words, a system with PoW is tolerant of security failures.

The process of verifying the Block's transactions to be added, organizing these transactions in chronological order in the Block, and announcing the newly mined Block to the entire network does not take much energy and time. The energy-consuming part solves the "hard mathematical problem" to link the new block to the last block in the valid blockchain. When a miner finally finds the right solution, the node broadcasts it to the whole network simultaneously, receiving a cryptocurrency prize (the reward) provided by the PoW protocol. Hereunder we show the algorithm compression [116].

The implementation of the PoW in hardware determines, among other things, the energy consumption, the difficulty in validating the block (time invested in identifying the legitimacy of the block), and the active participation of the Blockchain network miners. To the hardware block of the SHA-256 algorithm, it is necessary to adapt a function capable of adding at each round of the cryptographic encoding a string of zeros (from 4 to 18 at most, depending on the difficulty of the algorithm) that will act as an identifier of the block and the transaction on the entire blockchain. The PoW Algorithm 2 is compressed and identifies the place where it should be hosted within the SHA-256 algorithm. The PoW is part of the consensus process and requires analysis to be included in the transaction process within a Blockchain network.

Algorithm 2 Proof of Work

$r \leftarrow ab$ ▷ Define variable to answer

1: **for** Loop from 1 to n **do** var $x = n$;
2: **for** n major 1 $x_0 * y_0 + n$ **do**
3: var added = 0; (var i = 0; i minor $Math.abs(a)$; i++) added += answer;
4: answer = added (n–;)
5: **end for**
6: **end for**=0

Fig. **5-8** describes the process carried out to add the PoW to the SHA-256 algorithm in hardware. The four stages are:

1. **Generate Random Nonce**: once the clock for the hash and PoW is configured and synchronized, a 32-bit register and bus are generated. The first thing is to introduce a nonce every six cycles with a feedback delay of 12 cycles.

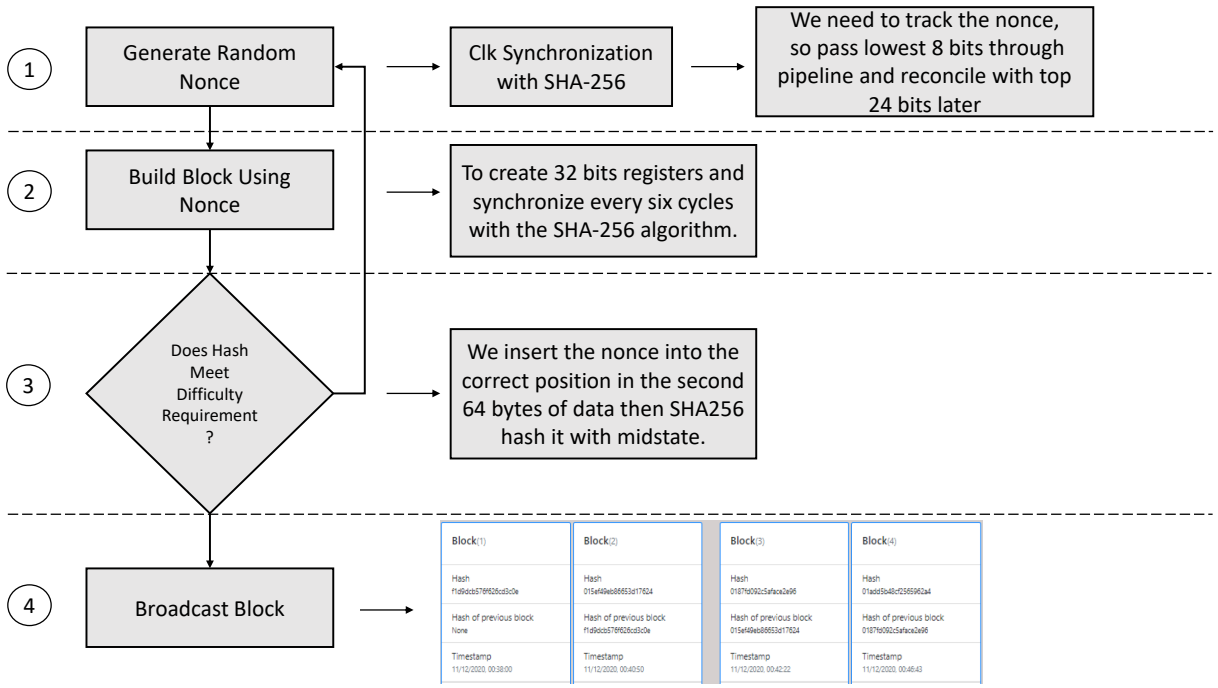


Figure 5-8.: Proof of Work Implementation on Hardware

2. **Build Block**: since this is not straightforward, we use a register that to track the hash through the bus. To follow the nonce, we pass the least significant 8 bits of the 32-bit register and then pair the remaining 24-bit.

3. **Difficulty**: in the second of two rounds of hashing of 64 bytes each, the header of the 80-byte block is the encrypted data space. The first round gives us the average state to insert the nonce at the beginning of the record of the second 64 bytes in the correct position.

4. **Broadcast Block**: subsequently, the internal hash transformation is performed to complete the register. It is still not the full SHA-256 because it involves multiple rounds. Nevertheless, this process is iterative. Here the VHDL code in the DE10-Nano is split into phases to discriminate the SHA-256 transformations and then unified into one block intended to do the complete hash transmission.

When the PoW algorithm checks zeros' existence in the hash encoded in base 64, the average and the maximum number of hashes is known to calculate the order of difficulty that increases exponentially by the expression 5-6. The Nonces included in hashes are pseudo-random, and this feature extends the capacity of the PoW.

$$h(\rho) = \alpha^{\rho} \tag{5-6}$$

Where, $h(\rho) =$ The average number of hashes required to find a valid solution α = The number of characters used in the encoding ρ = The arbitrary difficulty order.

$$h(\rho) = 64^{\rho}$$
$$h(3) = 64^{3} = 262,144$$

Thus, typically 262,144 hashes or less are required to mine each block while testing this algorithm. However, the difficulty is arbitrarily adjusted by modifying the ρ variable. Changing ρ changes h exponentially and could be used to maintain a consistent network block generation rate despite exponentially increasing computational power.

5.2.4. BIoTS Prototype

This section answers the specific objective three ***[To design an IoT sensor that contains the proposed storage and processing units.]***.

The BIoTS device comprises a platform of peripheral analog electronics connected to the digital module designed in a reconfigurable FPGA. The digital module contains several sections; cryptographic and consensus algorithms (SHA-256 and PoW) and SD storage hardware structure. The BIoTS hardware structure contains two modules (Yellow and green) and one software Blue module (Build of Blockchain on Python). Fig. **5-9** shows on the right the modules designed on the DE0-Nano FPGA; these hardware modules are the ones that make possible the parity and interoperability of BIoTS with a blockchain network. This module contains, among others, the SHA-256 Algorithm, PoW Algorithm, I2C module, and SD-CARD module. These modules will be briefly described below. The next green module shows the peripherals in analog electronics for BIoTS can interact with the media, store information collected, and become a Blockchain network node. The Blue area contains the software development module for the Blockchain network in Python, as described in the previous chapter.

Fig. **5-10** show the chip planner of DE0-Nano FPGA with the hardware development area implemented, barely sufficient resources for implementation [125]. In Table. **5-2**, we describe the resources available and used by the three modules.

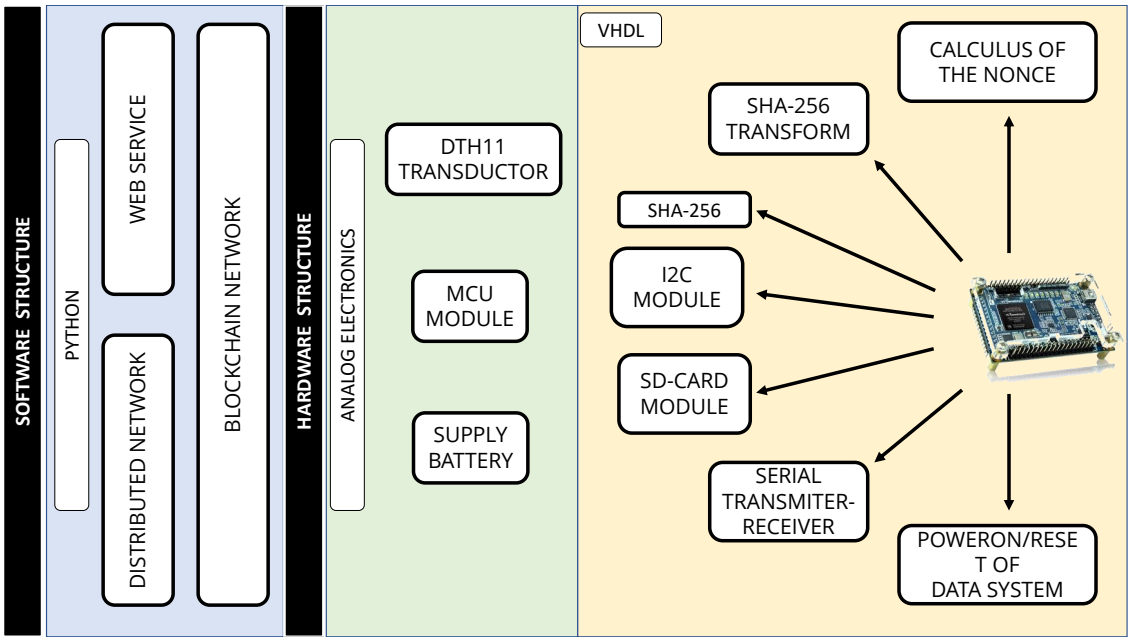


Figure 5-9.: Structure of Architectural Development

FPGA	Total Logic Elements	Percentage Available
DE0-Nano	22,320	100 %
Block	**Total Logic Elements**	**Percentage Used**
SHA-256 and PoW	10,347	46 %
I2C-Master	168	$\leq 1\,\%$
I2C-Slave	114	$\leq 1\,\%$
SD-CARD	289	1 %
Total Area Used	**10,556**	**47 %**

Table 5-2.: Logic Elements Used on DE0-Nano FPGA

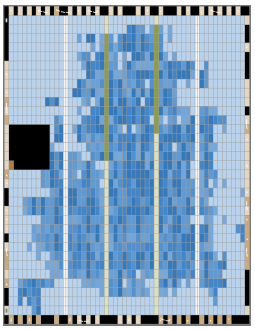


Figure 5-10.: Chip Planner of DE0-Nano FPGA

Fig. **5-11** shows the block diagram that summarizes the deployment of the BIoTS architecture in VHDL. As we can see, three blocks; I2C, SHA-256 (That contains the PoW algorithm), and the SD-CARD architecture. BIoTS need these three blocks to process two complex algorithms and store a distributed database. Here, we show the relationship between modules and how the functions and records interact. VHDL code representation for the construction of the BIoTS hardware from the highest level is represented in the three blocks (see Fig. **5-11**); each of these blocks contains the configuration of the logical elements that make possible the assigned tasks.

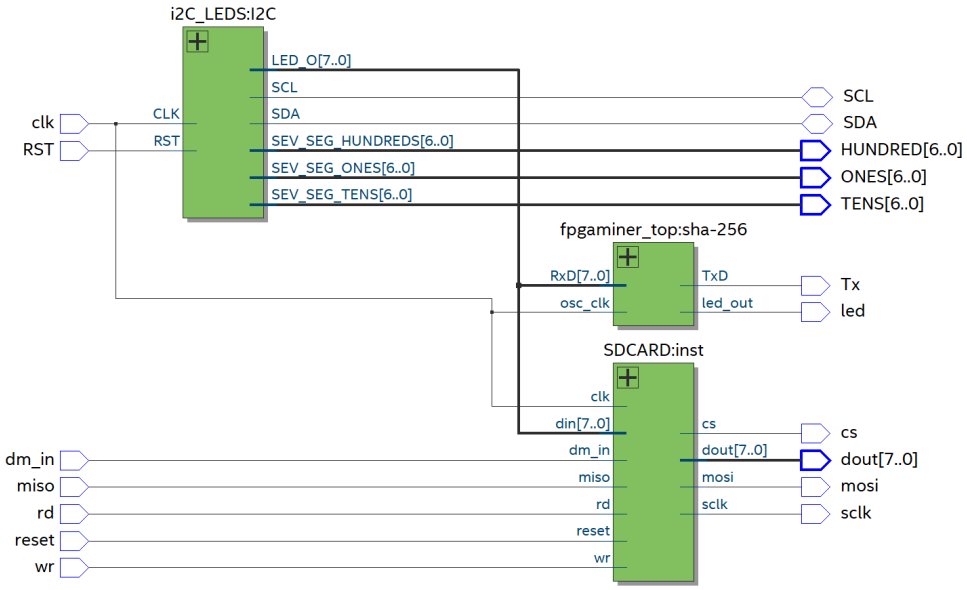


Figure 5-11.: Diagram Block of BIoTS

Fig. **B-4** show the hardware schematic diagram of the SHA-256 algorithm. This design contains the PoW algorithm development, which is necessary to calculate the Nonce and make possible participation in the consensus process.

Fig. **B-1** shows the I2C master component for single master buses, written in VHDL for use in FPGAs, has component reads from and writes to user logic over a parallel interface. It was designed using Quartus II, version 18.0. Resource requirements depend on the implementation. A design incorporating this I2C master to create an SPI to I2C Bridge is available.

Fig. **B-3** describes the SD interfaceable graphically with FPGA is implemented from VHDL code. Here, we implement in the standard size, but electrically all sizes work the same way. Let's focus on SD card standard size since that is conveniently popular nowadays. To this proposal, we install an SD card of 32 GB.

5.3. Results

This section answers the specific objective one ***[To verify the transparency of data transmitted from the designed IoT sensor to a Blockchain network without deploying intermediaries]***.

The BIoTS performance is evaluated according to the configuration shows in Fig. **5-12**. As we can see, the private Blockchain network in which the sensor tested consists of three nodes, two computers, and the BIoTS. The computers can propose simple transactions such as submitting a humidity and temperature value, only for the BIoTS to validate them as miners in the network. However, the importance lies in the transaction proposed by the BIoTS. The computers will validate this by comparing the humidity and temperature values indicated by an internet application. Suppose the humidity and temperature value is in the right proximity range. In that case, the transaction is validated, and the functions of BIoTS as a miner in a Blockchain network are satisfied.

Some values related to data transmission from BIoTS to the Blockchain designed for the use case are shown in Table. **5-3**. Each time cycle has an estimated amount of transactions per second (tps) that the device and the network can support. In this case, the data size sent humidity and temperature information grows in the stored data in the network's distributed database. Finally, there is a latency associated with each information transmitted and validation process for each transaction.

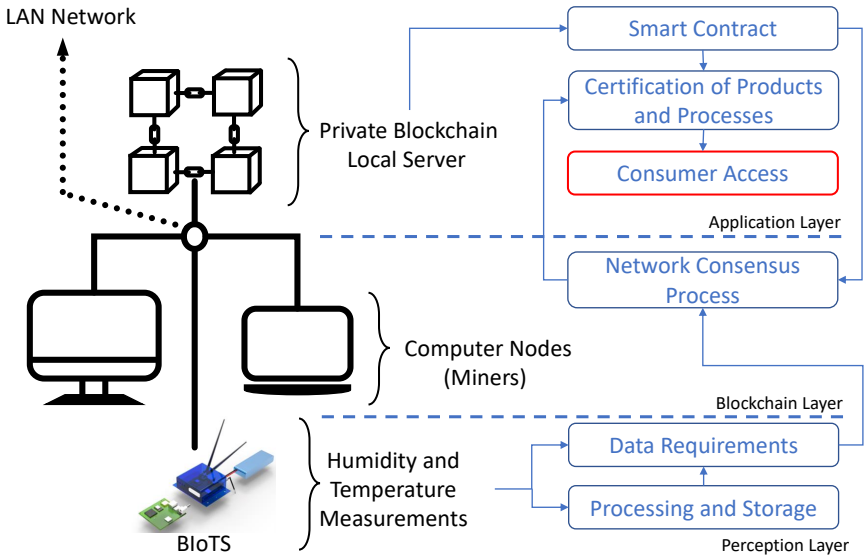


Figure 5-12.: Evaluation Scenario

Fig. **5-13** shows how the BIoTS device and Blockchain network interact to certify processes that depend on the information collected by BIoTS in the Supply Chain stages. Once

the Smart contract is programmed with the requirements to certify a process, in this case, humidity and temperature, the BIoTS devices act as miners to propose a transaction and validate it within the blockchain network. In this way, the collected data will enjoy the security privileges of a Blockchain system.

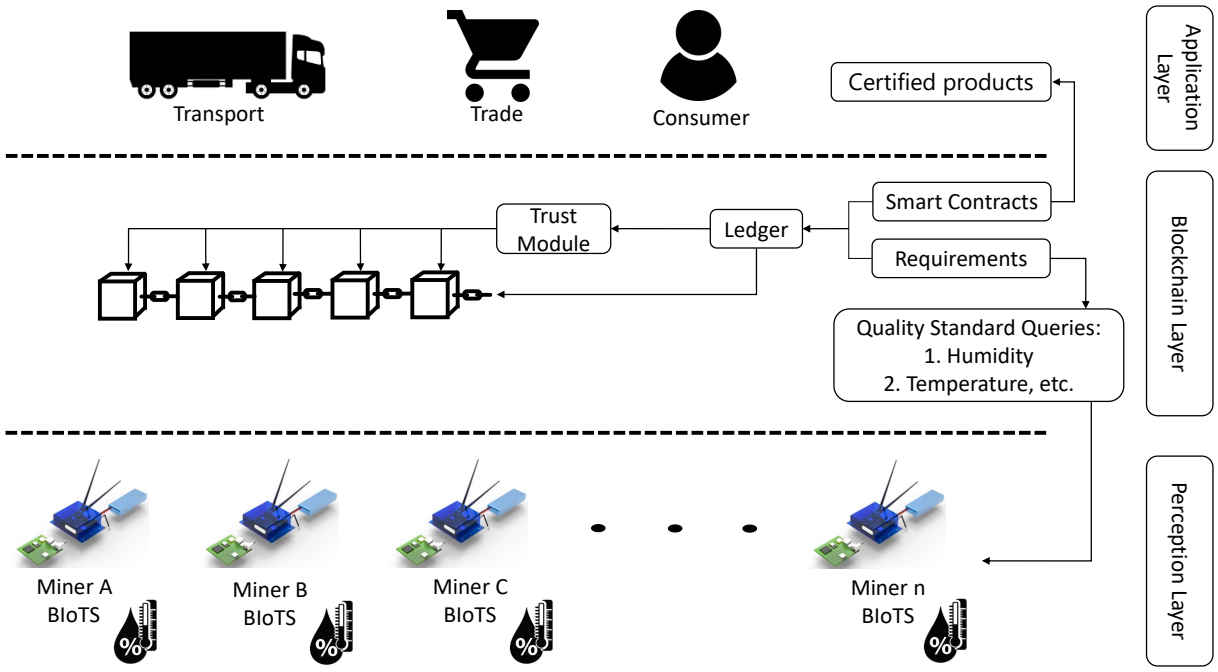


Figure 5-13.: BIoTS System Operation

These data Table. **5-3** show the technical behavior of BIoTS in eight successive transactions. BIoTS proposed eight times a block in the network, with humidity and temperature data validated by the nodes of the network described in Fig. **5-12**. As we can see, as the size of the data sent increases, the latency in the transmission process increases. This behavior is attributed to the consensus algorithm's performance in this type's network.

These measurements only represent the behavior of a small test Blockchain-IoT network. However, in a public Blockchain network of n number of nodes, it is expected that the performance of BIoTS will maintain the behavior as a mining agent.

Step-Time (Seconds)	Transaction Rate (tps)	Data Send (bytes)	Latency (Seconds)
0,16	0,43	14	0,03
0,31	0,54	30	0,05
0,46	0,69	46	0,06
0,52	0,68	62	0,07
0,71	0,87	78	0,09
0,80	0,93	94	0,13
0,90	0,99	110	0,10

Table 5-3.: Evaluated Parameters

The graph in Fig. **5-14** shows the performance of BIoTS in transmitting a data packet concerning the time it takes to propose a transaction on the Blockchain network. We observe that the time overhead in BIoTS transactions is one second; this is when it takes for the algorithm to encode and decode the accumulated data from seven humidity and temperature readings. The behavior of the transaction rate is linear, while the difficulty of the consensus algorithm grows exponentially. Directly, the size of the data packet sent in each transaction increases. This linear behavior may change to saturation lapses when BIoTS is subjected to the work of a Blockchain network where multiple BIoTS nodes participate. But at the same time, the network will work at the execution rate of the algorithms on FPGA. The transactions per second will surely increase, and the difference in network performance compared to a processor-based network can be determined.

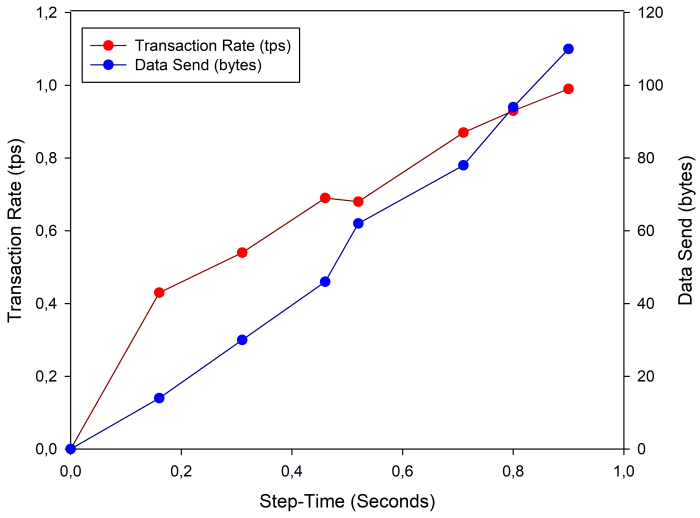


Figure 5-14.: Transaction Rate and Data Size Sent by BIoTS

The BIoTS power source is a three-cell LI-PO type battery at 11.2 Volts, 20-30c discharge, and 5000mA/h. BIoTS analog and digital electronics' energy consumption is calculated

based on the evaluation scenario's functional performance. The elements that consume the most energy are; the peripheral elements: the Wi-Fi module. The BIoTS analog module consumes 220 mA/h transmitting data at a step-time interval of Table. **5-3**.

The BIoTS digital modules developed on an FPGA such as the SHA-256 cryptography algorithm, PoW consensus algorithm, and the SD memory block with features of reading and write speed of the SD memory (Sequential Read = 90 MB/s and Sequential Write = 40MB/s), were calculated so; a resistor (200 Ohms) in series (shunt) of low capacity is placed on the power supply line (active load). The voltage on this resistor is measured, and this measured value is divided by the value of the resistor. Thus, the total value of the current drained by the FPGA development board will be obtained. This measurement is 157mA. Then, a shunt with a resistor is placed to interrupt the power line to the FPGA core, and thus we got the drain/consumption measurement ranging from 83mA to 157mA.

Under these conditions, the battery life is 45 minutes. Under these conditions, it is possible to calculate the duration time of the battery subjected to the previously measured consumption. The values that allow calculating the time are; battery charge capacity and current consumed by the device. These values are represented in equation 5-7. However, although we would expect to have a duration of 13.2 hours as shown in the calculation, factors such as the age and conservation state of the battery determine the accuracy of the calculation. However, as transactions occur, the complexity algorithm kicks in and demands more processing power from the FPGA. Thus, the power consumption is dynamic, and the FPGA performance is proportional to the Blockchain network's activity.

$$\frac{Drain\ current}{Consumption\ current} = \frac{5000mAh}{377mA} = 13{,}2\ horas \tag{5-7}$$

The data shown in remix.ethereum.org Fig. **5-15** is the response to the programming of a Smart Contract in Solidity language; it is designed to read the humidity and temperature data of BIoTS every so often. These data are sent from BIoTS generating a new transaction, or if it is the case, another device proposes the transaction, and BIoTS can corroborate this information. The data shown in Figure 9 shows the behavior of BIoTS acting as a Miner within the Blockchain-IoT network.

For the evaluation scenario, the transmitted humidity and temperature data from BIoTS are correctly encrypted and recorded in the blockchain network. Since the computational overhead increases as transactions (Measurements) and blocks grow, it is only possible to know the energy performance of BIoTS when hundreds or thousands of reads are accumulated. However, future work is expected to implement a BIoTS network and determine its performance as a Blockchain-IoT ecosystem.

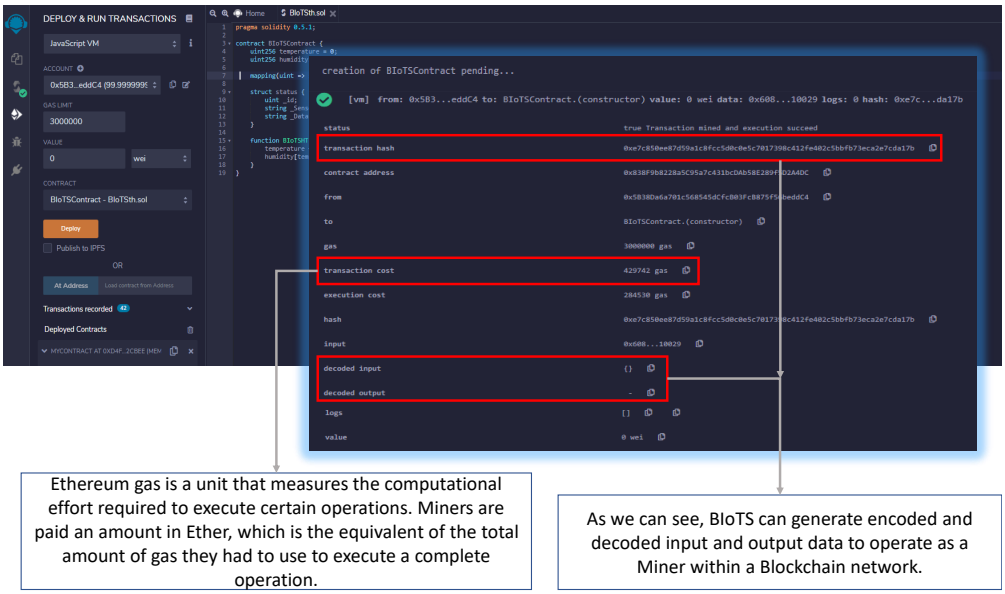


Figure 5-15.: Transaction made by BIoTS on Blockchain Ethereum

The transactions proposed and validated by BIoTS are considered honest because the ledger's data is passed directly from the sensor to the BIoTS system and translated to the Blockchain system. This seemingly little fact is the reason why BIoTS can withstand security attacks at all layers of the IoT architecture. The weighting criteria in the level of resistance and probability of security attacks are done from the analytical, theoretical, and conceptual perspectives, as shown in some related works. [16, 116, 126]

Table. **5-4** summarizes some of the IoT security issues that BIoTS has the potential to solve. As we can see, with this device, the resistance to specific security attacks is high and some moderate, considering the raids in a Blockchain-IoT network.

To identify the security flaws where BIoTS is a potential solution, we study a causality and effect correlation between the nature of the security attack in an IoT ecosystem and the Blockchain Hardware's architectural features implemented in BIoTS [16, 116, 126]. The scale is weighted according to the architecture's characteristics. For example;

- "Sensor Tampering": the attack on BIoTS is unlikely because the sensor data is hosted in the SHA-256 and PoW hardware algorithms; after this process, the information is encrypted.

- "Sensor Feed Modification": this attack is possible with BIoTS; however, the resistance is high because the BIoTS firmware is almost null, almost all elements are hardware.

- ”Sybil Attack”: this attack is unlikely in a network where BIoTS acts because it has the same Blockchain network’s resilience. However, it all depends on the network configuration (complexity level of PoW, etc.).
- ”DoS, Protocol tunneling, and man-in-the-middle”: these attacks are unlikely due to the Blockchain network’s nature. The communication channel by cryptography and the algorithms carried in hardware is immune to external intervention.
- ”Jamming and Collisions”: these attacks are possible in a BIoTS network. The resistance to the attack is moderate because it can identify the hash’s inputs and outputs to reproduce copies.

Attack	Description	Attack likelihood	Resistance to Attack
Sensor Tampering	Manipulate sensors to acquire data readings	Unlikely	High
Sensor Feed Modification	Modify the sensor feed and firmware during communications process	Possible	High
Sybil Attack	Creates multiple identities and manipulates the device’s reputation.	Unlikely	High
DoS, Protocol tunneling;man-in-the-middle	Shut down a machine or network and The attacker sets up rogue hardware pretending to be a trusted network as Wi-Fi	Unlikely	high
Jamming, Collisions	Is an attempt to find two input strings of a hash function that produce the same hash result	Possible	Moderate

Table 5-4.: Security Behavior

5.4. Conclusions

The BIoTS design contains modules in analog and digital electronics. All modules interact and perform specific functions that seek to provide the device with remarkable security capabilities to act in a Blockchain-IoT ecosystem. Analog electronics modules perform functions such as communication, power charging, the physical part of memory storage, voltage and current regulators, indicators, buttons, and interaction connectors. The design and development of the digital modules are the most important for this work; the cryptographic algorithm module represented a challenge concerning creating the consensus algorithm that internally contains the algorithm (PoW). These two modules are critical to

the performance of BIoTS as a mining agent within a Blockchain network.

Although the hardware performance of the algorithms included in the BIoTS architecture is satisfactory and meets the objective, future work could be to optimize the algorithms once they deploy functions in the Blockchain-IoT ecosystem. This aspect has a lot to do with the deployment of the Blockchain network software, so the configuration and programming of the network, so far, has essential features that can be extended.

BIoTS can solve most security issues in IoT systems described in Fig. **4-2**, where it is common to manage information with little security measures. Blockchain allows massive access to the information and guarantees validation and data incorruptibility. The food traceability systems can guarantee certain food products' safety from the data traceability of a specific process within a Supply Chain. The information contained in the Blockchain can certify products and processes, thus expanding IoT's capabilities in data security and food safety for the consumer.

BIoTS was successfully designed according to the safety requirements of the Blockchain architectures and a conventional IoT device. With the adaptation of these features, it was possible to make a sensor act as a mining agent within a blockchain network, allowing many security problems in the transmission of information affecting IoT ecosystems to be solved.

BIoTS required the design of a Blockchain environment to deploy its operation; this environment was designed according to the Blockchain architecture's general specifications but with connectivity adaptations in the deployment of the decentralized network. The information collected and transmitted to a blockchain block guaranteed transparency throughout path 1 of this proposal thesis, an almost null possibility of being degraded or visible by an external agent to the network. This behavior of BIoTS shows that Blockchain as a safety guarantor agent in IoT systems is a safety-enhancing complement for food and process products within IoT-based food traceability systems.

6. Conclusions and Future Work

6.1. Conclusions

This work propouse a solution to the security problems in the collection, storage, and transmission of information in an IoT ecosystem. The Bibliometric analysis made it possible to establish that the proposed solutions to security problems do not address hardware development and mainly focus on information management through software and generally at the transport and application layer. Thus, it was taken as a challenge to design BIoTS to integrate two Blockchain-IoT technologies to intervene in the IoT architecture's three layers, including the perception layer.

IoT ecosystems are designed as sensitive information systems, making them prone to severe and wide-ranging security issues, especially data integrity. For this reason, an integral security alternative was sought through the adaptation of technology such as Blockchain to the hardware of the devices immersed in an IoT ecosystem. Until today, IoT systems are conceived from their design as lightweight, ubiquitous, and security fragile information systems. For this reason, this work (BIoTS) significantly impacts the problem of security management in an IoT ecosystem and provides the missing complement to make IoT a secure ecosystem.

For the BIoTS development, it was necessary to map the most frequent, current, and dangerous security issues in IoT ecosystems. This map enjoys a necessary scientific rigor since it was built from the IoT architecture perspective, from the application field perspective, and the user's needs perspective. This map allowed us to outline the attacks and proposed solutions at each layer of the IoT architecture. In this way, we identify the system's vulnerability, the origin of the security attacks, and the application of external technologies, techniques, or devices.

This work proposed, designed, and implemented in hardware and software the Blockchain technology as a central information and communication management system in an IoT ecosystem. The Blockchain and IoT architectures integration extend devices' capability in transparent and secure information processing, storage, and dissemination, thanks to the decentralization, transparency, and data immutability characteristics of a BLOCKCHAIN. BIoTS integrates the features of a conventional IoT sensor and a Blockchain

network deployed in hardware. Besides, it guarantees transparency and integrity in the information provided to the user.

The context that served as motivation for this research is food safety based on supply chains' traceability through IoT systems. It is a sensitive field given the importance of information management and data communication concerning the safety and quality of food supplied to humans. This application field is just one in which BIoTS can act. However, BIoTS offers a comprehensive solution to a real-world problem by proposing a horizon in articulating information and communication technologies to secure IoT systems. As it is known, the application field perspective and the user are fundamental when the objective is to solve security problems in a technological environment. For this reason, food safety is an opportunity to project the deployment of the BIoTS ecosystem.

The Blockchain and IoT-device technologies articulation demanded studying, evaluating, and designing the two technologies' security architectural requirements. The most prominent elements in Blockchain technology were the decentralization of the network, the processing capacity to encode and decode data, and the participation by consensus for the Blockchain network members. These three elements were identified as primary elements in the construction of the BIoTS hardware. These features are related to the execution of algorithms that drive each action; the SHA-256 algorithm is responsible for generating cryptographic functions to encrypt data stored and transmitted on the network. The Proof of Work consensus algorithm is responsible for developing the transaction's transparency by identifying a code attached to the data encrypted by SHA-256. Finally, for this device to act as a decentralized node of the network, a module was designed to install storage capacity (SD Memory) and thus complete the Blockchain architecture requirements. A conventional IoT device's security requirements are; interoperability, processing, power, size, position, storage capacity, and security. The elements on which we focused the design were processing and storage capacity. Although the other elements were also included in BIoTS, we focus on this thesis's contribution to these two modules.

The hardware design of the SHA-256 and Proof of Work algorithms was adapted to the IoT device with the specifications mentioned above and a Blockchain Smart Contract's software architecture. With these two algorithms deployed on the IoT platform, we can guarantee the performance of BIoTS as an active agent (Miner) inside a Blockchain network. This device can propose and validate any transaction within the network.

In the BIoTS ecosystem, a transaction is understood as generating a humidity and temperature measurement to the Blockchain. This transaction is done from the programming of a Smart Contract, which directs the decentralized Blockchain network's operation. In this way, the Blockchain network's deployment defines the ecosystem in which BIoTS will act

as a guarantor of security and quality in the data collected from a process within a supply chain. For this reason, we can say that this ecosystem can guarantee the data integrity that will be useful to certify processes or products in a food production chain.

6.2. Future Works

This work can be naturally extended by focusing on evaluating the performance of BIoTS in a hazardous virtual environment for information management in an IoT network. Furthermore, one can focus this analysis on a network of n BIoTS nodes and evaluate the proposed BIoTS ecosystem's stability. These scenarios can be implemented and evaluated in different ways:

- Deploy a Blockchain network containing n BIoTS devices, one per stage in a food traceability system, governed by a Smart Contract subject to consensus participation by vote with algorithms other than PoW. With this test, the behavior of BIoTS versus participation in the Blockchain-IoT network will be determined.
- Generate a virtual environment of security attacks on the BIoTS network and focus the evaluation on attacks related to the transport and deployment of information. The work would focus on a specific security attack, and the solution would focus on the optimization of BIoTS in its architectural and operational elements.
- With the additional architectural elements of BIoTS, design a P2P network, intelligent, autonomous, and self-managed in security and information control. This approach will be worked at the application and network administrator management level. Additional elements will be built at the software level.
- With the help of software robots programmed to generate security attacks on a Blockchain network, study in-depth the optimization of consensus and cryptographic algorithms brought to hardware to measure their competence in scalable application scenarios (Precision Farming and international market scenarios).
- Implement on the BIoTS ecosystem the feature of parallelizing the data traceability process associated with the crypto-economy process. Generate natural environments in open access virtual platforms to generate economic transactions from certified productive processes.

A. Appendix: ATTACHED SCIENTIFIC ARTICLES

- The first approach to traceability platform based on the IoT concept. The assessment of sensors and actuators into Traceability Systems, one research paper titled “An IoT-Based Traceability System for Greenhouse Seedling Crop” Volume 6, Special Issue 2018, and indexed in the JCR Q1. We present the original paper attached.
- Bibliometric Analysis made for searching gaps and research opportunities in food safety from the information and communications technologies. This work is presented in an original and extended paper titled: “Visualizing a global panorama of the food traceability systems through science mapping: Gaps and research opportunities.” This paper is now evaluating in a scientific journal for possible publishing. We present the original paper attached. SJR Q2
- The core of this master thesis shows a general description of Blockchain-IoT Sensor for Traceability Systems (BIoTS) in a scientific paper titled: “Blockchain-IoT Sensor (BIoTS): A solution to IoT-Ecosystems Security Issues.” The article was accepted in the journal Sensors, indexed in the JCR Q1. It will be published in the next few days. We present the original paper attached.

B. Appendix: BloTS' Internal Hardware Blocks

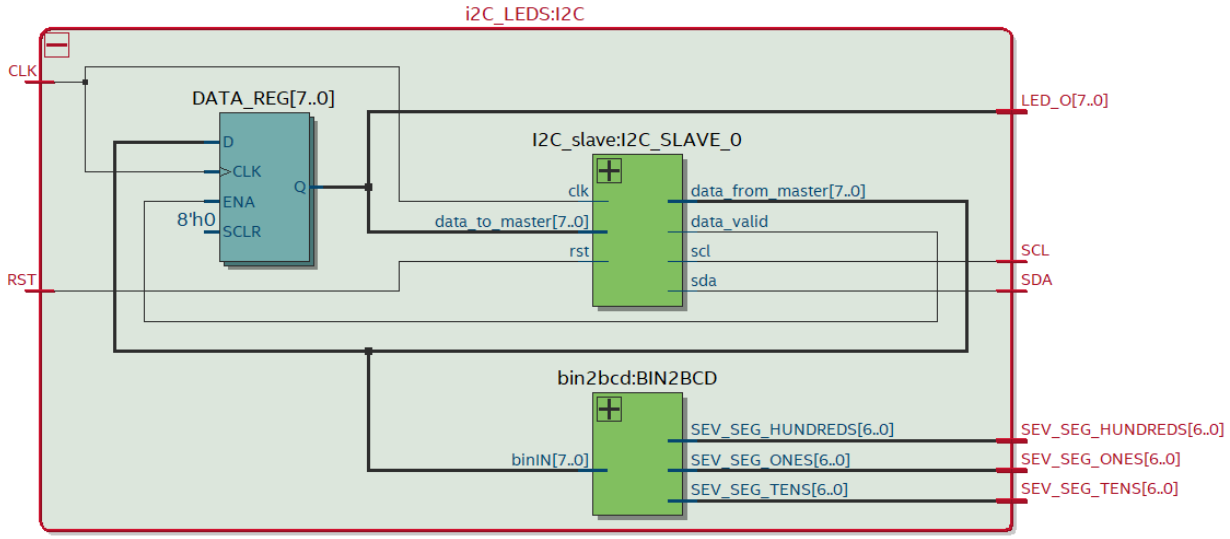


Figure B-1.: I2C Block Internal Description

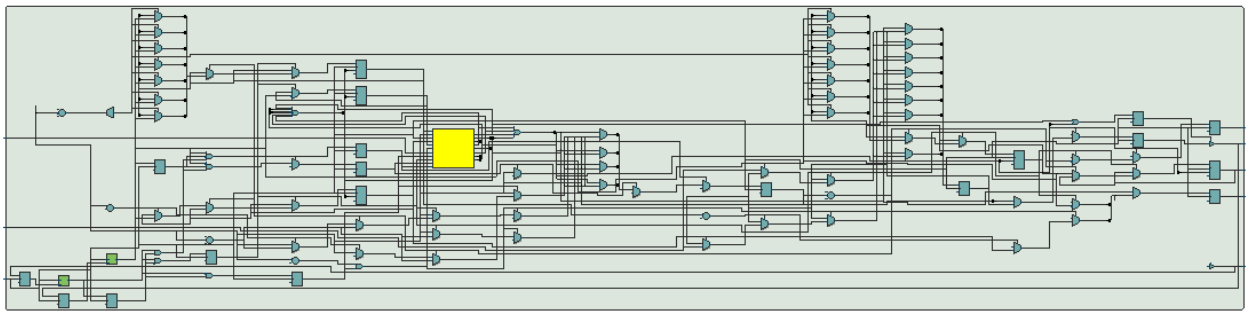


Figure B-2.: I2C Master-Slave

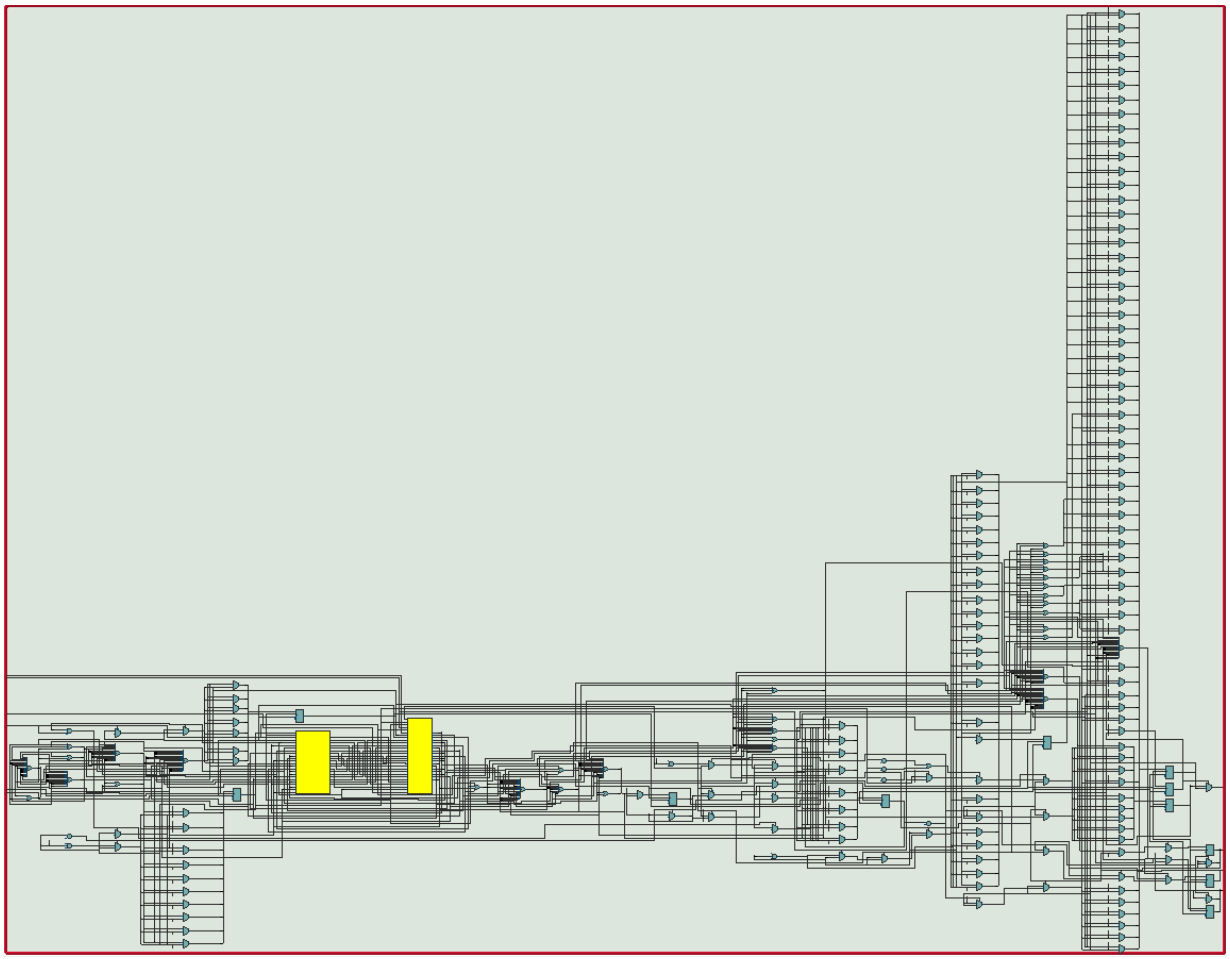


Figure B-3.: Schematic Blocks of SD-CARD General Design

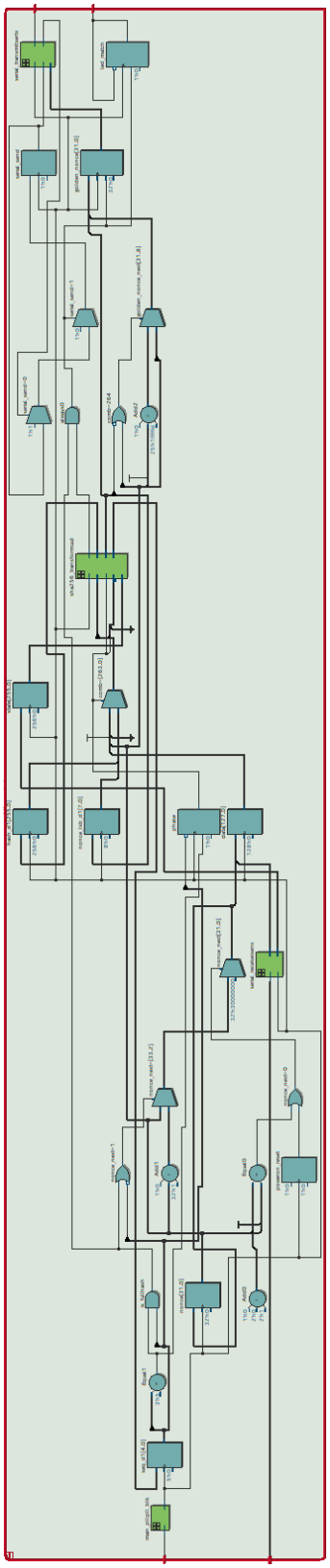


Figure B-4.: SHA-256 Block Internal Description

C. Appendix: BIoTS Schematic Diagram

Fig. **C-1** shows the electronic circuit design and the PCB of the BIoTS prototype device are done in the KiCAD software. This design includes all the modules referenced in the analog electronics stage and the FPGA module.

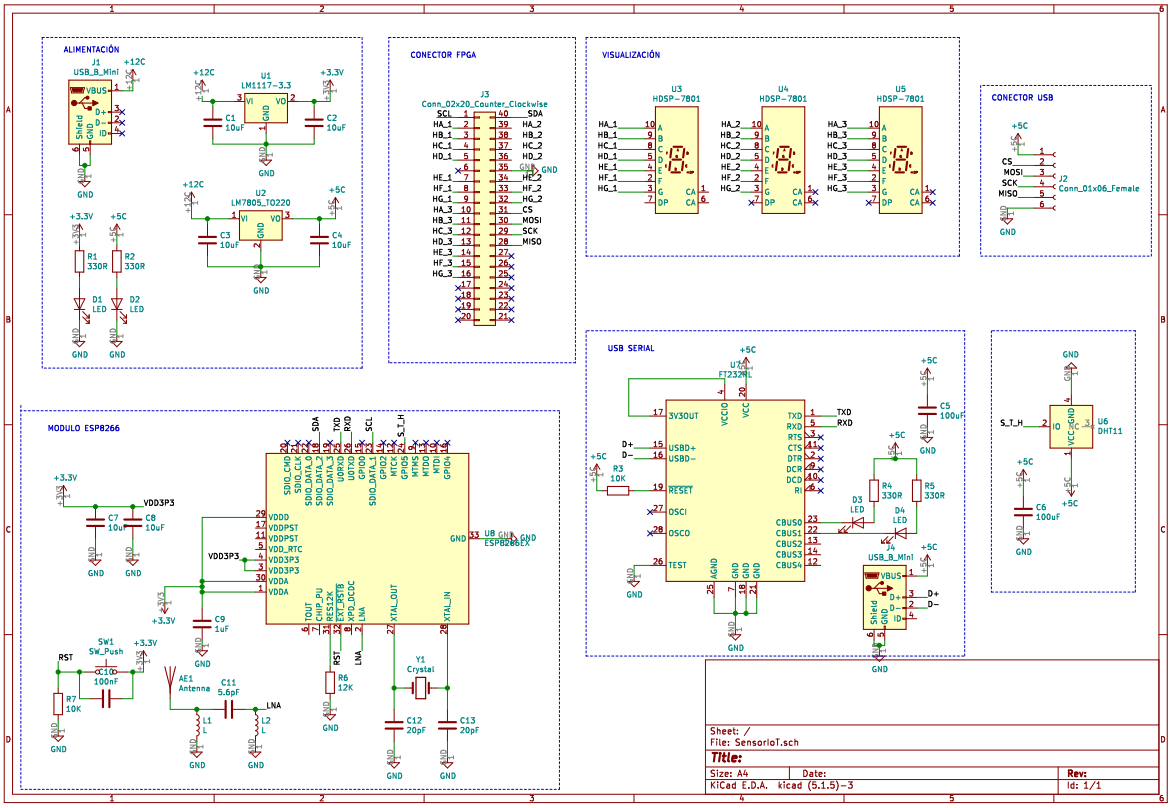


Figure C-1.: BIoTS Schematic Diagram

D. Appendix: Physical Design of BIoTS on PCB

Fig. **D-1** shows the electronic devices included in the PCB are surface mounted, and the board is designed as a double layer. This design is the prototype version of BIoTS, as it is expected to include the FPGA integrated circuit to omit the DE0-Nano board.

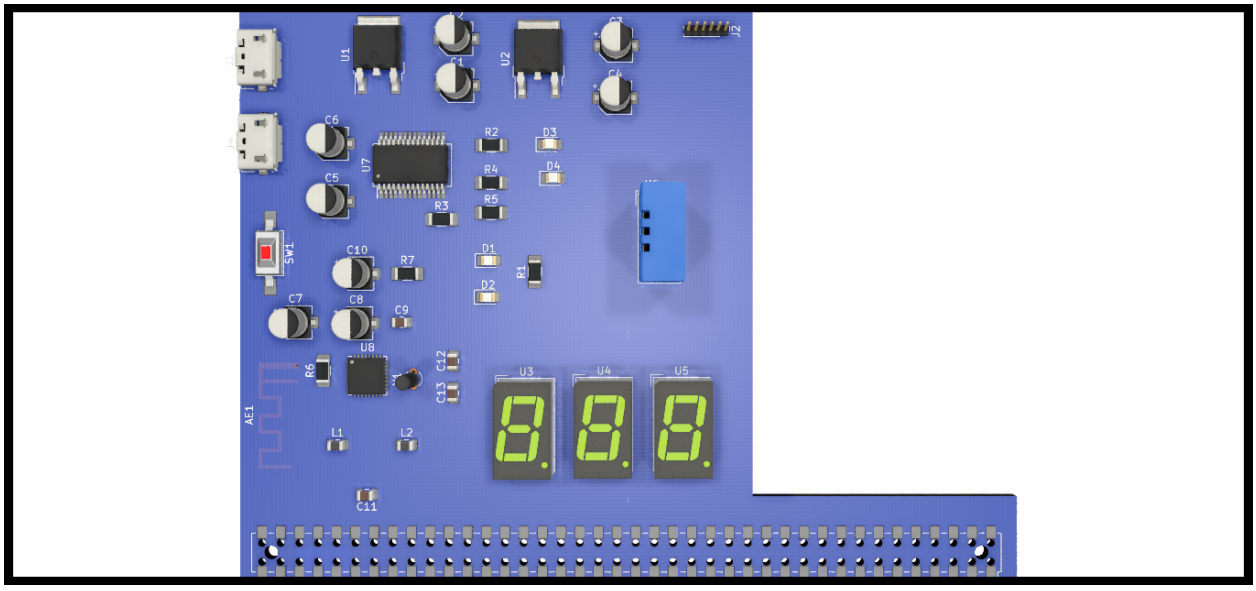


Figure D-1.: Physical Design of BIoTS on PCB

E. Appendix: BIoTS Prototype

Fig. **E-1** shows the physical design in its prototype version once it is moved to integrated circuit hardware in a professional Beta version. This BIoTS prototype is the result of the invention described throughout this thesis.

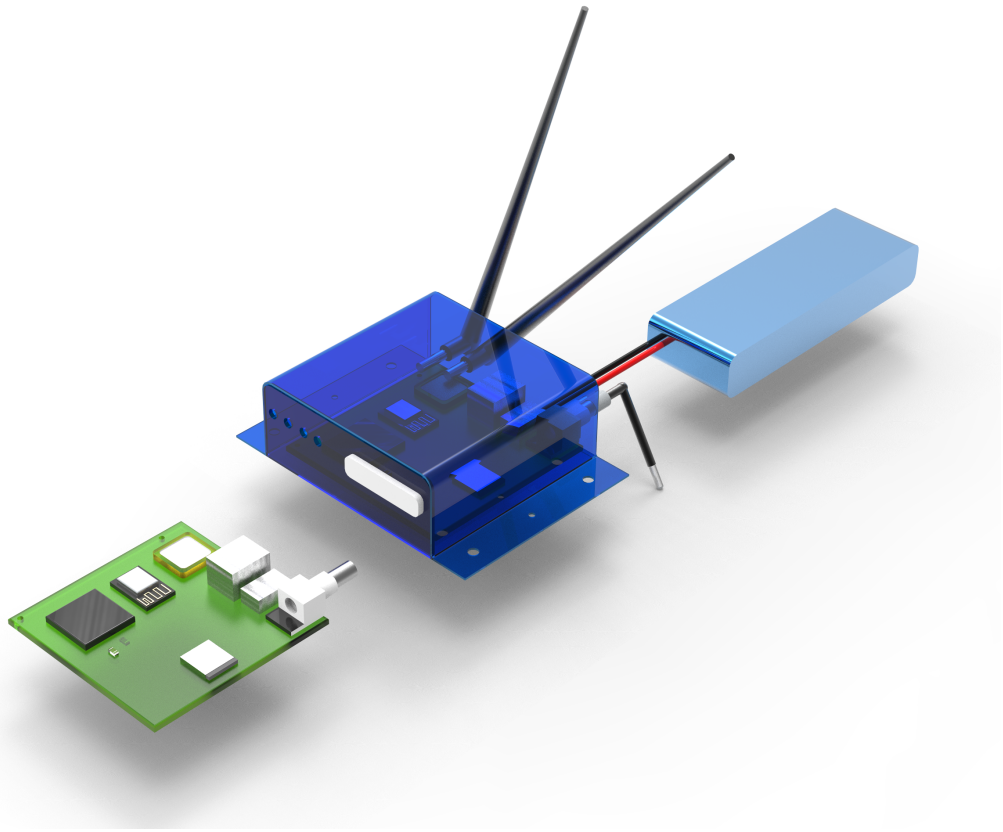


Figure E-1.: BIoTS Prototype

Bibliography

[1] D. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” 2014.

[2] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A review on consensus algorithm of blockchain,” in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2567–2572, 2017.

[3] N. Chaudhry and M. Yousaf, “Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities,” pp. 54–63, 12 2018.

[4] I. International trade centre, *TRACEABILITY IN FOOD AND AGRICULTURAL PRODUCTS*, vol. 91. 91 ed., 2015.

[5] L. Ramundo, M. Taisch, and S. Terzi, “State of the art of technology in the food sector value chain towards the iot,” in *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*, pp. 1–6, Sep. 2016.

[6] F. Gandino, B. Montrucchio, M. Rebaudengo, and E. R. Sanchez, “Analysis of an rfid-based information system for tracking and tracing in an agri-food chain,” in *2007 1st Annual RFID Eurasia*, pp. 1–6, Sep. 2007.

[7] G. Al, J. Rhee, H. Ahn, J. Lee, U. Farooq, M. Fazal, and M. A. Syaekhoni, “Integration of RFID , wireless sensor networks , and data mining in an e-pedigree food traceability system,” *Journal of food engineering*, vol. 212, pp. 65–75, 2017.

[8] F. Tian, “A Supply Chain Traceability System for Food Safety Based on HACCP , Blockchain & Internet of Things,” *IEEE*, 2012.

[9] M. A. L. Pena and I. M. Fernandez, “Sat-iot: An architectural model for a high-performance fog/edge/cloud iot platform,” in *2019 IEEE 5th World Forum on Internet of Things WF-IoT*, pp. 633–638, April 2019.

[10] A. R. Biswas and R. Giaffreda, “Iot and cloud convergence: Opportunities and challenges,” in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 375–376, March 2014.

[11] T. Qiu, H. Xiao, and P. Zhou, “Framework and case studies of intelligence monitoring platform in facility agriculture ecosystem,” in *2013 Second International Conference on Agro-Geoinformatics (Agro-Geoinformatics)*, pp. 522–525, Aug 2013.

[12] A. Khattab, A. Abdelgawad, and K. Yelmarthi, “Design and implementation of a cloud-based iot scheme for precision agriculture,” in *2016 28th International Conference on Microelectronics (ICM)*, pp. 201–204, Dec 2016.

[13] G. Suciu, C. Istrate, and M. Diţu, “Secure smart agriculture monitoring technique through isolation,” in *2019 Global IoT Summit (GIoTS)*, pp. 1–5, June 2019.

[14] FuBing, “Research on the agriculture intelligent system based on iot,” in *2012 International Conference on Image Analysis and Signal Processing*, pp. 1–4, Nov 2012.

[15] M. Singh, A. Singh, and S. Kim, “Blockchain: A game changer for securing iot data,” in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pp. 51–55, Feb 2018.

[16] G. Dittmann and J. Jelitto, “A blockchain proxy for lightweight iot devices,” in *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 82–85, June 2019.

[17] S. R. Niya, E. Schiller, I. Cepilov, F. Maddaloni, K. Aydinli, T. Surbeck, T. Bocek, and B. Stiller, “Adaptation of proof-of-stake-based blockchains for iot data streams,” in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 15–16, May 2019.

[18] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou, and B. Zhang, “A high performance blockchain platform for intelligent devices,” in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, pp. 260–261, Aug 2018.

[19] D. Fakhri and K. Mutijarsa, “Secure iot communication using blockchain technology,” in *2018 International Symposium on Electronics and Smart Devices (ISESD)*, pp. 1–6, Oct 2018.

[20] Y. Mezquita, “Internet of things platforms based on blockchain technology: A literature review,” *Advances in Intelligent Systems and Computing*, vol. 1004, pp. 205–208, 2020. cited By 0.

[21] T. Choudhary, C. Virmani, and D. Juneja, “Convergence of blockchain and iot: An edge over technologies,” *Studies in Computational Intelligence*, vol. 846, pp. 299–316, 2020. cited By 0.

[22] M. Dabbagh, M. Kakavand, and M. Tahir, “Towards integration of blockchain and iot: A bibliometric analysis of state-of-the-art,” *Advances in Intelligent Systems and Computing*, vol. 1010, pp. 27–35, 2020. cited By 0.

[23] D. Miranda, G. Fischer, and C. Carranza, *Los frutales caducifolios en Colombia-Situación actual, sistemas de cultivo y plan de desarrollo*. Bogotá, Colombia, DC: Ind, 1 ed., 2013.

[24] E. Gargouri and S. Hammadi, “An hybrid approach for a supply chain management in agro-food industries,” in *IEEE International Conference on Systems, Man and Cybernetics*, vol. 6, pp. 6 pp. vol.6–, Oct 2002.

[25] L. Carlson and V. Bitsch, “Applicability of transaction cost economics to understanding organizational structures in solidarity-based food systems in germany,” *Sustainability (Switzerland)*, vol. 11, no. 4, 2019. cited By 0.

[26] Z. Leng, P. Zhao, and X. Wang, “Study on the price mechanism and the policies of government for integration a rice supply chain,” in *2010 International Conference on Logistics Systems and Intelligent Management (ICLSIM)*, vol. 3, pp. 1573–1579, Jan 2010.

[27] D. Boyer, J. Sarkar, and A. Ramaswami, “Diets, food miles, and environmental sustainability of urban food systems: Analysis of nine indian cities,” *Earth’s Future*, vol. 7, no. 8, pp. 911–922, 2019. cited By 0.

[28] D. Matzembacher and F. Meira, “Sustainability as business strategy in community supported agriculture: Social, environmental and economic benefits for producers and consumers,” *British Food Journal*, vol. 121, no. 2, pp. 616–632, 2019. cited By 1.

[29] J. Andrei, R. Ion, L. Chivu, R. Pop, and A. Marin, “Investigations on farmers’ willingness to associate and join in environmental responsible short supply chain in romania,” *Applied Ecology and Environmental Research*, vol. 17, no. 2, pp. 1617–1639, 2019. cited By 0.

[30] T. Taha and R. Abdullah, “Keynote speakers big data and the internet of things (iot) challenges and opportunities,” in *2017 8th International Conference on Information Technology (ICIT)*, pp. 1–2, May 2017.

[31] L. Wei, W. Miao, C. Jiang, B. Guo, W. Li, J. Han, R. Liu, and J. Zou, “Power wireless private network in energy iot: Challenges, opportunities and solutions,” in *2017 International Smart Cities Conference (ISC2)*, pp. 1–4, Sep. 2017.

[32] F. Wang, R. Cao, W. Ding, H. Qian, and Y. Gao, “Incentives to enable food traceability and its implication on food traceability system design,” in *Proceedings of 2011 IEEE International Conference on Service Operations, Logistics and Informatics*, pp. 32–37, July 2011.

[33] R. Hou and X. Zhu, “The application of rfid technology in the food traceability system,” in *2012 International Conference on Industrial Control and Electronics Engineering*, pp. 788–791, Aug 2012.

[34] L. Xu and L. Wu, “The application of e-commerce in food traceability system - based on the analysis of consumers’ behavior of online searching for traceability information,” in *2009 International Conference on Management and Service Science*, pp. 1–4, Sep. 2009.

[35] J. Jiang, T. Lin, C. Wang, M. Liao, C. Chou, and C. Chen, “Integration of an automatic agricultural and livestock production management system and an agriculture and food traceability system based on the internet of things technology,” in *2017 Eleventh International Conference on Sensing Technology (ICST)*, pp. 1–7, Dec 2017.

[36] M. Khan and K. Salah, “Iot security: Review, blockchain solutions, and open challenges,” *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018. cited By 154.

[37] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, “End-to-end transport security in the ip-based internet of things,” in *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–5, July 2012.

[38] P. Urien, “Blockchain iot (biot): A new direction for solving internet of things security and trust issues,” in *2018 3rd Cloudification of the Internet of Things (CIoT)*, pp. 1–4, July 2018.

[39] R. Badia-melis, P. Mishra, and L. Ruiz-garcia, “Food traceability : New trends and recent advances . a review,” *Food Control*, vol. 57, pp. 393–401, 2015.

[40] T. Bosona and G. Gebresenbet, “Food traceability as an integral part of logistics management in food and agricultural supply chain,” *Food Control*, vol. 33, no. 1, pp. 32–48, 2013.

[41] T. Gomiero, “Food quality assessment in organic vs . conventional agricultural produce : Findings and issues,” *Applied Soil Ecology*, no. October, pp. 0–1, 2017.

[42] Y. Yun and W. Kun, “The key technology research of quality and safety traceability systems of agricultural products,” in *2015 International Conference on Intelligent Transportation, Big Data and Smart City*, pp. 880–882, Dec 2015.

[43] R. Schmidt and A. Gagnon, “A new worldwide tracebility technology to complement gps,” in *2007 41st Annual IEEE International Carnahan Conference on Security Technology*, pp. 125–132, Oct 2007.

[44] W. Cao, L. Zheng, H. Zhu, and P. Wu, “Studies of epc encoding and privacy of rfid tag in traceability systems,” in *2010 World Automation Congress*, pp. 383–387, Sep. 2010.

[45] M. Miao, X. Liu, Y. Duan, R. Wang, and Z. Fu, “Critical success factors for implementing traceability systems in chinese food enterprises,” in *2011 International Conference on Management and Service Science*, pp. 1–4, Aug 2011.

[46] Y. Cao, F. Jia, and G. Manogaran, “Efficient traceability systems of steel products using blockchain-based industrial internet of things,” *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.

[47] M. Trebar, A. Grah, A. A. Melcon, and A. Parreno, “Towards rfid traceability systems of farmed fish supply chain,” in *SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks*, pp. 1–6, Sep. 2011.

[48] Ke Zhang, Yi Chai, S. X. Yang, and G. S. Mittal, “Pre-warning analysis in traceability systems for food production supply chains,” in *2009 World Congress on Nature Biologically Inspired Computing (NaBIC)*, pp. 233–238, Dec 2009.

[49] S. Liu, H. Zheng, H. Meng, H. Hu, J. Wu, and C. Li, “Study on quality safety traceability systems for cereal and oil products,” in *2009 WRI World Congress on Software Engineering*, vol. 1, pp. 163–166, May 2009.

[50] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, “Blockchain-based traceability in agri-food supply chain management: A practical implementation,” in *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)*, pp. 1–4, May 2018.

[51] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc ’05, (New York, NY, USA), pp. 46–57, ACM, 2005.

[52] G. Noubir and G. Lin, “Low-power dos attacks in data wireless lans and countermeasures,” *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, pp. 29–30, July 2003.

[53] Y. . P. Hong, P. Lan, and C. . J. Kuo, “Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches,” *IEEE Signal Processing Magazine*, vol. 30, pp. 29–40, Sep. 2013.

[54] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 492–503, 2009. cited By 61.

[55] T. Bhattasali and R. Chaki, "A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network," in *Advances in Network Security and Applications* (D. C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, and D. Nagamalai, eds.), (Berlin, Heidelberg), pp. 268–280, Springer Berlin Heidelberg, 2011.

[56] R. Riaz, K. Kim, and H. F. Ahmed, "Security analysis survey and framework design for ip connected lowpans," in *2009 International Symposium on Autonomous Decentralized Systems*, pp. 1–6, March 2009.

[57] J. Granjal, E. Monteiro, and J. S. Silva, "Network-layer security for the internet of things using tinyos and blip," *International Journal of Communication Systems*, vol. 27, no. 10, pp. 1938–1963, 2014.

[58] J. Granjal, E. Monteiro, and J. S. Silva, "Enabling network-layer security on ipv6 wireless sensor networks," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pp. 1–6, Dec 2010.

[59] P. Mahalle, B. Anggorojati, N. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," *Journal of Cyber Security and Mobility*, vol. 1, no. 4, pp. 309–348, 2013. cited By 3.

[60] G. Peretti, V. Lakkundi, and M. Zorzi, "Blinktoscoap: An end-to-end security framework for the internet of things," in *2015 7th International Conference on Communication Systems and Networks (COMSNETS)*, pp. 1–6, Jan 2015.

[61] R. Wang, J. He, C. Liu, Q. Li, W. Tsai, and E. Deng, "A privacy-aware pki system based on permissioned blockchains," in *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, pp. 928–931, Nov 2018.

[62] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "Nutbaas: A blockchain-as-a-service platform," *IEEE Access*, vol. 7, pp. 134422–134433, 2019.

[63] C. Ehmke, F. Wessling, and C. M. Friedrich, "Proof-of-property - a lightweight and scalable blockchain protocol," in *2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pp. 48–51, May 2018.

[64] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to iot applications and beyond," *IEEE Internet of Things Journal*, vol. 6, pp. 8114–8154, Oct 2019.

[65] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, and B. M. Boshkoska, "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions," *COMPUTERS IN INDUSTRY*, vol. 109, pp. 83–99, AUG 2019.

[66] M. Diaz, C. Martin, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," *JOURNAL OF NETWORK AND COMPUTER APPLICATIONS*, vol. 67, pp. 99–117, MAY 2016.

[67] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149 – 160, 2018.

[68] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: From sensors to the internet of things," *Future Generation Computer Systems*, vol. 75, pp. 46 – 57, 2017.

[69] M. Samaniego and R. Deters, "Internet of smart things - iost: Using blockchain and clips to make things autonomous," in *2017 IEEE International Conference on Cognitive Computing (ICCC)*, pp. 9–16, June 2017.

[70] J. Yeh, S. Liao, Y. Wang, and Y. Chen, "Understanding consumer purchase intention in a blockchain technology for food traceability and transparency context," in *2019 IEEE Social Implications of Technology (SIT) and Information Management (SITIM)*, pp. 1–6, Nov 2019.

[71] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-driven iot for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019.

[72] H. Wu, J. Cao, Y. Yang, C. L. Tung, S. Jiang, B. Tang, Y. Liu, X. Wang, and Y. Deng, "Data management in supply chain using blockchain: Challenges and a case study," in *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–8, July 2019.

[73] Feng Tian, "An agri-food supply chain traceability system for china based on rfid blockchain technology," in *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1–6, June 2016.

[74] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *2017 IEEE Technology Engineering Management Conference (TEMSCON)*, pp. 137–141, June 2017.

[75] S. Figorilli, F. Antonucci, C. Costa, F. Pallottino, L. Raso, M. Castiglione, E. Pinci, D. D. Vecchio, G. Colle, A. R. Proto, G. Sperandio, and P. Menesatti, "A blockchain

implementation prototype for the electronic open source traceability of wood along the whole supply chain," in *Sensors*, 2018.

[76] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, pp. 1184–1195, April 2018.

[77] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," *ArXiv*, vol. abs/1608.05187, 2016.

[78] M. Young and R. Boutaba, "Overcoming adversaries in sensor networks: A survey of theoretical models and algorithmic approaches for tolerating malicious interference," *IEEE Communications Surveys Tutorials*, vol. 13, pp. 617–641, Fourth 2011.

[79] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, WiSe '04, (New York, NY, USA), pp. 80–89, ACM, 2004.

[80] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in iot: A novel perspective," *Information*, vol. 7, no. 3, 2016.

[81] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Transactions on Information Forensics and Security*, vol. 9, pp. 1617–1628, Oct 2014.

[82] M. Demirbas and Y. Song, "An rssi-based scheme for sybil attack detection in wireless sensor networks," in *2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06)*, pp. 5 pp.–570, June 2006.

[83] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, pp. 492–503, Sep. 2009.

[84] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 193–202, June 2007.

[85] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 2418–2434, Jun 2010.

[86] Q. Li and W. Trappe, "Light-weight detection of spoofing attacks in wireless networks," in *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 845–851, Oct 2006.

[87] T. Bhattasali and R. Chaki, “A survey of recent intrusion detection systems for wireless sensor network,” in *Advances in Network Security and Applications* (D. C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, and D. Nagamalai, eds.), (Berlin, Heidelberg), pp. 268–280, Springer Berlin Heidelberg, 2011.

[88] A. Dvir, T. Holczer, and L. Buttyan, “Vera - version number and rank authentication in rpl,” in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, pp. 709–714, Oct 2011.

[89] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, pp. 120–126, Feb. 1978.

[90] W. Hong, Y. Cai, Z. Yu, and X. Yu, “An agri-product traceability system based on iot and blockchain technology,” in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, pp. 254–255, Aug 2018.

[91] P. Danzi, A. E. Kalør, Stefanović, and P. Popovski, “Delay and communication tradeoffs for blockchain systems with lightweight iot clients,” *IEEE Internet of Things Journal*, vol. 6, pp. 2354–2365, April 2019.

[92] S. Kushch and F. Prieto-Castrillo, “Blockchain for dynamic nodes in a smart city,” in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 29–34, April 2019.

[93] S. Huh, S. Cho, and S. Kim, “Managing iot devices using blockchain platform,” in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, pp. 464–467, Feb 2017.

[94] J. Jemal and K. T. Kornegay, “Security assessment of blockchains in heterogenous iot networks : Invited presentation,” in *2019 53rd Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–4, March 2019.

[95] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, “Internet of things security: A survey,” *Journal of Network and Computer Applications*, vol. 88, pp. 10 – 28, 2017.

[96] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the internet of things: perspectives and challenges,” *Wireless Networks*, vol. 20, no. 8, pp. 1572–8196, 2014.

[97] J. Astill, R. A. Dara, M. Campbell, J. M. Farber, E. D. Fraser, S. Sharif, and R. Y. Yada, “Transparency in food supply chains: A review of enabling technology solutions,” *Trends in Food Science Technology*, vol. 91, pp. 240 – 247, 2019.

[98] S. Aich, S. Chakraborty, M. Sain, H. Lee, and H. Kim, “A review on benefits of iot integrated blockchain based supply chain management implementations across different sectors with case study,” in *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pp. 138–141, Feb 2019.

[99] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, “Security and privacy for cloud-based iot: Challenges,” *IEEE Communications Magazine*, vol. 55, pp. 26–33, January 2017.

[100] M. Sethi, J. Arkko, and A. Keränen, “End-to-end security for sleepy smart object networks,” in *37th Annual IEEE Conference on Local Computer Networks - Workshops*, pp. 964–972, Oct 2012.

[101] V. Román and J. Ordieres-Meré, “Wip iot blockchain technologies for smart sensors based on raspberry pi,” in *2018 IEEE 11th Conference on Service-Oriented Computing and Applications (SOCA)*, pp. 216–220, 2018.

[102] J. d. La Beaujardiere, R. Mital, and R. Mital, “Blockchain application within a multi-sensor satellite architecture,” in *IGARSS 2019 - 2019 IEEE International Geoscience and Remote Sensing Symposium*, pp. 5293–5296, 2019.

[103] W. She, Q. Liu, Z. Tian, J. Chen, B. Wang, and W. Liu, “Blockchain trust model for malicious node detection in wireless sensor networks,” *IEEE Access*, vol. 7, pp. 38947–38956, 2019.

[104] Y. Liu, B. Wei, Y. Du, F. Xiao, and Y. Deng, “Identifying influential spreaders by weight degree centrality in complex networks,” *Chaos, Solitons Fractals*, vol. 86, pp. 1 – 7, 2016.

[105] G. Zhao, Y. Guo, X. Sun, and X. Wang, “A system for pesticide residues detection and agricultural products traceability based on acetylcholinesterase biosensor and internet of things,” *International Journal of Electrochemical Science*, vol. 10, pp. 3387–3399, 01 2015.

[106] U. I. Zou Zhuo, Chen Qing and Z. Lirong, “Radio frequency identification enabled wireless sensing for intelligent food logistics phil.,” *Trans. R. Soc.*, vol. 10, pp. 1237–1245, 06 2014.

[107] S.-M. Seo, S.-W. Kim, J.-W. Jeon, J.-H. Kim, H.-S. Kim, J.-H. Cho, W.-H. Lee, and S.-H. Paek, “Food contamination monitoring via internet of things, exemplified by using pocket-sized immunosensor as terminal unit,” *Sensors and Actuators B: Chemical*, vol. 233, pp. 148 – 156, 2016.

[108] R. Badia-Melis and L. Ruiz-Garcia, “11 - real-time tracking and remote monitoring in food traceability,” in *Advances in Food Traceability Techniques and Technologies*, Woodhead Publishing Series in Food Science, Technology and Nutrition, pp. 209 – 224, Woodhead Publishing, 2016.

[109] R. Badia-Melis, U. M. Carthy, L. Ruiz-Garcia, J. Garcia-Hierro, and J. R. Villalba, “New trends in cold chain monitoring applications - a review,” *Food Control*, vol. 86, pp. 170 – 182, 2018.

[110] R.-Y. Chen, “Autonomous tracing system for backward design in food supply chain,” *Food Control*, vol. 51, pp. 70 – 84, 2015.

[111] T. Hu, M. Zheng, and L. Zhu, “Research application of the internet of things monitor platform in meat processing industry,” in *Proceedings of the International Conference on Human-centric Computing 2011 and Embedded and Multimedia Computing 2011* (H. Park, Jame J.and Jin and R. Liao, Xiaofeiand Zheng, eds.), (Dordrecht), pp. 165–172, Springer Netherlands, 2011.

[112] M. Markovic, P. Edwards, M. Kollingbaum, and A. Rowe, “Modelling provenance of sensor data for food safety compliance checking,” in *Provenance and Annotation of Data and Processes* (M. Mattoso and B. Glavic, eds.), (Cham), pp. 134–145, Springer International Publishing, 2016.

[113] J. Tervonen, “Experiment of the quality control of vegetable storage based on the internet-of-things,” *Procedia Computer Science*, vol. 130, pp. 440 – 447, 2018. The 9th International Conference on Ambient Systems, Networks and Technologies (ANT 2018) / The 8th International Conference on Sustainable Energy Information Technology (SEIT-2018) / Affiliated Workshops.

[114] M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an analysis of security issues, challenges, and open problems in the internet of things,” in *2015 IEEE World Congress on Services*, pp. 21–28, 2015.

[115] X. Shi, X. An, Q. Zhao, H. Liu, L. Xia, X. Sun, and Y. Guo, “State-of-the-art internet of things in protected agriculture,” *Sensors*, vol. 19, p. 1833, 04 2019.

[116] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, “Trustchain: Trust management in blockchain and iot supported supply chains,” in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 184–193, 2019.

[117] L. V. T. Duong, N. T. T. Thuy, and L. D. Khai, “A fast approach for bitcoin blockchain cryptocurrency mining system,” *Integration*, vol. 74, pp. 107–114, 2020.

[118] W. Wang, H. Dinh Thai, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. PP, pp. 1–1, 01 2019.

[119] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[120] Z. Ren, K. Cong, J. Pouwelse, and E. Zekeriya, "Implicit consensus: Blockchain with unbounded throughput," 05 2017.

[121] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism consortium blockchain," in *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 466–473, 2017.

[122] K. Christodoulou, E. Iosif, A. Inglezakis, and M. Themistocleous, "Consensus crash testing: Exploring ripple's decentralization degree in adversarial environments," *Future Internet*, vol. 12, no. 3, 2020.

[123] S. Jeon, I. Doh, and K. Chae, "Rmbc: Randomized mesh blockchain using dbft consensus algorithm," in *2018 International Conference on Information Networking (ICOIN)*, pp. 712–717, 2018.

[124] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services," *IEEE Transactions on Services Computing*, vol. 12, no. 3, pp. 429–445, 2019.

[125] J. Ruiz-Rosero, G. Ramirez-Gonzalez, and R. Khanna, "Field programmable gate array applications—a scientometric review," *Computation*, vol. 7, no. 4, 2019.

[126] J. Xu, X. Meng, W. Liang, H. Zhou, and K. C. Li, "A secure mutual authentication scheme of blockchain-based in wbans," *China Communications*, vol. 17, no. 9, pp. 34–49, 2020.