IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 31, 2021, accepted April 15, 2021, date of publication April 22, 2021, date of current version April 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3074874

A Blockchain-Based Traceability System in Agri-Food SME: Case Study of a Traditional Bakery

LUISANNA COCCO[1], KATIUSCIA MANNARO[1], ROBERTO TONELLI[1], (Member, IEEE), LORENA MARIANI[2,3], MATTEO B. LODI[2], (Graduate Student Member, IEEE), ANDREA MELIS[2], MARCO SIMONE[2], AND ALESSANDRO FANTI[2], (Member, IEEE)

[1]Department of Mathematics and Computer Science, University of Cagliari, 09123 Cagliari, Italy
[2]Department of Electrical and Electronic Engineering, University of Cagliari, 09123 Cagliari, Italy
[3]Studio-A Automazione s.r.l, 09038 Serramanna, Italy

Corresponding authors: Alessandro Fanti (alessandro.fanti@unica.it) and Katiuscia Mannaro (katiuscia.mannaro@unica.it)

This work was supported in part by the Project ''Ingegnerizzazione e Automazione del Processo di Produzione Tradizionale del Pane Carasau mediante l'utilizzo di tecnologie IoT (IAPC)'', funded by Ministero dello Sviluppo Economico, in AGRIFOOD PON I&C 2014–2020 under Grant CUP: B21B19000640008 COR: 1406652, and in part by the Sardegna Ricerche-Regione Autonoma della Sardegna—R&D Program Agroindutria—POR FESR Sardegna 2014–2020—Azione 1.2.2—under Project ''Crunch-Sunalle'' under Grant CUP: F26C18000350006, and in part by Sardegna Ricerche-Regione Autonoma della Sardegna—R&D Program Agroindutria—POR FESR Sardegna 2014–2020—Azione 1.2.2—under Project ''Complete Assessment of Smart contracts and Coin Offers (C.A.S.C.O.)'' under project code: 2014IT16RFOP015.

ABSTRACT In this paper we present a blockchain based system for the supply chain management of a particular Italian bread. Goal of the system is to guarantee a transparent and auditable traceability of the Carasau bread where each actor of the supply chain can verify the quality of the products and the conformity to the normative about the hygienic-sanitary conditions along the chain. To realize this system we relied on the Blockchain and the Internet of Thing technologies in order to provide a trustless environment, in which trust is placed in cryptography, in mathematical operations and on the network, and not in public or private companies. Thanks to the use of digital technologies the system aims to reduce the data entry errors and the risk of tampering. Our system is designed so that along the supply chain, the nodes equipped with several sensors directly communicate their data to Raspberry Pi units that elaborate and transmit them to Interplanetary File System and to the Ethereum Blockchain. Furthermore, we designed ad hoc Radio Frequency Identification and Near Field communication tags to shortly supply the proposed system with information about the products and batches. The dedicated RFID tags robustness during on-bread operation was numerically tested. The system will easily allow end consumers to have a transparent view on the whole journey from raw material to purchased final product and a supervisory authority to perform online inspections on the products' quality and on the good working practices.

INDEX TERMS Ethereum smart contracts, Interplanetary File System, agri-food supply chain, wireless sensors network, decentralized application.

I. INTRODUCTION

Blockchain technology is a new paradigm for distributed, decentralized and immutable ledger database that in the last few years attracted the attention of several researchers and companies due to the benefits that it could provide over existing solutions and for multiple fields and applications. Among the various benefits, blockchain technology can assure immutability and integrity of data without the need of a third trusted party and is perfectly suited to solve problems in sectors in which numerous untrusted actors have to operate/work together.

One of such sectors is represented by the agri-food industry. What people eat is now a matter of great importance especially in aspects related to health and safety. Controlling products quality and conformity to the current regulations in food industry, throughout its supply chain, is today one major challenge especially when it comes to typical food

The associate editor coordinating the review of this manuscript and approving it for publication was Wenbing Zhao.

products, that is products closely linked to their territory. Apaiah et al. [1] asserted that, contrary to other supply chains, the quality of the agri-food products along their supply chain, from the time in which the raw materials leave the grower, to the time in which the products reach the consumer, can change continuously. In addition typical agri-food supply chain is little digitalized. Food documentation about provenance and food properties are typically stored on paper and/or on private databases, and can only be inspected by trusted third-party authorities ([2], [3]).

In this paper we present a blockchain based system for the supply chain management of the Carasau bread, that is a traditional Sardinian bread, obtained from remilled semolina of durum wheat grown exclusively in Sardinia. Carasau bread is classified as Italian Traditional Agrifood Product (PAT). This is an official approval for traditional Italian regional food products similar to the Protected Geographical Status of the European Union. Carasau bread is an Italian excellence, with a limited production, linked to a territory and its history. The requirements to be recognized as such are to be obtained with processing, preservation and seasoning methods that are consolidated over time and homogeneous within the entire territory concerned, for a period of not less than twenty-five years, according to traditional rules. The definition of quality is not univocal as it must be defined with respect to the ability of a given good or service to satisfy the expressed or latent needs of end customers. The concept of quality has taken on more and more meanings over time to try to achieve maximum customer satisfaction, so that its achievement is necessary for the production company to remain competitive in the market. Insurance of products' quality implies the adoption of transparency requirements that can be achieved using a traceability system. The International Standards Organization by the *ISO 8402:1994* Standard [4] defines the quality as *"the totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs revolving around customer"*. Foods produced with traditional methods are increasingly appreciated by the end consumer for theirs reliability and genuineness.

Regulation (EC) n. 178/2002 of the European Parliament established a mandatory traceability system for food safety in 2005 to allow the authority in charge to intervene throughout the supply chain to identify and eliminate food hazards. The introduction of a documented traceability system makes all companies responsible of the entire supply chain in compliance with regulations to protect the characteristics of the products.

In general, the concept of quality of a food product is an articulated concept, which can be defined differently by the various actors. In an agri-food supply chain there are different actors involved that may perceive the concept of quality of a food product in different ways, depending on their different backgrounds and on their role in the supply chain.

Thus if we consider the case of the Carasau bread supply chain, grain quality is perceived in a different way by all the actors involved in the chain from the producer to the end consumer. For example from the point of view of the producer of wheat the quality is linked to the varietal purity and the degree of germination of the seeds while for the milling industry, the quality is dictated by the percentage of ash, the hectolitre weight, the uniformity and the size of the grain. Finally, just to give some examples, from the point of view of the final consumer, quality is linked to a healthy and nutritious product, to the origin of the products, to the absence of contaminants and to the ecological impact linked to its production.

In the light of these considerations, the main purpose of this paper is to propose a system to ensure a transparent and auditable traceability of a specific agri-food supply chain in such a way that each actor of the supply chain can verify the quality of the products and the conformity to the normative about the hygienic-sanitary conditions along the chain.

The proposed system will lead to a reduction in data entry errors and in addiction will provide reliable data on product traceability and a reduction in the risk of tampering thanks to the use of the Blockchain and the Internet of Thing (IoT) technologies such as Radio-Frequency Identification (RFID) and Near Field Communication (NFC). The information provided by a specific actor/sensor in the chain can directly be ascribed to him/it, and cannot be deleted or tampered with. At the same time the data entering and exiting from each supply chain's node/component can demonstrate the quality of all the intermediate products, and the conditions in which each actor operates along the chain.

This paper is an extended version of the work presented in [5] and presents a complete implementation of the proposed model. Specifically we illustrate in detail the implementation of the smart contract (see section IV-C1), and of the interaction between IPFS and Blockchain (see section IV-D), entering also in the detail of the RFID and NFC technologies used in order to design instruments for the traceability of the batches and for the check of the nodes along the supply chain (see section IV-E).

The main contributions of this paper are summarized as follows. The paper presents a decentralized application that deals with the development and implementation of a smart contract that manages the logic of the whole Carasau bread supply chain, so that each actor of the chain can verify the quality of the batches/products along the chain, and assure that batches/products are safe, will not cause harm to the consumer, and are suitable for consumption.

In addition, since effective hygiene control is also essential to avoid negative health consequences, the system enables the actors to verify the conformity to good hygiene practices, that are the basic conditions to maintain a hygienic environment, for example to comply with the HACCP requirements (see sections IV-C and IV-D for more details).

We conceived the Carasau supply chain as a chain of components/nodes from which batches/products enter and exit, so that along the supply chain under study there are nodes equipped with sensors for the monitoring of temperature and humidity, nodes equipped with sensors for the monitoring

of the presence of mycotoxins, chemical residues, or ash in the wheat, flour and bread, and nodes equipped with optical cameras for monitoring the storage points and the working practices. A detailed description of how the Carasau supply chain operates is shown in section III. Every sensor, just quoted, is connected to a Wifi network and/or to a router in a local connection. Each node directly communicates its data to a Raspberry Pi, that is a processing unit that can store, elaborate and transmit data to IPFS and Ethereum Blockchain, as described in detail in Section IV. In addition we implemented and simulated the logic that allows actors to retrieve information on batches/products in the chain through ad hoc designed RFID and NFC tags (see section IV-E for more details).

Note that this work is part of the *UniCarasau* research industry project, in which the design, functioning and characterization of Wireless Sensor Networks (WSNs) to allow the real-time monitoring of the processing parameters of the Carasau bread manufacturing has been already dealt with. The project, along our paper, aims to further advance in the monitoring of the food industry, especially bakeries, and to give *value* to the food product, especially Carasau bread.

The paper is organized as follows. Section II gives an overview about Blockchain applications and research works present in the market and in literature respectively. Section III presents a brief overview of the Carasau Bread supply chain. Section IV describes in detail the proposed decentralized Application (dApp) and its subsystems. Finally, Section V concludes the paper.

II. RELATED WORK

Today more than ever the demand for transparency and traceability in food supply chain has become a relevant challenge to face, given the growing interest of customers in knowing what happens in the path of the food product from field to table.

The combination of Internet of Things with blockchain technologies has become strategic to ensure traceability along the agri-food chain. According to Aung and Chang [6], Radio-frequency identification (RFID), Near Field Communication (NFC) devices and sensor based systems will be widely used both for tracking the goods in the supply chain and also for monitoring the quality of the products itself; and according to Rejeb *et al.* [7] the combination of the Blockchain technology with IoT devices enhances the supply chain integrity, and impacts positively on scalability, security, immutability and auditing, information flows, traceability and interoperability of the systems.

In the last years many decentralized traceability systems have been proposed. Tian [8] proposed a decentralized traceability system for real-time food monitoring and tracing based on Hazard Analysis and Critical Control Points (HACCP), IoT and Blockchain technology, precisely BigchainDB. Huang *et al.* [9] proposed a safe food traceable scheme based on Ethereum blockchain and smart contract to effectively execute transactions and encoding food by EPC technology. In addition, they proposed a data management system structure combining on-chain and off-chain data. Baralla *et al.* [10] designed and developed a blockchain oriented platform to guarantee the origin and provenance of food products in a Smart Tourism Region context. The system interfaces with IoT network devices providing detailed information about data monitoring such as storage temperature, environment humidity, and other data suitable to manage cold chain. Baralla *et al.* [11] proposed a generic agri-food supply chain traceability system based on Hyperledger Sawtooth Blockchain technology to reconstruct the product's history in order to verify product's health and quality, thanks to digital data coming from RFID, IoT devices and sensors. Mondal *et al.* [12] propose a blockchain inspired Internet-of-Things architecture for creating a transparent food supply chain. In their architecture they integrate a RFID-based sensor at the physical layer and blockchain at the cyber layer. RFID provides a unique identity of the product and the sensor data help in real time quality monitoring. In addition, the authors fabricated a small feature size 900-MHz RFID coupled sensor and demonstrated for real time sensor data acquisition.

In their study, Zhang *et al.* [13] proposed a system architecture based on blockchain technology to achieve the sharing and the exchange of information in the entire grain supply chain, to ensure the safety and reliability of information storage in the entire grain supply chain and also designed a multimode storage mechanism to improve blockchain storage efficiency. They designed customized smart contracts and instantiated a prototype system based on Hyperledger Fabric. The prototype was tested and verified thanks to a specific application case and the authors shown the advantages of their system over traditional food supply chain systems.

Some of the largest software companies offering cloud services, such as IBM, Accenture and Baidu, offer supply chain-oriented versions of blockchain ledger that can be tailored and integrated into existing systems [14]. Furthermore many companies in the agri-food sector, such as Walmart, Auchan, Carrefour have demonstrated their interest in blockchain technology applications, mainly for tracing the products (see works [15]–[17]).

According to Galvez *et al.* [18] most existing blockchain systems for traceability management have been developed since 2015, but there are still few uses to the state of practice, and according to Behnke and Janssen [19] many blockchain projects remain at the piloting level because, on the basis on the results of their study, they claimed that supply chain systems have first to be modified and organizational measures need to be taken to fulfill the boundary conditions, before blockchain can be used successfully.

In a recent article, Ferdousi *et al.* [20] proposed a smart contract-based supply chain framework that they applied to the US beef cattle industry but it can be applied to other supply chains with minimal modifications. The authors used a permissioned blockchain network to solve the issues of security and privacy, and control of private and shared

data. The proposed system supports anonymity for the users to protect identities and lets every user store their data locally. The technical contribution is in the system design on how users, data, and communications are handled to maintain data ownership and user privacy while ensuring immutability and confidentiality at different levels of data aggregation.

Yu *et al.* [21] proposed a quality monitoring system within a fruit juice production enterprise by combining smart contracts and machine learning technologies. Their system can utilize the traceability of the blockchain and the auto-execution of smart contracts to achieve reliable and efficient quality monitoring by combining the off-chain models with on-chain data.

Recently several works dealt with the combination of IPFS and Blockchain. Huang *et al.* [22] proposed a safe food traceable scheme based on blockchain, EPC technology and IPFS to alleviate the data size stored on-chain. Xu *et al.* [23] implemented a decentralised social network application on the Ethereum private blockchain with the use of smart contract and IPFS; Chen *et al.* [24] proposed an improved P2P file system scheme based on IPFS and Blockchain; Ali *et al.* [25] proposed a network architecture for providing IoT data privacy via blockchains and IPFS; and Zheng *et al.* [26] and Norvill *et al.* [27] proposed a system that stores Ethereum/Bitcoin blockchain transaction data on the IPFS and stores on chain only the hashes which identify a file in IPFS.

In this work we propose a complete and functioning decentralized application for the Carasau bread supply chain of a small typical enterprise located in an Italian island. The application allows customers to trace the product and supervisory authority to conduct on line inspections. Our near future work is to implement the system within the real Carasau supply chain going beyond the piloting level of our proposal.

Our dApp includes also a system in which the Blockchain technology interacts with the IPFS to guarantee an efficient decentralized data storage. The combination of these two technologies allows the reduction of chain size in Ethereum and the optimization of the system thanks to the reduction of the storage costs. In addition we reviewed some representative studies about distributed file systems integrated with blockchain, with particular reference to IPFS, that sought to address the issues related to the lack of access control.

The work by Huang *et al.* [28] conducted an overview about the joint use of blockchain and distributed file systems, mainly focusing on IPFS and Swarm, and then presented relevant cutting-edge studies to find solutions devoted to privacy-preserving distributed file systems. A large number of efforts have been made for enforcing privacy in IPFS taking into account that IPFS aims to share information. In specific scenarios that have to deal with private data the solution provided by Steichen *et al.* [29] seems to have a strong privacy level. They proposed a modified version of IPFS that is a decentralized access control version of IPFS named acl-IPFS constructed by an IPFS peer and an Ethereum account. Its architecture is composed of Ethereum nodes executing the smart contract capable of adding, removing and updating files ownership and handling the access control list of each file and acl-IPFS nodes that enforce the permissions. Entities are identified by their Ethereum public key and files are identified by their unique cryptographic hash. They focused also on the evaluation of the proposed decentralized access control version of IPFS in regards to its efficiency when compared to the original IPFS. According to the authors the combination of blockchain and a private-network IPFS allows for compliance with current data protection and sharing legislation. This is a good approach for managing access control policies but because a file cannot be accessed unless proper permissions are assigned to users, the proposed solution suffers delay while accessing files from the server due to blockchain interaction ([30]).

In addition another solution that can be reusable in our scenario and has also a strong privacy level was provided by the work by Naz *et al.* [30]. In their paper they use IPFS, Ethereum and an encryption mechanism for sharing digital data in a secure and trusted consolidated platform. In the presented scheme the problem of storage is catered by IPFS which stores data and returns hashes to the owner or seller. To achieve data security, data owners can set access rules and encrypt the hashes, so that data is not released to unauthorized parties and data on IPFS can only be accessed by verified requestors that send requests to access the data and which get authenticated through digital signature. Here data security is achieved by integrating an encryption scheme to the hashes of uploaded data on IPFS. These hashes are encrypted by the owner using the shamir secret sharing (SSS) scheme and stored in a smart contract. Therefore SSS is used to split and then encrypt the hashes of files uploaded to IPFS.

It is worth to underline that in this work we not only propose a system to ensure a transparent and auditable traceability of a product, as other literature works do, but we apply this system to a precise case study, the supply chain of a typical traditional Sardinian bread, and conceive it to allow regional bodies/Authorities to verify the conformity to the normative about the hygienic-sanitary conditions that each node in the chain has to comply with. Contrary to what has been done in the aforementioned papers, we present in deep detail our decentralized system focusing on the blockchain oriented software engineering principles applied in order to design/develop a system software of high quality. Furthermore we focus also on the implementation of the IoT devices, such as a unique and novel Wireless Sensors Network (WSN) for monitoring the bread manufacturing process [31], [32], while studying and developing robust and effective NFC and RFID tags for the bread supply chain, used in combination with Blockchain and IPFS technology, that is a topic little investigated in the research works that deal with supply chain systems in combination with these two typologies of technology.

III. CARASAU BREAD SUPPLY CHAIN: A SUMMARY

In agreement with the articles 8 D. Lgs. 173/98 and 2 D.M. 350/99, the *Carasau bread* is the product obtained from re-milled semolina of durum wheat, grown exclusively in Sardinia, natural enzymes, sea salt extracted in Sardinia, dechlorinated drinking water and without adding any chemical and/or biological products. The bread must be produced in Sardinia with mechanical and physical processes, which aim to guarantee the best organoleptic quality to the product. In addition, it has to be produced in structures suitable for guaranteeing adequate hygienic-sanitary conditions. The finished product must be packaged using food containers produced according to the regulations in force, hence sealed packages constituting a physical barrier impermeable to the atmospheric-physical and polluting agents, and must be suitably labeled.

A first systematic approach to the production of food that meets the criteria of quality and safety were addressed by the International Organization for Standardization in ISO 9000 series, ISO 22005:2007 and the HACCP system.

In particular, ISO 22005:2007 [33] is a specific standard for traceability in the food and feed chain and here the traceability is defined as *"the ability to follow the movement of a feed or food through specified stage(s) of production, processing and distribution"*. HACCP stands for Hazard Analysis and Critical Control Point and represents a system aiming at ensuring food safety. According to Marques *et al.* [34] HACCP system provides a systematic and structured approach to identify and analyze the hazards – biological, chemical and physical - and the likelihood of these occurring at all stages of the food supply chain from raw material to the final product. The application of HACCP is mandatory since January 2006, by EC Regulation 852/2004 of April 29 [35], and it is a plan of rules to be implemented that guarantees the healthiness of food by monitoring the entire supply chain of the food production and distribution process and defining preventive measures to minimize occurrence of hazards by application of immediate corrective measures.

The control of the correct handling of food throughout the supply chain is an obligation of the various actors along the supply chain which translates into risk assessment, mandatory training for each actor and his/her employees, drafting of the HACCP manual and any laboratory analyses.

HACCP is made up of the following seven key principles:

1) Conduct hazard analysis;
2) Identify critical control points;
3) Establish critical limits;
4) Establish monitoring procedures;
5) Establish corrective actions;
6) Establish verification procedures;
7) Establish effective record keeping.

These principles constitute the basis for the establishment of a HACCP plan aiming at ensuring the food safety of products.

Several studies demonstrate that the HACCP system has a positive effect of the quality of end products and a HACCP Plan for bakeries and all hazards must be analyzed from the initial stages with your suppliers and raw ingredients through to your baking processes and the sale of the bread [34], [36]. The supply chain of Carasau bread begins with the production of the raw material, the durum wheat. The durum wheat is considered a low-risk raw material, but since the presence of mycotoxins and/or chemical residues cannot be excluded with a simple inspection action, the milling industry has to request appropriate documentation from wheat suppliers, certifying the checks carried out to exclude the presence of these residues or mycotoxins and reporting any antifungal measures adopted. All documentation has to be kept and made available for any inspections by the supervisory bodies.

The milling industry, if equipped with suitable tools, can perform further analyses on incoming grain to confirm the documents received. In addition to the analysis of the incoming grain, it has to perform analyses on the outgoing batches, and therefore on all the batches of flour produced and has to perform periodic microbiological and chemical analysis of the drinking water used. There are many definitions on the quality of flours and different ways to determine it. In the analysis of the flours, parameters such as humidity, ash, protein content are essentially evaluated for the classification of wheat flours. There are also parameters that refer to the rheological properties of the flours. From these parameters depend the behavior of the doughs during their mechanical processing [37]–[39]. Flour storage, as well as the bagging and palletizing phase, has to take place in healthy environments in order to maintain the characteristics of the flours unaltered before shipping to the bread producer/bakery. Similarly, the bread producer has to arrange the raw materials entering his factory in such a way as to prevent their deterioration.

In general, each actor of the supply chain, that is involved in storage, transport or distribution has to know the conditions to be applied and maintained after a given batch has left a given chain's component. In our case study, all batches present along the supply chain can be kept at room temperature, as long as not excessively hot, preferring cool and dry environments and a storage temperature as uniform as possible, especially in summer. Therefore the temperature in the storage rooms has to be continuously monitored to ensure that the batches do not undergo thermal shocks that could alter their organoleptic properties, as well as favor the formation of bacteria. In addition to avoid deterioration a rotation of products has to be guaranteed so that the products that enter the storage area first, are also those that leave the area first. Vehicles intended for the transport of products throughout the supply chain has to meet general hygiene criteria. All surfaces in contact with the transported products have to be of suitable material, smooth and easy to clean and disinfect, so that the packaging material remains intact and the product is not contaminated and is protected from dust and / or any form of fouling.

From what has been described so far, it is clear that the quality of the final product depends on the entire supply chain and on the way in which each actor operates within the chain. Reliable and verifiable documentation, which certifies the characteristics of each product entering and leaving each component of the supply chain, and which certifies the health and hygiene conditions adopted by each component, are essential for tracing and verifying the quality of the final product.

Therefore to have effective traceability systems for food production becomes of fundamental importance in order to ensure the safety of food and the protection of quality products. To be able to count on technologically advanced systems is essential for a timely and efficient management of traceability information, even more if we consider that today consumers are more attentive to quality, and more and more often they search for information on the foods they bring to the table, via smartphones and apps.

The application of HACCP can be managed via blockchain combined with IoT approaches. In this context, our system - consisted of a sensors network for monitoring (for example the temperatures), of cameras for monitoring the storage points, of smart contracts on the blockchain to store essential data of the batches and nodes, and of the external database to store large amount of data, and described in detail in Section IV - contributes to the protection of quality productions by favoring the management of a large amount of data and by relating all the actors in the supply chain, from field to table.

IV. THE PROPOSED DAPP

A. AN OVERVIEW

In this section we give an overview of the proposed dApp. DApps stands for decentralized applications, they do not rely on centralized servers as traditional applications, but they have their own backend code running on a decentralized peer-to-peer network. Our dApp was designed for the Ethereum blockchain, with an external system for the access control, an external database (the IPFS), a sensors network, several Rasperry Pi units, and NFC and RFID tags. We used Ethereum that is a permissionless platform in which anyone can set up a node and participate to the network and/or access data. Moreover, among the main benefits of Ethereum there is the possibility to deploy and use Turing-complete smart contracts. Due to the significant costs and to the limits of the on-chain storage, an external database is used to store data coming from all nodes along the supply chain. We used an external database to store data documents, and stored in the blockchain only the hash code of the documents and the URL in which the documents reside, as described in detail in Section IV-D. We considered the Sardinia Region, or a specific Sardinian regional body, as the system administrator and supervisory body. The administrator supervises every read and write operations of data by each actor of the supply chain and provides to everyone the proper access permission. The sensors network, set along the supply chain, allows to monitor nodes and batches entering and exiting nodes, and to communicate collected data to the Raspberry Pi units along the chain. Node.js and Web3.js packages[1] are installed inside each Raspberry Pi, present along the chain, to allow these devices to interact with the on-chain components, hence with the smart contract that deployed in our blockchain system. Every IoT device, being connected to a Raspberry Pi board, interfaces with the blockchain, listens events and executes transactions that can also trigger events that lead to a modification of the blockchain state, hence in our case to changes of the batch's and node's parameters. We deploy our system on Ganache,[2] that is a local blockchain, and also on Rinkeby, that is a test network.

As already mentioned our dApp was developed applying the ABCDE method (see work [40] for more details), that is a software development process specific for blockchain software systems consisting of eight steps. The first three steps aim to collect the requirements of the system to be realized without assuming the use of a blockchain. Specifically, in the first step the goal of the system is defined in one or two sentences. In the second step the actors –human and/or external systems / devices – are identified. In the third step the system requirements are written in terms of user stories or features. The fourth step provides for dividing the system into two subsystems: the on-chain components (smart contracts running on the blockchain) and the off-chain component (the App System, that is the external system for users interaction). The fifth step provides the design of the blockchain system and the sixth that of the external system, making appropriate security assessments for both systems and following the main GAS optimization patterns during the design of the blockchain system. The last two steps involve the test of the two subsystems and their integration and release. In the following sections each step is described in detail.

B. GOAL, ACTORS AND USER STORIES

Goal of the proposed dApp is to guarantee a transparent and auditable traceability of the Carasau bread in such a way that each actor of the supply chain can verify the quality of the products and the conformity to the normative about the hygienic-sanitary conditions along the chain.

Taking into account the six main segments in the Carasau Bread supply chain, that are seed sector, production and commercialization of grains, milling, baking, distribution and consumption (see work by Galli *et al.* [41]), we defined seven main actors in our supply chain.

1) *Authority* is represented by a specific regional Sardinian body. It is the administrator of the system and supervisory body.

[1]Both these packages are provided by *npm* that is the default package manager for the JavaScript Node.js runtime environment. Node.js allows to execute scripts to interact with our smart contract, whereas Web3.js package provides a JavaScript API to interact with the Ethereum blockchain.

[2]Ganache is used for setting up a personal Ethereum Blockchain for testing Solidity contracts.

2) the *provider/seed producer* provides the raw material, hence the seeds of durum wheat;
3) the *farmer* is the responsible for example of the seeding and harvesting;
4) the *milling industry* produces the re-milled semolina of durum wheat;
5) the *bakery industry* produces the Carasau bread;
6) the *distributor* is responsible of moving the output of the farmer from farmer's site to milling industry, the output of the milling industry from milling industry's site to bakery, and the output of the bakery from bakery's site to retailer;
7) the *retailer* sells the products;
8) the *consumer* is the final actor of the supply chain.

Let us describe our system in terms of User Stories. User Stories serve to identify users, describe the goal of the system, and are centered on the result. They consist of a short description written from user's point of view, with natural language and do not focus on what the system should deliver.

The following user stories were individuated.

1) The seed producer stores technical information of his product (seeds), and data on their sale.
2) The farmer stores data on the purchases of raw materials (seed), amount and technical information of the harvested grain, but also for example data on irrigation, fertilizing, and on the sales of the harvested grain.
3) The farmer transfers the ownership of his product, the durum wheat, to the distributor in order to deliver the product to the milling industry, and stores technical documentation on the products transferred.
4) The milling industry system stores details about the received amount of product (incoming grain/durum wheat batches) from distributors, and data concerning its production of flour (outgoing re-milled semolina/flour batches). The system of this industry also records information about hygienic-sanitary conditions in which it works, and about the temperature and humidity in its storage rooms.
5) The milling industry transfers the ownership of its product, the flour, to the distributor in order to deliver it to the bakery.
6) The bakery system stores details about the received amount of product (incoming re-milled semolina batches) from distributors, and data concerning its production of bread (outgoing bread batches). In addition, as the milling industry system does, it records information about hygienic-sanitary conditions in which it works, and about the temperature and humidity in its storage rooms.
7) The bakery system transfers the ownership of its outgoing batches, the Carasau bread, to the distributor in order to deliver them to the retailer for the sale.
8) The distributor records information about hygienic-sanitary conditions of the means he works with, and about temperature and humidity in the means used.
9) The consumer via user-friendly app can retrieve data on the bought bread and can trace and verify each step along the supply chain.
10) All actors/systems record information to make available to other actors in the chain by using pdf and jpeg files. So at precise and predefined time intervals, data coming from sensors and optical cameras are automatically elaborated in order to obtain the files idoneous.
11) Authority manages and controls the reading and writing accesses in the system by the different actor and devices, and performs inspections to verify the conformity of the products and the work of each actor in the chain. The inspections can be performed by viewing the data documents stored by the nodes of the chain.

C. BLOCKCHAIN SUBSYSTEM

In our Carasau supply chain management system, a certifying authority, a Sardinian regional body, gives access to the system to precise actors. So only the authorized actors can record data within the system and contribute to the traceability of their product. In our supply chain we can define several nodes/components. They are the structure/location in which the seed are produced (the seed producer is the actor in this node), the field where the wheat is grown (the farmer is the actor in this node), the milling industry in which the flour is produced (the industry is the actor), the bakery industry in which the Carasau bread is produced (the industry is the actor), the means of transport the distributor uses to deliver the outgoing batches from farmer's site to milling industry, from milling industry's site to bakery, and from bakery's site to retailer.

Next we describe in detail the logic of this subsystem by using the terminology adopted in the implementation of the smart contract in order to facilitate the description of the smart contract reported later on.

Each node enters the supply chain only when the authority gives it the access to the system. It has a precise unique identifier, the `id`, that is a her/him/its Ethereum account/address, and is characterized by a set of parameters, named `nodeConf`, describing its condition in terms of preservation of the required quality. The node condition can be *Eligible* when all the requirements are satisfied, and *In Reservation* when some corrective measures are necessary to allow the node to continue to work. This parameter is set to *Eligible* by the authority when this body adds the node to the chain. Next this body performs inspections at random to verify the node conformity with the requirements of quality. If not all the requirements are satisfied, it sets the `nodeConf` parameter to *In Reservation*. Note that only this body can change the node parameter from *In Reservation* to *Eligible*.

At each node there are an incoming batch and an outgoing batch. Each batch has a precise unique identifier `id`, and an owner, that is the responsible for that batch. The batch's owner is uniquely identified by his/her Ethereum address and only the batch's owner can add a batch to his/her node. Whenever a batch passes from a node to another node in the

chain, its identifier changes as well as its owner. As for the nodes, also batches have a parameter used to evaluate the batch condition in terms of preservation of the required quality. This parameter is set by the batch's owner when he/she adds the batch to her/his node, or by the authorized body that at random performs inspections to verify the batch conformity with the requirements of quality. The batch condition can be *Eligible* when all the requirements are satisfied and *Withdrawn* if the requirements have not been individuated enough and the authority withdrew the batch. The node's owner cannot change the node condition from *In Reservation* to *Eligible*; and the batch's owner cannot change the batch condition from *Withdraw* to *Eligible*.

After performing an inspection, the authority performs a blockchain transaction, warning, by the emission of the so called *events*,[3] that an inspection has been performed and the node and/or batch condition could be changed. The node owner, that is listening for such events, has to adopt the needed corrective measures in order to change the node condition if this is in *In Reservation*. In turn the node's owner, that adopts corrective measures on his/her node, has to perform a blockchain transaction. Also this transaction emits an *event*, warning that corrective measures have been adopted, and that the node condition has to be revalued. In turn the authority, that is listening for such events, has to check/inspect the state of the node, and performs a blockchain transaction that modifies the data stored in the blockchain, changing the node condition from *In Reservation* to *Eligible*, if the inspection is successful.

Let us give some details about the access control system. Each user/device in our system is identified by a specific Ethereum address, hence each user/device is identified by an Ethereum account. Only the owner of a given address owns the private key associated with that address. Authority manages and controls the accesses to the system by storing all the addresses associated to all users/devices authorized to access to the system in a smart contract that is deployed in the blockchain. If the private key is stolen or lost, the Authority can lock the address associated with that key. In turn, the identity of the Authority can be made public, for example by declaring in the Authority's web site its Ethereum address. All users who want to make a transaction on the Blockchain must sign the transaction with their private key, so only authorized users, hence only the addresses stored on the blockchain by the authority can execute Blockchain transactions.

1) A DETAILED DESCRIPTION OF THE PROPOSED SMART CONTRACT WITH A FOCUS ON THE PRINCIPLES OF SOFTWARE ENGINEERING ADOPTED

Fig. 1 shows the structure, precisely the UML class diagram of the smart contract that manages the Carasau supply chain system. Our smart contract, named *CarasauSupplyChain*, implements the logic just illustrated, and was written in Solidity language. It contains two main data structures of type *struct*. *Struct* in Solidity is a customizable data type. We defined two *structs* with a name and precise properties. The first is named `aBatch`, the second is named `aNode`. In the following we describe in detail only the *aBatch struct*, since the description of a *aNode struct* is similar and follows easily. The *aBatch struct* contains several properties used to store essential data for the traceability of a batch along the supply chain.[4] It contains two variables of type *bytes32*. One is named `id`, and the other `name`. The property `id` uniquely identifies a batch and changes when the batch passes from a node to another. It contains a property, named `owner`, of type *address* that identifies the owner of the batch. The *aBatch struct* contains also properties of type *enum*,[5] that are defined at first into our smart contract. The proposed smart contract defines four *enums*, that allow to define the conformity, the typology and the state of a batch and/or of a node. They are defined as follows.

- `enum batchTypology {Seed, Wheal, Flour, Bread}` describes the typology of a batch along the chain. A batch can be seed, wheal, flour or bread.
- `enum batchConformity {Eligible, Withdrawn}` describes the conformity of a batch along the chain. A batch can be eligible, or withdrawn.
- `enum nodeConformity {Eligible, InReservation}` describes the conformity of a node along the chain. A node can be eligible or in reservation.
- `enum nodeTypology {Producer, Retailer, Distributor}` describes the typology of a node along the chain. A node can be a producer node, a retailer node, or a distributor node.

The three *enums* defined into our *aBatch struct* are `batchStatus`, `batchConf`, and `batchType`, respectively of type `batchState`, `batchConformity`, and `batchTypology`. The *aBatch struct* defines also a mapping, named `hashesMap`. It contains all hashes of the documents associated to the batch and stored in the IPFS. Mapping in Solidity is seen as hash tables. So mappings contain keys and map each of them to a value. In our case `hashesMap` maps keys of type *uint256* to a value of type *bytes32*.

In the following we continue to describe the smart contract focusing on the principles of software engineering adopted in the development of our application on-chain. Indeed, contrary to design and implementation of traditional software applications, the development of smart contracts implies patterns and best practices that are in their early stage. For this reason

[3]Events are inheritable members of contracts. When you call them, they cause the arguments to be stored in the transaction's log - a special data structure in the blockchain (extracted from https://docs.soliditylang.org/en/v0.6.7/contracts.html#events).

[4]Note that our smart contract manages the main essential data related to the traceability of a batch and to the hygienic-sanitary conditions of a node. However it can be easily customizable to include more properties and functionalities.

[5] *Enums are one way to create a user-defined type in Solidity. They are explicitly convertible to and from all integer types but implicit conversion is not allowed. The explicit conversion from integer checks at runtime that the value lies inside the range of the enum and causes a failing assert otherwise. Enums needs at least one member.* (extracted from https://docs.soliditylang.org/en/v0.5.3/types.html).

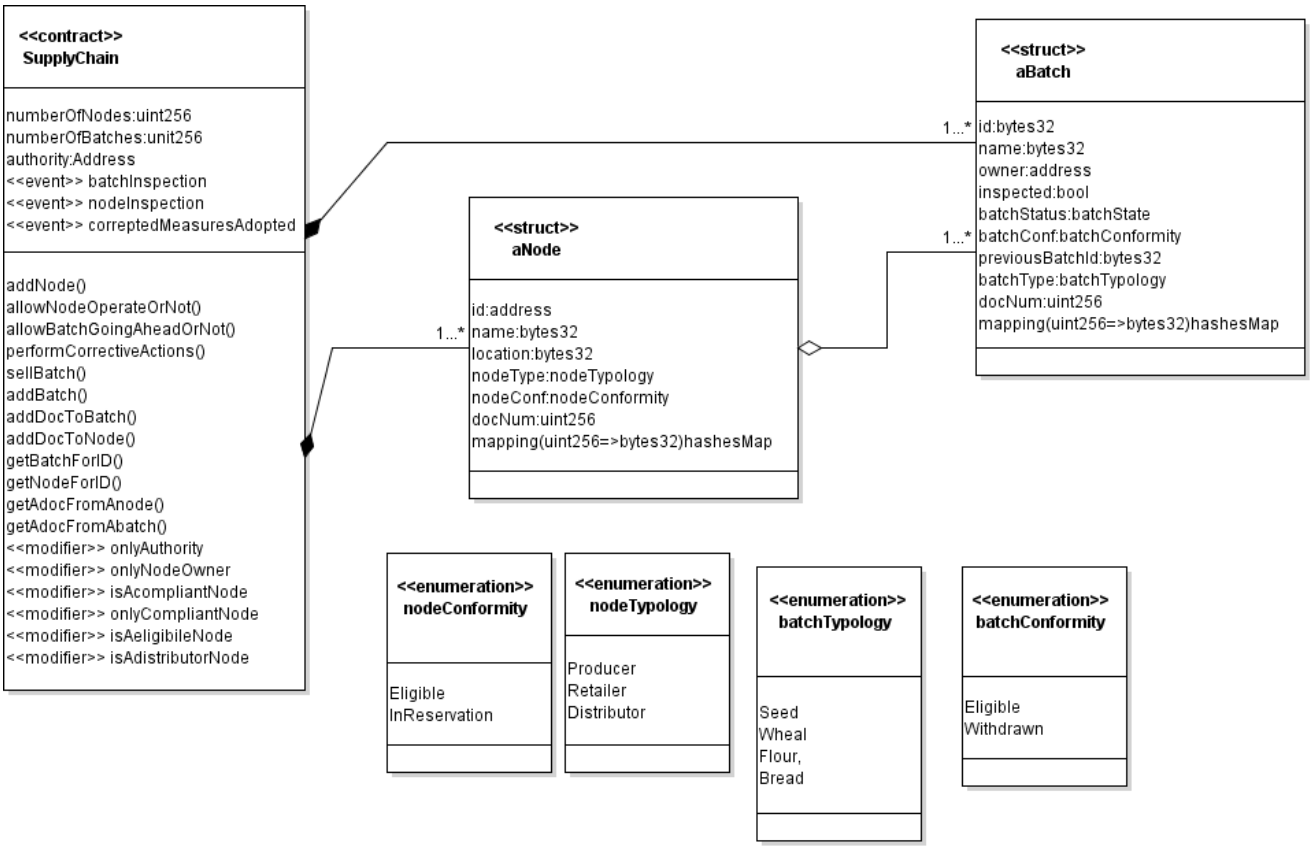

FIGURE 1. UML Class Diagram describing our smart contract.

we focus on the on-chain application of the proposed dApp, emphasizing all the best practices adopted (see works by Marchesi *et al.* [40], [42], [43] for more details).

Developing dApps is a process very different from developing traditional software applications. This is because the development of dApps implies the implementation of the so called smart contracts, that are pieces of code, whose bytecode is public. Whenever a smart contract is deployed on Ethereum blockchain, its code is visible to anyone. In addition deploying smart contract on Ethereum blockchain and generating transactions, that modify the blockchain state, costs gas, hence this implies the consumption of real money. For this reason following patterns and best practices during the development of this typology of applications is essential in order to avoid all possible exploits and excessive spending.

First of all since the code is publicly available the access to the dApp has to be checked, and since the application provides for functions that can be triggered only by authorized actors also this point has to be managed. So, in our dApp the access to the dApp is guaranteed through a correct use of the private keys of the various actors/devices along the supply chain, and the trigger of given functions is managed through the use of addresses *mapping* and *modifiers*, as illustrated in the UML diagram (Fig. 1). Specifically the *nodesMap mapping* associates the nodes' addresses with the identifier of the node, that is an *uint* (unsigned integer), and *batchesForNode mapping* associates the nodes' addresses with an array of unsigned integers that identify all the batches associate to a particular node, hence to an address. As regards the restrictions on the functions use, they are managed through the so called *modifiers*. A *modifier* allows us to control the behavior of smart contract's functions. It includes a variety of use cases and in our case our smart contract contains a modifier that allows only the contract owner to run a given function. So the contract owner, that in our study case can be a regional body, is the only entity that can generate transactions calling some specific methods. He/she is identified by a specific Ethereum account /address, the only address that can add a node to the `nodesMap mapping`, hence is the only address that can generate a blockchain transaction using the smart contract's method named `addNode`. It is also the only address that can generate a blockchain transaction using the smart contract's methods named `allowNodeOperatingOrNot` and `allowBatchGoingAheadOrNot`. With such configuration only the authority is enabled to change the node/batch condition from *In Reservation* to *Eligible* / *Withdraw*, allowing the node to continue working, and the batch to move on to the next node/component along the supply chain.

In addition to *modifiers* also *guard functions*, such as *require()* functions, are implemented to validate state

conditions preceding an execution. For example, in the *modifier* named `onlyAuthority` a guard function has to check if the address sending the transaction is the address of the contract's owner.

Finally, as regards to the gas consumption, it is worth mentioning that, when an Ethereum smart contract is compiled, it is converted into a sequence of ''operation codes''. Each operation code implies a predetermined consumption of gas (see the so-called Ethereum yellow paper [44]). Every transaction executed on Ethereum blockchain has two parameters, the gas price and the gas limit. The gas price is the number of wei to be payed for unit of gas. So the gas has to be payed from the address sending the transaction, using its ethers and paying on the basis of the gas price specified into the transaction. An address can set the gas price it prefers, but miners are free to choose transactions with a higher gas to maximize their profits. We designed our smart contract following the collection of patterns for the design and development of Smart Contracts, with the aim of saving gas presented by Marchesi *et al.* [43]. Hence for example we minimized on chain data, limited the storage, used *mapping* in place of *array*, and used *Event Log*.[6]

The costs of data storage in blockchain are variable and expensive and recently the combination of blockchain and distributed file systems is becoming a promising solution. In this context it is crucial to identify what data should be stored on-chain and what should be uploaded and saved off-chain. There are several off-chain solutions to store data. In this research work, in order to limit the storage on chain we chose to use the most popular and well-established platform, namely IPFS, because its design ensures immutability and non-reliance on a central server but not only. *IPFS is short for Inter Planetary File System that is a peer-to-peer distributed file system that looks for connecting all computing devices with the same system of files*. It was launched by Juan Benet in May 2014 and is an open source project with the aim *to re-decentralize the web* by providing a *high-throughput block storage model with content-addressed hyperlinks* ([45]). In the more general case in which data must be accessible and verifiable by everyone and no longer editable in any way, we combined IPFS with the blockchain in the following way (a more detailed description is presented in Sec. IV-D). We store data/documents coming from IoT devices placed along the supply chain into the IPFS, that returns the hash codes of the uploaded data/documents to our external application, that in turn interacts with our smart contract transmitting the hash to be stored on-chain. This is the so called Oracle, that is a web application, that provides the information from the outside world to the blockchain, hence to our application on-chain.

As regard the *Event Log* memory, we used this typology of memory to store information about the result of an inspection or a corrective measure adopted. So the smart contract defines three *events*:

- `event batchInspection(address owner, bytes32 id, bool result),`
- `event nodeInspection(address owner, bool result),`
- `event correptedMeasuresAdopted (address owner).`

These *events* are emitted respectively during the execution of the `allowNodeOperatingOrNot`, `allowBatchGoingAheadOrNot`, and `performCorrectiveActions` methods.

Finally, note that, as in the traditional software development, also in the smart contract development, the testing and deployment phases are important. We performed the testing phase using Remix IDE, that is a browser-based real-time compiler and runtime environment for Solidity. We tested our application on Rinkeby, a test network, but also on Ganache by the Truffle suite. Ganache is a local Ethereum blockchain that allows of deploying our smart contracts, generating transactions, and inspecting the state of our local blockchain.

D. EXTERNAL SUBSYSTEM: GUI AND SERVER COMPONENTS

The external system of proposed dApp is constituted mainly by two parts. The first is a web application running on the browser. It is the GUI, hence a client application that allows the actors/consumers to trace a product, and the authority to perform online inspections by viewing the various uploaded documents. The GUI has been implemented using React, that is a JavaScript library, provided by *npm*. It is connected to an Ethereum network node through Metamask, that is a browser plugin that injects a web3 instance into our subsystem. Before a user can trace a product using our GUI, and authority can perform online inspection, he/she has to have Metamask enabled in order to be able to manage his/her Ethereum account, hence his/her private key. The second part, that is uploaded in each Raspberry units, is the so called Oracle. An oracle is a software application that interacts with the Blockchain and the IPFS. It provides data, by listening and responding to events issued by the Blockchain subsystem [46]. It allows the interaction between the Ethereum Virtual Machine and the outside world generating Ethereum transactions. To generate a transaction, the oracle has to encode the transaction in order to obtain its Application Binary Interface (ABI). Then it has to create and sign the transaction with its private key.[7]

As already mentioned an external database is used to store data coming from all nodes in the supply chain. Specifically we used the IPFS, a system similar to BitTorrent, based on a peer-to-peer protocol where each node stores a collection of hashed files. This system distributes the documents we want

[6]Note that deploying a smart contract on blockchain entails the possibility to use different types of memory. *Storage* is a persistent memory, instead *event log* is a memory to which only external applications can access and that contains data related to the *events* issued by smart contracts.

[7]To implement this process we used the *ethereumjs-tx* package, provided by *npm*. To handle events we used the websockets (WSS) connections in place of HTTP connection, by defining a websocket INFURA URL.

to archive among all those who decide to install the client program associated with the IPFS project on their computer.

An actor/IoT device along the supply chain who wants to upload a pdf file, or a jpeg file, into the IPFS, has to install the system and follow the procedure to add his /its file in the IPFS network. The IPFS generates a hash of the file and makes available the file on the IPFS network. To share this file with the other actors in the supply chain the hash of the uploaded file has to be known.

One main issue with this system is that in IPFS data content is stored in different peers and so accessible by every peer, although data can be encrypted. Data sharing is crucial to guarantee a transparent traceability system but we are aware that access control and securing sensitive data are issues to solve in a non-private IPFS. One possibility to cope with this issue is to keep track on the blockchain transactions of IPFS documents hashes and to store on IPFS plain or encrypted documents depending on the privacy policies. A second option is to directly use a private IPFS for storing private documents. In this paper we choose to adopt a public IPFS eventually encrypting private data. We refer to the related work section for all the possible solutions. Our system can be customized by including in particular two main contributions provided by Naz *et al.* [30]: the Identity management, according to which users are first authenticated using RSA signatures before giving them access to data, and the Security of digital assets, namely adding encryption to the data hashes, that ensures the security and avoids data leakage.

In our case study data are upload automatically by the system at predefined time intervals or in response to *events* emitted by the smart contract executing its specific methods. In the first case, when the system uploads automatically data at predefined time intervals, the system is designed in such a way that it uploads data files and image files, coming from IoT devices at predefined and random time intervals, such as once a day. This is because all data coming from IoT devices serve to prove the condition in which a node operates and that a batch is in. So these data have to be collected, analysed at random intervals, and stored in a secure database to guarantee transparency and trustworthiness.

As regards the file uploaded in response to events emitted, the system works as follows. For example, after an event of type `event nodeInspection(address owner, bool result)`, emitted by the authority and following an inspection, a node can emit an event of type `event correptedMeasuresAdopted(address owner)` executing the smart contract method named `performCorrectiveActions`. This implies that the node's owner adopted the measure needed to restore its structure/location to an eligible condition, and uploaded specific documents to prove it, generating ethereum transactions by executing the smart contract method named `addDocToNode`.

The React application, that allows the actors to upload the files in the IPFS network and to interact with the blockchain, works as follows. Choosen a file, this file is converted to a buffer for upload to IPFS. The buffered file is sent to IPFS

FIGURE 2. GUI used to upload the file on the IPFS network and on Ethereum blockchain.

using the `ipfs.add()` function, and the IPFS network returns a hash. Thanks to the returned hash the file can then be viewed on an IPFS gateway.

The actors interact with our blockchain system making a transaction by their Metamask accounts, by using the appropriate method of our Ethereum contract and the web3's `send()` function, to store the IPFS hash forever on the blockchain. This task is completely automated in the first case above described. Specifically in that case, data collected by the various sensors and optical cameras are processed by appropriate software programs that, at predetermined intervals, give in output the files that have to be stored on the IPFS network, and then forever in the Ethereum blockchain. Actors have only to confirm the transaction with their MetaMask account.

Fig. 2 shows the GUI used to upload manually the file on the IPFS network and on Ethereum blockchain.

In this case the user is connected to an IPFS node via localhost, hence after having uploaded a file on the IPFS network and on the Ethereum blockchain, the user can see his/her file at one of the IPFS gateways, that is *https* : *//gateway.ipfs.io/ipfs/* + *ourIPFShash#*, hence *https* : *//gateway.ipfs.io/ipfs/QmRxyfV*3*aXhD*5*Kr*3*fsaPHp*6*VK*2*CZ*3*UhZ*3*j DqiYW*35*nxwAW* in the example shown in Fig. 2.

In our dApp files and data have to be upload also automatically by our external system and a similar system has to be integrated in each Rasbperry unit so that it can work automatically.

E. EXTERNAL SUBSYSTEMS: RFID AND NFC TECHNOLOGIES

In the external subsystem passive RFID tags were designed to provide instruments for the traceability of the batches and the check of the nodes along the supply chain, and NFC tags were designed to be deployed onto the packaging of batches/products. When managing with food, it is typical to deal with materials which present very different electromagnetic properties, e.g. lossy and/or high dispersive materials. Moreover, for its intrinsic characteristics in manufacturing process, and the use of organic raw materials, the food production is not able to replicate the same electromagnetic properties in each final product, unlike from electrical devices

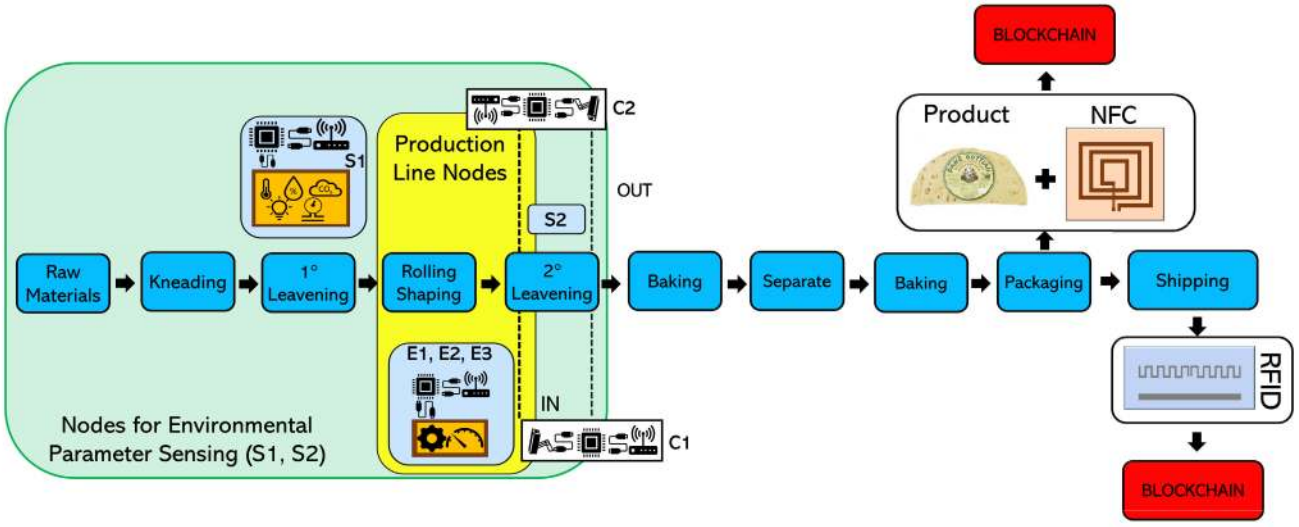

FIGURE 3. Schematic description of the Carasau manufacturing process, highlighting the IoT devices that participate to the proposed blockchain system. Wireless Sensors Network (WSN): Environmental nodes (S1, S2) for acquiring temperature, relative humidity, gas concentration, pressure data; Production line nodes (E1, E2, E3) for the kinematic parameters of the machinery; Morphological bread analysis nodes (C1, C2). Near Field Communication (NFC) tag for product tracking. Radio Frequency Identification (RFID) antenna for the logistic operations related to the shipping.

where this issue is a design requirement. In our case, the bread slices where the tag is placed on top can present variable dielectric permittivity and electrical conductivity during the working day or among different batches of products, since the final product is realized with a process starting from a moist dough and involving different leavening and cooking steps, which cannot assure a very accurate repeatability of the product. Because of this, in addition to the cheapness and easy manufacturing required to produce such devices, we decided to realize in-house tags which guarantee the necessary robustness. We designed ad hoc tags to provide robust, reliable and efficient systems to the traditional bakery industry. In the industrial scenario under analysis, the functioning of NFC may be hampered by the positioning over the bread (which is a lossy medium) [47], [48]. This calls for a stable response of the tag. As regards the RFID, the design criteria are: i) the robustness of the antenna in terms of matching and tuning, ii) the possibility to interrogate the tag from an unknown reader position [49].

NFC tags and RFID antennas will be manufactured and characterized in future works.

In Fig. 3 NFC tags, in the product packaging, and RFID antennas on the batches of products to speedup and simplify logistic operations are shown. It follows a detailed description of the design, functioning of the NFC tags and RFID antennas and their interactions with the proposed blockchain system.

1) RFID SOLUTION FOR BATCH TRACKING

Radio Frequency Identification (RFID) is a wireless technology mainly used to transfer data using the backscattered signal from an antenna [50]. It allows to identify and track a tag attached to an object. Also Near Field Communication (NFC) is a wireless technology. It allows devices to establish communication with each other by touching or touching them together. In the proposed dApp, passive RFID tags were designed to provide instruments for the traceability of the batches and the check of the nodes along the supply chain, and NFC tags were designed to be deployed onto the packaging of batches/products.

The RFID are low-size, cost-effective, reliable and data safe devices which can be easily interfaced with sensors for monitoring physical quantities of the batches and of the nodes/components along the chain [50], [51].

RFID technology is appealing for several applications, such as logistics, identification, tracking and traceability [50], [52], [53], especially in the agri-food sector.

RFID tags have already been proved to be a powerful tool for locating animals, monitoring and assessing food product or ingredient, while allowing to follow and track the entire history in the supply chain forward, from the source to the consumer, and backward, from the consumer to the source [53]. For example, RFID systems have been used to monitor milk freshness, bacterial presence, by integrating the tag with humidity, gas or temperature sensors The RFID tools could be used at any point of a given supply chain (production, transportation, storage and delivery) [53]. In our case study these devices can be used at any nodes/components to monitor both the nodes and the batches entering and exiting from nodes. However, the use of general purpose commercial RFID systems could be not effective since the deployment on a lossy media, such as bread, may cause the tag detuning and then hamper the RFID functioning [49]. Furthermore, the peculiar industrial scenario and warehouse organization call for a specific design and engineering process.

The geometry of the proposed RFID antennas is shown in Fig. 4(a). The passive tag layout is a meander line, capacitively coupled to a loading bar, with length l. This topology is easy to tune and match, can be manufactured

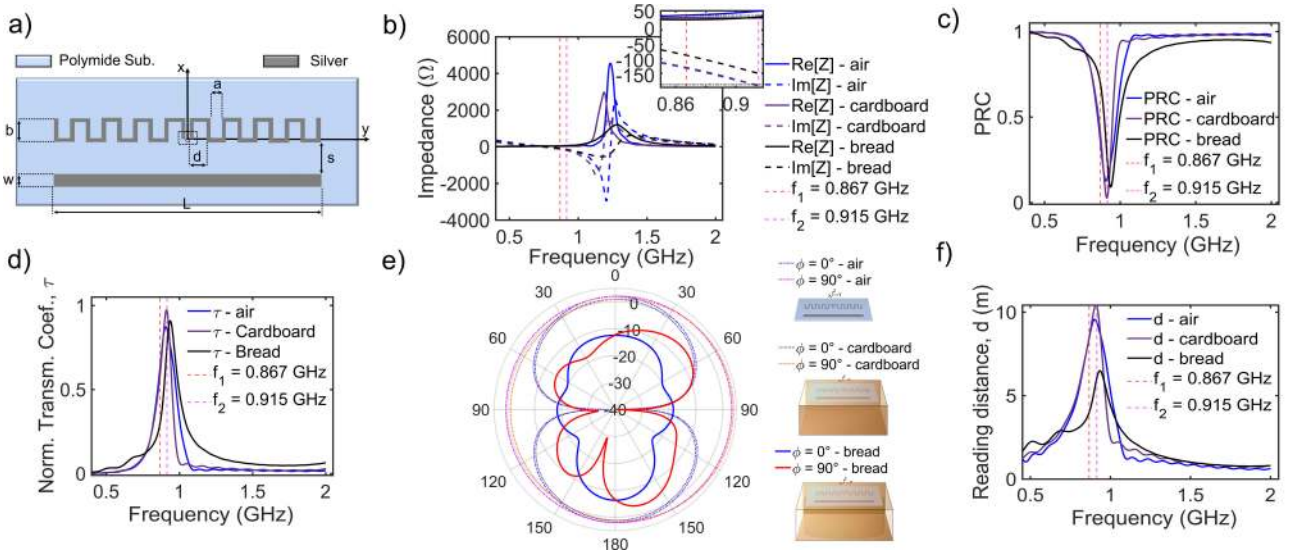

FIGURE 4. a) Geometry of the proposed RFID tag for the traceability of the Carasau supply-chain. Comparison of tag responses in air, on cardboard and on the cardboard box filled with bread: b) Real and imaginary parts of the simulated tag impedance versus frequency. c) Estimated power reflection coefficient (PRC) of the tag. d) Estimated power transmission coefficient (PTR or τ) for the designed RFID. e) Radiation pattern for $\phi = 0°$ and $\phi = 90°$ at $f = 0.868$ GHz. f) Simulated reading distance range for EIRP $= 2$ W.

with several technologies and ensure robust and effective performances [50], [54], [55]. The antenna is re-worked for operating at 0.915 GHz, forecasting to be manufactured on a 160 mm × 60 mm polymide substrate ($\epsilon_r = 3.5$, $\tan\delta = 0.0027$, in the range 0.4 GHz - 2 GHz, having 0.051 mm of thickness), by depositing silver ink ($\sigma = 63\,\mathrm{MSm}^{-1}$, thickness 0.018 mm) with ink-jet technology.

The antenna tag was simulated using CST Simulia Studio Suite (3ds, Dassault Systémes, GE) using the Time Domain solver. The tag excitation was simulated using a lumped port set between the two arm of the folded dipole, as shown in Fig. 4(a). The simulations are run considering a chip NXP UCODE G2XM (NXP), for identification and data storage. The chip is simulated as a lumped element having complex impedance equal to $Z_c = 30\Omega - j189\Omega$. The antenna tag was first studied, tuned and matched operating in free space. The device is aimed to be deployed above boxes (31 mm × 39 mm × 39 mm) made of cardboard, using the properties found in [56], which are filled with 15 packages of cooked bread (36 cm of diameter, 20 cm of depth), with the electromagnetic properties taken from [47], [48]. Therefore, the RFID performances were also investigated when the tag is placed on empty boxes and, finally, on the full box.

The final set of geometrical parameters which characterize the tag for the three cases, reported in Tab. 1, was found by performing an extensive number of numerical simulations in order to match the input impedance of the tag to the chip one, and to ensure a resonance at $f_r = 0.867$ GHz, as shown in Fig. 4(b). From Tab. 1 and Fig. 4(b), it is possible to observe that the height (b) of the size of the meander arms can be reduced of 2 mm and of 5 mm, with respect to the free space case, to ensure the tuning and matching over cardboard and when operating placed on the box filled with bread, respectively.

TABLE 1. RFID geometric parameters.

Param. Name	L	w	b	s	a	d
RFID in air - Value (mm)	125	1.5	11	15	7.4	9
RFID on cardboard - Value (mm)	125	1.5	9	15	7.4	9
RFID on bread - Value (mm)	125	1.5	6	15	7.4	9

Given the frequency response of the tag impedance (Z_t), we estimate the power reflection coefficient (PRC) and the transmitted power coefficient (τ) as [57]:

$$\tau = \frac{4R_tR_c}{|Z_t + Z_c|^2} \tag{1}$$

and

$$\mathrm{PRC} = 1 - \tau; \tag{2}$$

where R_t and R_c are the real parts of the tag and chip impedances, in Ω, respectively. Fig.s 4(c) and 4(d) demonstrate that the reflected power is minimized and the transmitted information is maximized at the working frequency. From Fig. 4(c) and 4(d) it can be noticed that the available bandwidth of minimum/maximum reflected/transmitted power increases in presence of the lossy bread. Furthermore, in order to provide a reasonable assessment of the RFID performances, we reported in Fig. 4(e) the polar plots of the far-field along the main directions. From Fig. 4(e), when deployed in air or on the empty cardboard box, the designed RFID can back-scatter the field in a quasi-omni-directional way, with a maximum gain of 3.25 dB, thus being suitable as building block for the proposed system. The RFID tag radiation pattern is significantly altered by the presence of the bread, as can be observed in Fig. 4(e). Indeed, the presence of a lossy medium below the tag, reduces of about 20° the available scanning angle, for a maximum gain of 2.3 dB. Under these conditions it is possible to acquire data from the RFID tag [58]–[60].

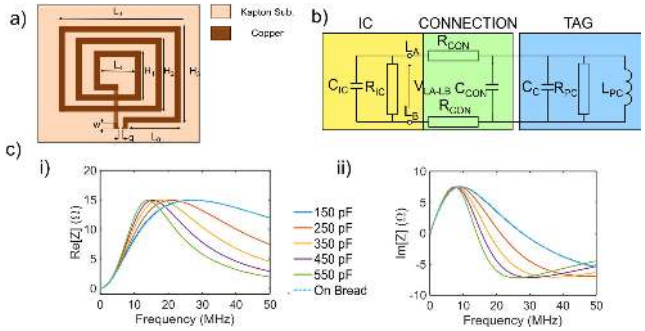

FIGURE 5. a) Geometry of the proposed NFC tag for the traceability of the Carasau supply-chain ($H_3 = 30$ mm, $H_2 = 24$ mm, $H_1 = 18$ mm, $L_0 = 12.5$ mm, $L_3 = 30$ mm, $L_4 = 14$ mm, $g = 1$ mm, $W = 3$ mm). b) Equivalent circuital model for the NFC during reading (yellow = IC, green = connection, blue = tag). c) Characteristic impedance of the NFC device over the selected frequency range: i) real and ii) imaginary parts.

By knowing τ and the gain pattern (G), the simulated reading range of the RFID tag can be obtained from Friis free-space formula as [57]:

$$d = \frac{\lambda}{4\pi\sqrt{\frac{\text{EIRP}\cdot G\cdot\tau}{P_{th}}}} \tag{3}$$

where the effective isotropic radiated power of the reader antenna (EIRP) is set to 2, and the chip sensitivity is assumed to be $P_{th} = -15$ dBm. The proposed tag antenna presents a minimum reading range of 2 m and a maximum of 9.86 m in air. If the tag is deployed on the empty cardboard box, then a maximum value of about 10.67 m would be obtained, as shown in Fig. 4(f). However, when the cardboard boxes are filled with the cooked bread, the reading range reduces to about 6.8 m at the working frequency (i.e. a 31% reduction). As a result, the working condition of the RFID tag (i.e., over empty or full bread boxes) can be very different and a specific study was necessary. Given the findings from Fig. 4, the designed RFID tag could be deployed onto the bread boxes over wood pallet, where the final packages are stored.

2) ON-PACKAGING NFC DEVICE FOR TRACEABILITY

As regards the devices designed to establish the link between the actors along the chain and the process information, as shown in Fig. 3, in our dApp, passive NFC tags were designed to be deployed onto the packaging of batches along the supply, and at the end of the chain onto the packaging of the Carasau bread (see Fig. 3). A suitable NFC tag is designed to cope with the unusual development on bread, which, from an electromagnetic point of view, is a lossy medium [47], [48], and has a complex relative permittivity of about $\epsilon_r = 8.64 - j4.1$. The NFC tags can be investigated by the actors' smartphone and all the information about the batch/product are made available in a clear and transparent way.

The geometry of the proposed NFC antenna is shown in Fig. 5(a). The layout is a squared, planar spiral coil, with length $a_1 = 30$ mm, $a_2 = 10$ mm. The planar squared coil is compact, easy to tune and match, and can be manufactured with several technologies, while ensuring robust and effective

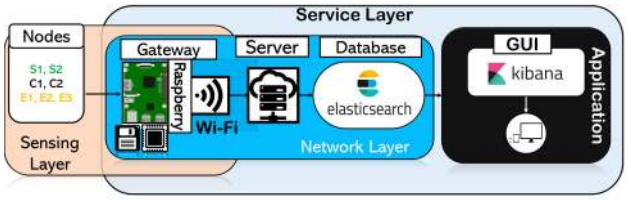

FIGURE 6. b) Details of the WSN architecture: sensing, network, application and service layers.

performances [61]. The device is designed for operating at 0.013 GHz, on a flexible kapton substrate ($\epsilon_r = 2.78$, $\tan\delta = 0.01$ at 0.013 GHz). The conductor is copper and the trace width is 1 mm. The coil is tuned by inserting a 150 pF capacitance, as derived from the circuital theory [61]. The antenna tag was simulated using CST Simulia Studio Suite (3ds, Dassault Systémes, GE) using the Time Domain solver. The NFC device is composed of an integrated circuit (IC) transceiver, the passive antenna and the connection between the two previous elements, as shown in Fig. 5(b). The tag excitation was simulated by assuming an impinging magnetic field perpendicular to the coil plane (see Fig. 5(a)) and a lumped port was used to recover the overall NFC impedance. We consider as IC the chip NTAG21x (NXP Semicond., USA), for identification and data storage, which was simulated as a 17 pF capacitive load, coherently with Fig. 5(b). From Fig. 5(c), it is possible to notice that the tag is matched and can operate at 0.013 GHz. The final design exploits a capacitance of 150 pF, and it results to keeps its operation when placed on top of the bread package (the curves of 150 pF in free-space and on bread in Fig. 5(c) are overlapped).

3) WSN ARCHITECTURE AND FUNCTIONING

The WSN along the supply chain, whose architecture is shown in Fig. 6, was conceived as a layer network to manage all the information and data collected by the multi-sensors nodes interfaced with different Raspberry Pi 3 B+ (Raspberry Pi, UK) units. The heterogeneous data, acquired by the network, are stored and organized by using the open-source software Elasticsearch (Elasticsearch, US) in ".json" format. As explained in [32], at Network layer the database acts as a coordinator element among the different gateways and nodes, which are identified by a timestamp, to ensure synchronization, and a unique label.

The elaborated data are made available to the operators through the application layer and automatically trigger the actions to interacts with the blockchain.

V. CONCLUSION

Musigmann *et al.* [62] provide a bibliometric analysis about the status of research of Blockchain technology in logistic and supply chain management concluding that RFID, smartphones, and other IoT applications might fix the data quality gap that most supply chains still face. We also agree with them that the evolvement of IoT in combination with blockchain technology as an underlying technology is an interesting playground for future research and in this paper we tried to outline the way. In particular, we proposed two

simple, but effective design of NFC and RFID devices to be manufactured and used as engineering tools for enhancing the traceability of bread manufacturing process. As demonstrated in numerous studies, the adoption of blockchain technology in supply chains has a number of benefits. Two well-known advantages concern the ease of managing bureaucratic practices and the ability to trace the origins of products as well as identifying cases of fraud and of counterfeited products, but also facilitating the use of the Internet of Things, allowing the connection of sensors and digital devices taking part in the various stages of the supply chain. References [63]

Our work stems from the need to show the applicability of the blockchain technology in combination with other ones such as IPFS, and RFID and NFC tags, providing a detailed description of a typical agri-food industry that generally operates by applying an HACCP plan. The proposed system contributes to assure the agri-food product quality by improving the management of a large amount of data and by relating all the actors along the supply chain, from field to table, in a secure, transparent, distributed way. It was designed for a typical bread supply chain, that of the Carasau bread, however it can be easily extended to general agri-food supply chains.

As already mentioned this work is part of the *UniCarasau* research industry project, in which a Wireless Sensor Network has been already implemented in order to monitor the processing parameters of the Carasau bread manufacturing. For this reason our future work aims to implement the whole proposed system within this small industry, evaluating its feasibility. The proposed dApp was designed relying on a permissionless platform, an access control system, and on an external database, but can easily be generalized.

A blockchain can be classified as public/permissionless, private or permissioned. In a public blockchain anyone can set up a node and join to the network. In a private blockchain a given number of entities agree and prepare the validator nodes and the access to the network can be public or reserved. Finally in a permissioned blockchain a given number of entities agree and prepare the validator nodes but additional entities can request to become validators.

Our proposed dApp relies on a permissionless Blockchain since our main goal is to render all information around the production of the Carasau bread completely transparent, giving all the actors in the chain the certainty that no type of control or tampering is possible.

As regards the access control system, it is necessary to guarantee the correct access to the system to the various actors. We decided to give this task to a solid and reassuring figure. This figure may be that of a regional body, such as a central authority, that in our case study may be the Sardinia Region.

Finally, as regards the use of an external database, specifically the use of IPFS, it is justified by the fact that WSN may provide an excessive amount of data (see work [64]), an amount of data that may be too large compared to the number of transactions that the blockchain can handle.

In future work our goal will be to create a complete functioning system that operates within the small regional industry representing the case study of this work. So we will evaluate the entire realization cost of the system, taking into account the cost of the gas to execute the Ethereum transaction, the costs due to the use of the external database and the cost of setting up the WSN, giving more details and a PoC about the implementation of the system and its functioning.

ACKNOWLEDGMENT

The authors would like to express their thanks Fabrizio Di Napoli e Antonio Loddo from the M.F.M. of Urrai Salvatora & C. S.N.C to for participating in this study and for the information they freely provided.

REFERENCES

[1] R. K. Apaiah, E. M. T. Hendrix, G. Meerdink, and A. R. Linnemann, "Qualitative methodology for efficient food chain design," *Trends Food Sci. Technol.*, vol. 16, no. 5, pp. 204–214, May 2005.

[2] J. Manyika, S. Ramaswamy, S. Khanna, H. Sarrazin, G. Pinkus, G. Sethupathy, and A. Yaffe, "Digital America: A tale of the haves and have-mores," McKinsey Global Inst., Tech. Rep., 2015, pp. 1–120. [Online]. Available: https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/Digital%20America%20A%20tale%20of%20the%20haves%20and%20have%20mores/ Digital%20America%20Full%20Report%20December%202015.pdf

[3] J. H. Trienekens, P. M. Wognum, A. J. M. Beulens, and J. G. A. J. van der Vorst, "Transparency in complex dynamic food supply chains," *Adv. Eng. Informat.*, vol. 26, no. 1, pp. 55–65, Jan. 2012.

[4] ISO Technical Committee, *Quality Management and Quality Assurance Vocabulary*, Standard ISO 8402:1994, withdrawn and revised by ISO 9000:2000 Quality management Systems–Fundamentals and Vocabulary, 1994. Accessed: Oct. 11, 2020. [Online]. Available: https://www.iso.org/standard/20115.html

[5] L. Cocco and K. Mannaro, "A blockchain-based traceability system model for a typical Italian bread supply chain," in *Proc. IEEE Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, 2021, pp. 669–678, doi: 10.1109/SANER50967.2021.00085.

[6] M. M. Aung and Y. S. Chang, "Traceability in a food supply chain: Safety and quality perspectives," *Food Control*, vol. 39, pp. 172–184, May 2014.

[7] A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the Internet of Things and blockchain technology in supply chain management," *Future Internet*, vol. 11, no. 7, p. 161, Jul. 2019.

[8] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. 14th Int. Conf. Service Syst. Service Manage.*, Jun. 2017, pp. 1–6.

[9] H. Huang, X. Zhou, and J. Liu, "Food supply chain traceability scheme based on blockchain and EPC technology," EasyChair Preprint no. 1525, EasyChair, 2019.

[10] G. Baralla, A. Pinna, R. Tonelli, M. Marchesi, and S. Ibba, "Ensuring transparency and traceability of food local products: A blockchain application to a smart tourism region," *Concurrency Computation: Pract. Exper.*, vol. 33, no. 1, Jan. 2021, e5857. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.5857.

[11] G. Baralla, A. Pinna, and G. Corrias, "Ensure traceability in European food supply chain by using a blockchain system," in *Proc. IEEE/ACM 2nd Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB)*, May 2019, pp. 40–47, doi: 10.1109/WETSEB.2019.00012.

[12] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired RFID-based information architecture for food supply chain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5803–5813, Jun. 2019.

[13] X. Zhang, P. Sun, J. Xu, X. Wang, J. Yu, Z. Zhao, and Y. Dong, "Blockchain-based safety management system for the grain supply chain," *IEEE Access*, vol. 8, pp. 36398–36410, 2020.

[14] *IBM Food Trust: A Modular Solution Built on Blockchain, Benefiting All Network Participants With a Safer, Smarter and More Sustainable Food Ecosystem*. Accessed: Oct. 19, 2020. [Online]. Available: https://www.ibm.com/products/food-trust

[15] L. Parker. (2016). Walmart, IBM and Tsinghua University to use a blockchain for food supply chain tracking in China. Brave New Coin. Accessed: Nov. 9, 2020. [Online]. Available: https://bravenewcoin.com/insights/walmart-ibm-and-tsinghua-university-to-use-a-blockchain -for-food-supply-chain-tracking-in-china

[16] Carrefour. *A Technological Innovation Guaranteeing Secure and Tamper-proof Product Traceability*. Accessed: Oct. 19, 2020. [Online]. Available: https://www.carrefour.com/en/group/food-transition/food-blockchain

[17] Auchan. *Auchan Retail, Press Release–5 November 2018: Food Traceability. After Successful Tests in Vietnam, Auchan Retail is Launching Blockchain Technology Internationally*. Accessed: Oct. 19, 2020. [Online]. Available: https://www.auchan-retail.com/wp-content/uploads/2019/02/28112018_tracabilite_alimentaire_auchan_retail.pdf

[18] J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis," *TrAC Trends Anal. Chem.*, vol. 107, pp. 222–232, Oct. 2018.

[19] K. Behnke and M. F. W. H. A. Janssen, "Boundary conditions for traceability in food supply chains using blockchain technology," *Int. J. Inf. Manage.*, vol. 52, Jun. 2020, Art. no. 101969. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0268401219303536

[20] T. Ferdousi, D. Gruenbacher, and C. M. Scoglio, "A permissioned distributed ledger for the US beef cattle supply chain," *IEEE Access*, vol. 8, pp. 154833–154847, 2020.

[21] B. Yu, P. Zhan, M. Lei, F. Zhou, and P. Wang, "Food quality monitoring system based on smart contracts and evaluation models," *IEEE Access*, vol. 8, pp. 12479–12490, 2020.

[22] H. Huang, X. Zhou, and J. Liu, "Food supply chain traceability scheme based on blockchain and epc technology," EasyChair Preprint no. 1525, EasyChair, 2019.

[23] Q. Xu, Z. Song, R. S. Mong Goh, and Y. Li, "Building an ethereum and IPFS-based decentralized social network system," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 1–6.

[24] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved P2P file system scheme based on IPFS and blockchain," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 2652–2657.

[25] M. S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS," in *Proc. 7th Int. Conf. Internet Things*, Oct. 2017, pp. 1–7.

[26] Q. Zheng, Y. Li, P. Chen, and X. Dong, "An innovative IPFS-based storage model for blockchain," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. (WI)*, Dec. 2018, pp. 704–708.

[27] R. Norvill, B. B. Fiz Pontiveros, R. State, and A. Cullen, "IPFS for reduction of chain size in ethereum," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1121–1128.

[28] H. Huang, J. Lin, B. Zheng, Z. Zheng, and J. Bian, "When blockchain meets distributed file systems: An overview, challenges, and open issues," *IEEE Access*, vol. 8, pp. 50574–50586, 2020.

[29] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "Blockchain-based, decentralized access control for IPFS," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1499–1506.

[30] M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, "A secure data sharing platform using blockchain and interplanetary file system," *Sustainability*, vol. 11, no. 24, p. 7054, 2019.

[31] M. Baire, A. Melis, M. BrunoLodi, A. Fanti, and G. Mazzarella, "Study and design of a wireless sensors network for the optimization of bread manufacturing process," in *Proc. 26th Telecommun. Forum (TELFOR)*, Nov. 2018, pp. 1–4.

[32] M. Baire, A. Melis, M. B. Lodi, P. Tuveri, C. Dachena, M. Simone, A. Fanti, G. Fumera, T. Pisanu, and G. Mazzarella, "A wireless sensors network for monitoring the carasau bread manufacturing process," *Electronics*, vol. 8, no. 12, p. 1541, Dec. 2019.

[33] ISO Technical Committee, *Traceability in the Feed and Food Chain—General Principles and Basic Requirements for System Design and Implementation*, document ISO 22005:2007, Geneva, Switzerland, 2016. Accessed: Nov. 10, 2020. [Online]. Available: https://www.iso.org/standard/36297.html

[34] N. Marques, J. Matias, R. Teixeira, and F. Brojo, "Implementation of hazard analysis critical control points (HACCP) in a SME: Case study of a bakery," *Polish J. Food Nutrition Sci.*, vol. 62, no. 4, pp. 215–227, 2012.

[35] E. Parliament and Council. (2004). *European Parliament and Council Regulation (EC) no 852/2004*. Accessed: Dec. 8, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004R0852&from=DE

[36] I. S. Arvanitoyannis and A. Traikou, "A comprehensive review of the implementation of hazard analysis critical control point (HACCP) to the production of flour and flour-based products," *Crit. Rev. Food Sci. Nutrition*, vol. 45, no. 5, pp. 327–370, Jul. 2005.

[37] F. Fanari, G. Carboni, M. Grosso, and F. Desogus, "Thermogravimetric analysis of different semolina doughs: Effect of mixing time and gluten content," *Chem. Eng. Trans.*, vol. 75, pp. 343–348, 2019.

[38] F. Fanaria, F. Desogusa, E. A. Scanob, G. Carbonic, and M. Grossoa, "The rheological properties of semolina doughs: Influence of the relative amount of ingredients," *Chem. Eng.*, vol. 76, pp. 703–708, Oct. 2019.

[39] F. Fanari, G. Carboni, M. Grosso, and F. Desogus, "Effect of the relative amount of ingredients on the thermal properties of semolina doughs," *Chem. Eng.*, vol. 76, pp. 1207–1212, Nov. 2019.

[40] L. Marchesi, M. Marchesi, and R. Tonelli, "ABCDE–agile block chain DApp engineering," *Blockchain: Res. Appl.*, vol. 1, nos. 1–2, 2020, Art. no. 100002. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2096720920300026

[41] F. Galli, F. Bartolini, G. Brunori, L. Colombo, O. Gava, S. Grando, and A. Marescotti, "Sustainability assessment of food supply chains: An application to local and global bread in Italy," *Agricult. Food Econ.*, vol. 3, no. 1, p. 21, Dec. 2015.

[42] L. Marchesi, M. Marchesi, L. Pompianu, and R. Tonelli, "Security checklists for ethereum smart contract development: Patterns and best practices," 2020, *arXiv:2008.04761*. [Online]. Available: http://arxiv.org/abs/2008.04761

[43] L. Marchesi, M. Marchesi, G. Destefanis, G. Barabino, and D. Tigano, "Design patterns for gas optimization in ethereum," in *Proc. IEEE Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, Feb. 2020, pp. 9–15.

[44] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.

[45] J. Benet, "IPFS–content addressed, versioned, P2P file system," 2014, *arXiv:1407.3561*. [Online]. Available: http://arxiv.org/abs/1407.3561

[46] R. Gist. (Apr. 22, 2018). *Building an Ethereum Oracle With Web3.js 1.0*. Accessed: Nov. 6, 2020. [Online]. Available: https://medium.com/@robinagist/building-an-ethereum-oracle-with-web3-js-1-0-1272b59cfc31

[47] J. Zuercher, L. Hoppie, R. Lade, S. Srinivasan, and D. Misra, "Measurement of the complex permittivity of bread dough by an open-ended coaxial line method at ultrahigh frequencies," *J. Microw. Power Electromagn. Energy*, vol. 25, no. 3, pp. 161–167, Jan. 1990.

[48] N. L. Chin, G. M. Campbell, and F. Thompson, "Characterisation of bread doughs with different densities, salt contents and water levels using microwave power transmission measurements," *J. Food Eng.*, vol. 70, no. 2, pp. 211–217, Sep. 2005.

[49] R. Jedermann, T. Pötsch, and C. Lloyd, "Communication techniques and challenges for wireless food quality monitoring," *Phil. Trans. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 372, no. 2017, Jun. 2014, Art. no. 20130304.

[50] D. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*, 2nd ed. Oxford, U.K.: Newnes, Nov. 2007, p. 504.

[51] F. Bibi, C. Guillaume, N. Gontard, and B. Sorli, "A review: RFID technology having sensing aptitudes for food industry and their contribution to tracking and monitoring of food products," *Trends Food Sci. Technol.*, vol. 62, pp. 91–103, Apr. 2017. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01602565

[52] A. Fanti, R. Secci, G. Boi, S. Casu, G. A. Casula, G. Mazzarella, and G. Montisci, "A polycarbonate RFID tag for blood chain tracking," in *Proc. IEEE Int. Symp. Antennas Propag. USNC/URSI Nat. Radio Sci. Meeting*, Jul. 2015, pp. 356–357.

[53] F. Gandino, B. Montrucchio, M. Rebaudengo, and E. R. Sanchez, "On improving automation by integrating RFID in the traceability management of the agri-food sector," *IEEE Trans. Ind. Electron.*, vol. 56, no. 7, pp. 2357–2365, Jul. 2009.

[54] K. V. S. Rao, P. V. Nikitin, and S. F. Lam, "Antenna design for UHF RFID tags: A review and a practical application," *IEEE Trans. Antennas Propag.*, vol. 53, no. 12, pp. 3870–3876, Dec. 2005.

[55] G. Marrocco, "The art of UHF RFID antenna design: Impedance-matching and size-reduction techniques," *IEEE Antennas Propag. Mag.*, vol. 50, no. 1, pp. 66–79, Feb. 2008.

[56] H. Saghlatoon, L. Sydanheimo, L. Ukkonen, and M. Tentzeris, "Optimization of inkjet printing of patch antennas on low-cost fibrous substrates," *IEEE Antennas Wireless Propag. Lett.*, vol. 13, pp. 915–918, 2014.

[57] G. A. Casula, G. Montisci, and G. Mazzarella, "A wideband PET inkjet-printed antenna for UHF RFID," *IEEE Antennas Wireless Propag. Lett.*, vol. 12, pp. 1400–1403, 2013.
[58] G. Marrocco, E. Di Giampaolo, and R. Aliberti, "Estimation of UHF RFID reading regions in real environments," *IEEE Antennas Propag. Mag.*, vol. 51, no. 6, pp. 44–57, Dec. 2009.
[59] P. Mariage, M. M. Handeme Nguema, and L. Clavier, "Study of the readability of passive UHF RFID Tags placed inside a cargo Van by a reader located outside," *J. Commun. Softw. Syst.*, vol. 10, no. 2, pp. 76–82, 2014.
[60] C. Peres, M. Pigeon, N. Rather, D. Gawade, J. Buckley, H. Jafarzadeh, and B. O'Flynn, "Theoretical models for underwater RFID and the impact of water salinity on the design of wireless systems," *Int. J. Adv. Netw. Services*, vol. 13, no. 34, pp. 45–59, 2020.
[61] F. W. Grover, *Inductance Calculations: Working Formulas and Tables*. Chelmsford, MA, USA: Courier Corporation, 2004.
[62] B. Musigmann, H. Von Der Gracht, and E. Hartmann, "Blockchain technology in logistics and supply chain management—A bibliometric literature review from 2016 to January 2020," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 988–1007, Nov. 2020.
[63] P. Gonczol, P. Katsikouli, L. Herskind, and N. Dragoni, "Blockchain implementations and use cases for supply Chains–A survey," *IEEE Access*, vol. 8, pp. 11856–11871, 2020.
[64] M. Conoscenti, A. Vetro, and J. C. De Martin, "Peer to peer for privacy and decentralization in the Internet of Things," in *Proc. IEEE/ACM 39th Int. Conf. Softw. Eng. Companion (ICSE-C)*, May 2017, pp. 288–290.

LUISANNA COCCO received the Ph.D. degree in electronic and computer engineering from the University of Cagliari, in 2013. Since June 2013, she has been collaborating with the Agile Group, which is a research group in the field of software engineering at the Universit degli Studi di Cagliari, Italy. Since 2014, she has extended her research interest to the modeling and simulation of the cryptocurrencies systems publishing articles of great significance for the scientific community and in general to the blockchain technology. Her research interests include modeling of the complex systems, in particular economic and financial systems with heterogeneous agents.

KATIUSCIA MANNARO received the Engineering degree *(summa cum laude)* from the University of Cagliari, Italy, in 2001, and the Ph.D. degree in electronic engineering and computer science, in 2008, with a thesis on Adopting Agile Methodologies in Distributed Software Development. From 2010 to 2017, she worked as a Postdoctoral Fellow with the Department of Electrical and Electronic Engineering (DIEE), University of Cagliari, where she has been holding a postdoctoral fellowship position with the Department of Mathematics and Computer Science, since 2019. Her research interests include blockchain technologies, software modeling, and agile and lean methodologies. She received a Scholarship for the Young Researchers in FIRB Project (MAPS-Agile Methodologies for Software Production), in 2003.

ROBERTO TONELLI (Member, IEEE) received the Ph.D. degree in computer engineering and the Ph.D. degree in physics from the University of Cagliari. He was with Abilitazione Scientifica Nazionale Universitaria, MIUR, as a Full Professor in Computer Science (Inf-01) and as an Associate Professor in Sistemi di elaborazione delle informazioni (Ing-Inf 05). He currently teaches at the University of Cagliari the courses of informatics and datascience. He holds a postdoctoral position and has been a Visiting Researcher at EECS Department, University of California at Berkeley and the University of Maryland, Washington. His research interests include multidisciplinary and include power laws in software systems, complex software systems, agile development, and software quality. Since 2014, he extended his research interest to the Blockchain technology. He has been awarded the 50 topmost interesting articles on Blockchain at the Blockchain Connect Conference, in San Francisco, in 2019, where he was an Invited Speaker. He is the Delegated Representative of Unica for the Italian Blockchain Service Infrastructure (IBSI) and an MISE Representative for the ESSIF at European Blockchain Service Infrastructure (EBSI).

LORENA MARIANI received the bachelor's degree in electrical and electronic engineering and the master's degree in electronic engineering from the University of Cagliari, in 2015 and 2019, respectively, where she is currently pursuing the Ph.D. degree in electronic engineering and computer science, framed in an Industrial Ph.D. program with Studio A. Her research interests include design and manufacturing of electromagnetic devices for industrial process monitoring and the quality assurance, compliance and control systems for industrial applications, and especially in the bread manufacturing industry.

MATTEO B. LODI (Graduate Student Member, IEEE) received the bachelor's degree in biomedical engineering from the University of Cagliari, Cagliari, in 2016, and the master's degree in biomedical engineering from the Politecnico di Torino, Turin, Italy, in 2018. He is currently pursuing the Ph.D. degree in electronic engineering and computer science with the University of Cagliari. His research interests include modeling of bioelectromagnetic phenomena, especially hyperthermia treatment, the study, manufacturing, and synthesis of magnetic biomaterials for tissue engineering applications, and the use of microwave for biotechnology and environmental applications. He was awarded as the Young Scientists at General Assembly and Scientific Symposium of URSI 2020. He serves as Topic Editor for *Electronics* (MDPI). He has been appointed as a Representative for the Young Professionals of the IEEE Region 8 Nanotechnology Council. He is a member of the Editorial Board of the IEEE Future Directions Newsletter, Technology Policy Newsletter, and Ethics Newsletter.

ANDREA MELIS received the bachelor's degree in biomedical engineering from the University of Cagliari, Italy, in 2017. He worked as an Assistant Researcher with the University of Cagliari. His research interests include EM modeling and development of RF coils at low and high frequencies, especially for MRI at high field, the design and realization of WSN systems for the monitoring of industrial processes, such as bread manufacturing, and intelligent transportation systems.

MARCO SIMONE received the master's degree in electronic engineering and the Ph.D. degree in electronic and computer engineering from the University of Cagliari, Italy, in 2011 and 2016, respectively. His research interests include optimization techniques applied to electromagnetics problems, microwave components design for radioastronomy applications, and antennas design.

ALESSANDRO FANTI (Member, IEEE) received the Laurea degree in electronic engineering and the Ph.D. degree in electronic engineering and computer science from the University of Cagliari, Cagliari, Italy, in 2006 and 2012, respectively. He worked as Postdoctoral Fellow with the Electromagnetic Group, University of Cagliari, from 2013 to 2016, where he is currently an Assistant Professor. His research interests include use of numerical techniques for modes computation of guiding structures, optimization techniques, analysis and design of waveguide slot arrays, analysis and design of patch antennas, radio propagation in urban environment, modeling of bio-electromagnetic phenomena, and microwave exposure systems for biotechnology and bio-agriculture. He is also an Associate Editor of the IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology (J-ERM).