

UNICA UNIVERSITÀ DEGLI STUDI DI CAGLIARI



This is the Author's accepted manuscript version of the following contribution:

Baralla G, Pinna A, Tonelli R, Marchesi M, Ibba S. Ensuring transparency and traceability of food local products: A blockchain application to a Smart Tourism Region. Concurrency Computat Pract Exper. 2021;33:e5857. https://doi.org/10.1002/cpe.5857

When citing, please refer to the published version.

This article may be used for non-commercial purposes in accordance with Wiley Terms and Conditions for Use of Self-Archived Versions. This article may not be enhanced, enriched or otherwise transformed into a derivative work, without express permission from Wiley or by statutory rights under applicable legislation. Copyright notices must not be removed, obscured or modified. The article must be linked to Wiley's version of record on Wiley Online Library and any embedding, framing or otherwise making available the article or pages thereof by third parties from platforms, services and websites other than Wiley Online Library must be prohibited.

This full text was downloaded from UNICA IRIS https://iris.unica.it/

Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

ARTICLE TYPE

Ensuring transparency and traceability of food local products. A blockchain application to a Smart Tourism Region

Gavina Baralla*[1] | Andrea Pinna[1] | Roberto Tonelli[2] | Michele Marchesi[2] | Simona Ibba[1]

[1]Department of Electrical and Electronic Engineering (DIEE), University of Cagliari, Italy
[2]Department of Mathematics and Computer Science, University of Cagliari, Italy

Correspondence
*Gavina Baralla. Email: gavina.baralla@diee.unica.it

Summary

This paper proposes a blockchain oriented platform to guarantee the origin and provenance of food items in a Smart Tourism Region context. Local food and beverage, in fact, can become a good combination to attract tourist and to promote the area provided that their provenance is clearly certified. We designed and developed a blockchain based system to manage an agri-food supply chain for tracking food items. By using smart contracts the platform guarantees transparency, efficiency and trustworthiness. Our system is particularly suitable to manage cold chain since the system interfaces with IoT network devices providing detailed information about data monitoring food such as storage temperature, environment humidity and GPS data. All involved actors can share data and information in a more efficient, transparent and tamper proof way than traditional systems.

The final consumer can access with transparency to all the agri-food chain of the purchased product and verify provenance by retrieving all detailed information registered in the blockchain public ledger.

The proposed system has been designed according to the ABCDE method, an agile development process recently conceived, to obtain a higher software quality to design a general blockchain system by means software engineering practices. A real case study applied to local products from Sardinia, Italy, is proposed at the end of the paper.

KEYWORDS:
blockchain, smart contract, supply chain, traceability, IoT, smart tourism

1 | INTRODUCTION

Until recently, only experts and connoisseurs travelled to discover local food and wine, dying to meet new territory and searching for new taste or authentic flavours. Nowadays, gastronomic tourism is a fast-growing industry, many areas are popular for food thus becoming a holiday destination. Touristic destinations must, therefore, be equipped with cutting-edge tools that, in a context of Smart Tourism, guarantee the originality of local products. Indeed, this kind of tourism can attract potential visitors, offering huge potential growth for local areas, cities, regional and national economies. A good visitors experience can ensure loyalty from visitors, in addition, the same visitors can become promoters of the area for future tourists. To exploit this potential, on the one hand, destinations have to adopt marketing strategies and on the other hand authorities have to protect and promote cultural heritage. For these reasons, the guarantee of product quality, authenticity and provenance is a key aspect to take into account in the supply chain management.

Within this context we propose a blockchain oriented platform to secure storage origin and provenance for food data. By exploiting the blockchain distributed and immutable nature the proposed system ensures the supply chain transparency with a view to encouraging local regions by promoting the smart food tourism and by increasing the local economy. Thanks to the decentralized application platforms that make us able to

develop smart contracts, we define and implement a system that works inside the blockchain and guarantees transparency, reliability to all actors of the food supply chain.

The food supply chain is a complex system in which citizens, institutions, businesses and tourists converge in a meeting based on two strategic axes: innovation and protection of product quality.

In the field of food safety, the guarantee of products quality is a key element. Traceability is considered a must and it is necessary not only from a regulatory standpoint: it allows monitoring the effectiveness of production, of processing, of logistics and sales systems in food chains and increases customer confidence and trust. The integrity of the food chain does not only include security problems, but it is also involved in the field of counterfeiting in order to limit the possibility of forgery and fraud. To address these requirements, a traceability system is needed to provide information on the origin, on processing, on retailing and on the final destination of food products. It is, therefore, necessary to have a product identity card which guarantees its originality, provenance and properties in an immutable way and that certifies in a transparent and reliable way every single step in the production, supply and retail chain.

In addition, food quality must be preserved in all the distribution process. To satisfy this requirement, the environmental conditions must be continuously monitored and this is usually done by means of specific sensors. The temperature is one of the physical dimensions that mostly impact the final quality, especially for easily perishable or frozen food. It is very important to monitor storage and transport conditions, and, in relation to the time, evaluate if these are compliant or not with requirements. Excursion tolerance from optimal storage conditions is related to the duration of the excursion. In a transparent traceability system, eventual anomalies in the storage and transport conditions should be made available for the checking to the final customer.

In order to comply with all these needs, we use an approach based on the blockchain technology as a means of safeguarding the local foodstuffs with special characteristics. In fact transparency, reliability and invariability of data are intrinsic properties of any blockchain technology. The distributed digital ledger enables a secure strategy for implementing and recording transactions, contracts and agreements, it is an excellent solution for those who wish to tell the history of their product in order to ensure reliability. We design our system according to an Agile development process method which allows developers to obtain a higher software quality by applying software engineering practices. To guarantee the food provenance and its integrity, we introduce in our system IoT devices, such as sensors to monitor food storage conditions, and GPS to trace food delivery. Lastly, we introduce the *certifier* figure to evaluate and certify the food integrity during all phases within the distribution chain. The integration of all these elements makes our system particularly suitable for cold chain management given the environmental food monitoring by means of temperature or humidity sensors.

As a case study, we applied the proposed system to trace the food distribution chain in the Sardinia Region. It must be noted that the geographical characteristics of the insularity of Sardinia characterize typical gastronomic products which are very original and connected to the agro-pastoral world.

The paper is structured as follows. Section 2 and 3 present research background and related works. Section 4 describes a system overview of the proposed platform and Section 5 illustrates the system design. In Section 6 we present the case study. Section 7 presents discussion and limitation of the system. Finally, Section 8 contains the conclusions.

2 | BACKGROUND

Blockchain has got most of the media attention thanks to cryptocurrencies popularity, such as Bitcoin. The two concepts are so intertwined that many people still confuse them. As the name suggests, a blockchain is composed of blocks, a growing list of records, chained in chronological order and managed by a peer to peer network. Therefore, a record within the blockchain can not be modified retroactively because of its structure. Due to the recent success of the Ethereum blockchain and other platforms that allow the execution of smart contracts, blockchain represents a promising alternative to the classic databases managed by central authorities and is likely to have a wide range of applications also in industry. Smart contracts are computer programs which are implemented to run inside the blockchain. In general, a smart contract allows to organize information of a specific domain of interest and provides functions to interact with data stored inside it or inside other smart contracts. Currently, the most used blockchain platform for deploying and running smart contracts is Ethereum and the most used programming language is *Solidity*, which is a domain specific language. The Ethereum blockchain contains hundreds of thousands of smart contracts and these are characterized by a very varied set of aims and technical characteristics [1].

The blockchain is gaining attention at all levels, especially political and institutional; this technology can support the digital revolution that is already underway, especially in the industry field. The blockchain is inappropriately called by many people a democratic technology, furthermore, it is defined by many as the third Internet: the Internet of Value [2] [3], after the first Internet of People and the second one, the Internet of Things. Contrary to a centralized model managed by a few people, the blockchain paradigm leads to a distributed model, closer to the territory, where all participants can have control with a radical and new approach on the issues of transparency or security.

A blockchain can be not only permissionless, therefore public, but also private or federate (permissioned). The choice of the blockchain to be used depends on a number of factors such as the problem to be faced, the actors involved and the objectives intended to achieve. Hyperledger is one of the most important projects of blockchain permissioned.

At the start of 2018, the European Commission launched the EU Blockchain Observatory and Forum[4]. It has as primary objectives to map key initiatives, to support the emergence of new ones, to monitor developments and inspire common actions enabling the provision of more efficient services. Recently, also the MISE, Ministry of Economic Development in Italy, started a pilot project, focused to exploit the blockchain technology for the protection of the Made in Italy. The project is entrusted to IBM and looks into the issues of products traceability within the supply chain. The purpose is to guarantee the origin of agri-food products and, at the same time, to provide new technology solutions to hinder the counterfeiting. The need to know the benefits and effects that come from the use of blockchain expands also to the increasing interest of the companies.

Among all sectors, one that is apprehending a strong use of blockchain technology is the food industry[5 6 7 8 9 10]. The blockchain supports companies in the traceability within the supply chain, following the product from its origin, production, and distribution to the final consumer that has the possibility to read all product history. The use of that technology allows to remove intermediaries and to improve trust among actors in the value chain.

Also, startups are showing their interest in the blockchain technology to guarantee product traceability. Examples of that kind of startups are Everledger[11] for diamonds, Provenance[12] for food, BlockVerify[13] for pharmaceutical and luxury goods.

Among the big companies who are using the blockchain solution we have: Carrefour, Nestlè, Unilever, Walmart, Alibabà, Barilla supported by IBM and Baci Perugina supported by Microsoft.

Eventually, blockchain can improve business process both in governments and in companies starting a new distributed business based on the peer-to-peer exchange without the need for intermediaries.

2.1 | Blockchain and Iot

In literature, there are several works proposing blockchain-based technologies solutions applied to smart cities[14 15 16] where the use of IoT devices is seen with a huge business potential due to the possibility of the devices to generate data, interconnect and communicate each other by means of the Internet. Dabbagh et al.[17] conducted a bibliometric analysis on the state of the art concerning the use of IoT with blockchain technology, where they state that the integration between the two has opened up new lines of research, especially in security and privacy. Several works[18 19 20 21] proposed the blockchain as a secure execution environment to satisfy IoT devices security requirements and to prevent IoT attacks. Dorri et al.[22 23] presented an IoT system applied to a smart home. Devices composing the system are connected by means of a private blockchain where a miner manages the network and the access policies. A smart device is able to store data on a local storage system by using a shared key provided by the miner, or within cloud storage. The recording within the cloud is checked by the miner. He generates a signed transaction with the device's key within a public blockchain by sending the addresses of the cloud, and the payment through bitcoin. Similarly, Bahga et al.[24] proposed a blockchain platform for Industrial of Things (IIoT) in which devices communicates both with the cloud and with the blockchain network. The IoT devices can send transactions to the associated smart contracts and receive transactions from other devices on the Ethereum blockchain by means of an integrated single-board computer (SBC) which also allows communication with the cloud. Hang et al.[25] proposed a decentralized architecture for runtime monitoring of IoT devices behaviour where the system business logic is handled by a smart contract which automates time-consuming processes. Authors implemented a prototype by using Hyperledger Fabric for the business logic and a single-board computer for the access control. Huh et al.[26] proposed the use of Ethereum blockchain to build an IoT system. They conceived the IoT keys management by using the RSA public-key cryptosystem in which public keys are stored within the blockchain network whereas private keys are recorded in each device. Like the two previously mentioned works, IoT devices use a Raspberry Pi board, so they are able to interface with blockchain by triggering events and executing transactions.

3 | RELATED WORKS

The concept of Smart Tourism is very recent. It is a logical consequence of the innovations and of the technological progress applied to traditional tourism, but not only that. Smart Tourism is connected to the idea of smart destinations and more generally of Smart Cities. All those specific characteristics of urban or even rural areas typical of a Smart City, and therefore useful to residents can also be used by tourists in the context of mobility, sustainability and quality of visits[27 28]. According to Buhalis and Amaranggana[29] the Smart Tourism destinations could contribute to the improvement of tourists experiences proposing products and services tailored for each visitor with the understanding of its needs, wishes and desires.

In 2015 Bateman [30] focused on the value of traceability. The paper presents an encrypted item (bar-codes, tags or the serial number representing physical goods) of the transaction and sends it out to all other nodes in the blockchain network. The nodes verify if this item of transactions is legitimated and add it to a ledger that then serves for future transactions.

Tian [5] proposed in 2016 the use of blockchain technology in an agrifood context. The work is based on RFID and blockchain technology for sharing and transferring information about the production, the processing, the storage, the distribution and the selling of foodstuffs. The next year Tian [31] proposed a system which considers the real-time food tracing, based on an Internet of Things, IoT, blockchain and HACCP (Hazard Analysis and Critical Control Points) and provides a platform transparent, reliable, secure and useful to all the actors of the supply chain.

However, Toyoda et al. in their work [32] analyzed the limits of RFID technology proving it unreliable in the post supply chain since tags can be rather easily cloned in the public space. Moreover, authors develop an experimental Ethereum blockchain based on the proof-of-concept block validation providing an analysis of cost performances, the cost of managing the ownership of a product with six transfers results in about one USD.

Baralla et al. [33] implemented a generic agri-food supply chain system by using Hyperledger Sawtooth, a permissioned blockchain characterized by a control layer that allows a central authority to legitimate participant of the chain.

In his research Jeppsson and Olsson [10] studied the blockchain technology applied to a supply chain for a four-party logistic (4PL) firm to increase traceability and transparency. A scalable blockchain database named BigchainDB is described by McConaghy et al. [34]. It combines the key benefits both of traditional distributed databases and traditional blockchain. From enterprise-grade distributed DB, BigchainDB inherits high throughput, high capacity, low latency, NoSQL query language, and permissioning. At the same time, it has the blockchain benefits of decentralized control, immutability, and creation and transfer of assets

The works of Kim et al. [35] [36] focused on ontologies as tools that can contribute to blockchain design applied to food provenance knowledge and traceability. Authors use the Ethereum blockchain platform for developing smart contracts supporting goods traceability and analyze the provenance of luxury goods produced and transported in international, big and complex supply chains.

We report in Table 1 the comparison between analyzed related works with the results of this paper. Compared to the mentioned works, the main novelties of our work are:

- the use of a new design method, ABCDE, specific for blockchain software systems, Agile approach-based with the aim to correctly guide the design of a blockchain system accordingly to the software engineering principles.
- the use of a public blockchain with an additional layer responsible for the data access related to the distribution chain. By means of a smart contract, read and the write access can be allowed only to enabled stakeholders. This solution matches the advantages of a public blockchain (transparency, trust, robustness) with those of a private blockchain (access control, customized policies and privileges).
- the development of a decentralized application which interfaces with an off-chain centralized database. It contains sensitive data or data protected by privacy policy and data strictly related to the distribution chain for which an access authorization is required.
- The use of IoT and GPS devices to constantly monitor goods in the whole distribution chain.

4 | SYSTEM OVERVIEW

The proposed system is a blockchain based traceability system of agri-food products distribution. The main purpose of the system is to provide a decentralized database of products history from the production to the selling. In our model, the key element of the distribution chain is the *batch*: for it we define its identification code, ID, and its state. We assume that the status of a production batch changes every time a particular "Event" occurs (i.e. exit and entry from warehouse, handling, split, see 4.2). A batch is a lot of products with homogeneous characteristics, as defined in a specific production disciplinary, that transits from its procurer to the final destination. The system is conceived to provide historical data to guarantee and make transparent the preservation of the quality of local products, especially during the storage and the distribution phase. This is made possible by continuous monitoring of a set of relevant environmental conditions, in every point of the distribution chain. Specific IoT devices such as temperature and humidity sensors compose a Wireless Sensor Network (WSN) of the system, which is in charge of launching alerts in the anomalies event. Furthermore, during the distribution phase, some WSN nodes are equipped with a global GPS positioning system possibly supported by an integrated external GIS system. To allow the communication between IoT devices and blockchain network, we assume the use of a single-board computer, i.e. Raspberry Pi, which contains a wallet with keys and ethers, so that devices will be enabled to send transactions and to register events that trigger smart contracts.

Each actor within the system, included IoT devices, is uniquely identified through a blockchain address, thus providing a secure digital identity. We can associate an address to each IoT device by defining it through its MAC address. In the case of sensors, private keys are recorded in each device, whereas public keys are stored in the blockchain. Furthermore, each IoT device is linked to a specific batch and it can only record data related

TABLE 1 A comparative table of analyzed related works

Reference	Design method	Blockchain typology	Architecture	Study Case	Sensors	Costs analysis
Tian [5] (2016)	NA	Public	NA	China food safety and cold chain	RFID based and realtime monitoring	Hardware cost
Tian [31] (2017)	HACCP based	Public	Distributed database	Cold chain	RFID based and realtime monitoring	NA
Toyoda [32]	NA	Ethereum public blockchain	Distributed ledger	Pre and post supply chain	NA	Transaction costs based on gas price
Baralla [33]	ABCDE (Agile based)	Hyperledger private blockchain	dApp with off-chain repository	NA	NA	NA
Jeppsson [10]	NA	Hyperledger private blockchain	dApp with mobile interface	Bring SCM	NA	Overview of Economic efficiency
McConaghy [34]	Feature based	Complementary Public blockchain	Decentralized Database	DNS implementation	NA	NA
Kim [36]	Ontology driven	Ethereum public blockchain	dApp with web based interface	Goods provenance	NA	NA
Our solution	ABCDE (Agile based)	Ethereum public blockchain with permission editing	dApp with off-chain centralized database	Sardinian traditional agri-food products	IoT sensors and active monitoring	Transaction costs based on gas price

to that batch. Only registered devices can access the blockchain system and only authorized address will be able to access the device protecting it from potential external tampering. The risk of hacking is in fact reduced by reducing the potential access points. Definitely, we can consider the values of IoT sensors as a trusted data source for smart contracts.

Below we propose a typical case of distribution chain under normal conditions. It is not the purpose of this manuscript to address in detail possible borderline cases such as wrong goods receiving, anomalies due to transport phase (road accident, strike etc.), undelivered goods, the delivery attempt failed, partial delivery of the batch and so on. Moreover, these cases have often different policies management, depending on the state or region.

Nevertheless, we point-out that any sub-case can be managed by implementing new features within designed smart contracts, each of which manages a specific part of the distribution chain. Besides, our system is implemented by following the ABCDE, an new Agile methodology, the latter well known to allow a flexible and iterative software development, suitable for ever-evolving projects. As discussed later, the use of blockchain technology allows the data storage in a permanent and unchangeable way, therefore all past information can be easily recovered to be analyzed in order to detect anomalies or suspicious behaviour.

Our system is designed as a Decentralized Application (dApp) and in this system, the role of the blockchain is crucial because of its property of transparency, availability and because records are unchangeable. We defined a set of blockchain operations that are executed at each change of the batch status.

4.1 | Batch states in the distribution chain

In our system, a certifying authority authorizes local producers to be part of the system (see 5.2). The authorized producer is able to demonstrate compliance with the procedural guideline, he can record information within the system about his production batch defining a label and an ID. Conversely, given a batch ID, it is possible to associate the "owner" of the batch. A batch changes ID and changes label whenever it is delivered to a new owner. Given an ID, the matching batch is characterized by two typologies of conditions. These are its *current state* and its *conformity*.

The current state describes the batch state in terms of its handling. Given an ID, a batch can be "In Stock" when it is placed in the production site or in a warehouse, "In Transit" when it is transported on a means of transport, or "Delivered" if the batch has left the associated owner.

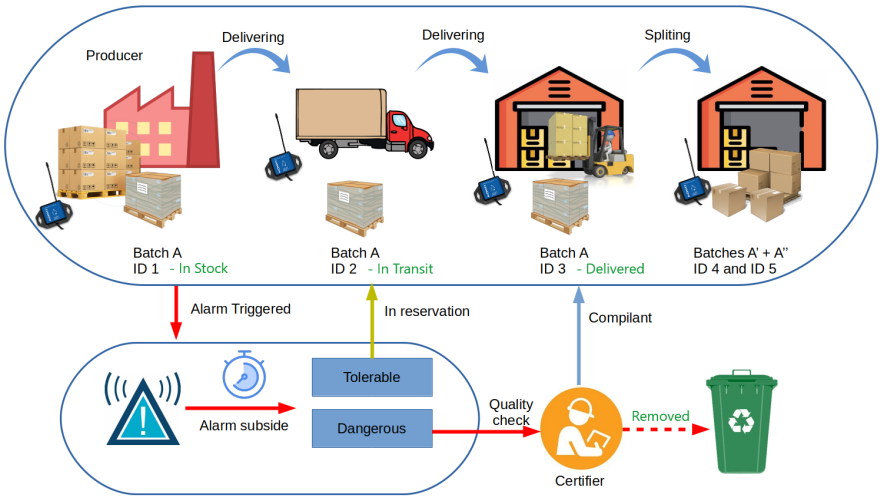


FIGURE 1 Representation of the food distribution chain and the certification chain.

The conformity parameter describes the batch state in terms of preservation of the required quality. Conformity is "Eligible" if it is possible to assure the total integrity of the batch conditions. The conformity of the batch can be "In Reservation" if the batch proceeds in the distribution chain despite it has gone through minor alteration of storage conditions. However, at any point of the distribution chain, an authorized verifier or certifier, can eventually inspect a batch in state of "In Reservation" in order to verify its conformity with quality requirements. After this quality check, the batch conformity recorded in the system can change from "In Reservation" to "Eligible" if the quality check result is positive. Otherwise, the batch is definitively removed from the distribution chain.

We have an "In Pending" conformity whenever the batch has undergone an important alteration of environmental storage conditions. In this case the batch is blocked within the distribution chain, only the certifier can reinsert the batch within the chain by means of a proper evaluation.

Finally, a batch can have "Withdrawn" conformity if it has been withdrawn from the distribution chain because its integrity was not guaranteed.

4.2 | Events in the distribution chain

A batch enters in the traceability system whenever a producer completes the production of a defined quantity of a product and makes it ready to be delivered. As represented in Figure 1, a batch is initially "In Stock" in the production site. Since then, the environmental conditions of the batch are monitored by the WSN and produced data are sent to the blockchain upon the occurrence of certain events. In our model, events lead to a modification of the state of a batch. We model four events which are "Delivering", "Splitting", "Alert" and "Checking". Every time a new event is triggered, the batch information is written to the blockchain. All operations are automated by means of the use of special smart contracts that manage the access and the data writing within the system as described in Section 5.

The event "Delivering" affects a batch in a state of "In Stock" or "In Transit". At this event, a new batch ready to be delivered is created with a new label and a different ID.

The event "Splitting" affects a batch that is in the state of "In stock" inside a warehouse. This event represents the act of dividing the batch in two or more batches of lower quantity of homogeneous products.

The event "Alert" affects batches in a state of "In Stock" or "In Transit". This event occurs when the WSN detects an anomaly in the environmental conditions around a batch. Automatically the system modifies the conformity of the affected batches from "Eligible" to "In pending" and prevents any delivering or splitting operations for these batches. Only a certifier, by means of a "Checking" event, may modify the "In pending" state to reintroduce the batch within the distribution chain. In a borderline case, if no certifier reacts to the alert, after a given period the batch is automatically removed from the entire supply chain. A detailed list of operations relating to each event is described in subsection 5.3.

The event "Checking" affects a batch in a state "In Stock" and occurs when a verifier decides to analyze the conformity of a batch. The conformity state can be "In Reservation", "In Pending" or even "Eligible". Indeed, a certifier may decide to verify the actual suitability of the batch even if no alteration has been recorded by a previous "Alert" event.

5 | SYSTEM DESIGN

As discussed before, the blockchain technology can provide an appropriate solution in all those cases in which a system of relationships entirely based on a concept of trust and transparency is needed, even if the technology still suffers from various drawbacks, mainly related to the missing or to the poor application of good practices of software engineering for blockchain-oriented software development [37].

Due to the innovative technology, the software development involving the Blockchain technology is growing in a quickened rate, this speed is leading to an unregulated and hurried software development where the software quality or the basics concepts of software engineering are not necessarily guaranteed [38].

In order to take into account the correct software development, we adopted the ABCDE method, Agile Block Chain Dapp Engineering proposed by Marchesi et al. [38]. This is the first Agile method designed with the aim of minimizing the risks on the insecure development of smart contracts through security patterns, checklists and testing. Following this innovative development process, we define requirements system by means of User Stories or Use Cases and by using modified versions of UML diagrams to simplify and allow a correct development. The objective of our system is to certify a generic agri-food supply chain, ensuring integrity and traceability of the food especially during all phases on the distribution chain. The system interfaces with IoT network devices which provides detailed information about data monitoring food such as storage temperature or GPS data.

We assume that all products registered in the system are traditional products certified as such under the current Italian regulation. Therefore, we decide not to monitor, through the blockchain, the upstream phases of food production because we assume that they are already backed up by the control of their origin, and according to the procedural guideline, labelled as "traditional". The 'traditional' Italian products are agri-food references that do not fall within the European food law, but that the Italian Government chose to protect by means of specific regulations, such as those relating to 'PAT', Traditional Agricultural Products. In Italy, 'traditional agri-food products' are defined as typical items whose methods of processing, preservation and maturing are performed homogeneously into a particular territory and according to traditional rules which are extended over time, for a period of at least 25 years. On the contrary, European law identify as quality marks only DOP, IGP, STG and organic certification.

5.1 | Blockchain platform choice

There are different possible choices of blockchain for implementing our platform. We choose the Ethereum blockchain for our system since it offers the possibility to implement smart contracts in a simple way. Furthermore, Solidity is up to now the most used coding language for writing smart contracts, it is continuously supported by the evolution of the Ethereum Virtual Machine with new versions of the compiler and it is continuously documented. Examples of smart contracts source codes are freely available and validated on different online platforms, like Etherscan [39], and bugs and fixing are continuously managed and documented.

A contract in Ethereum, or smart contract, is a special typology of account. It is recorded in a block of the blockchain and can receive and transmit messages from and to another account, by means of transactions. Messages can request the execution of a specific contract function. In the case of agri-chain traceability, for instance, a message can contain the address of the receiver, the name of the function, and a list of parameters that ensure the reliability of the system and protect the originality of local products. For instance, smart contracts can be used in the blockchain to record measurements of product coming from the producers. All actors of the food supply chain can be considered as senders and recipients of transactions. They can be blockchain accounts and defined by an alphanumeric code called address.

Another DLT solution recently applied to the agri-chain industry are private or permissioned blockchain systems. Unlike the previous solution, a central authority or a consortium (limited group of authorized individuals) manages the access to read and write data within the ledger. A private blockchain is not visible from the outside, it does not allow access to external nodes and only known participant can join the network. Actually, permissioned blockchains are becoming increasingly popular to manage agri-food supply chains because of the need to protect sensitive data, to supervised the data access and to avoid the spread of fraudulent information.

Conversely, a permissioned blockchain may still give the sensation to the customer that a control, not actually needed, is in any case applied to the food chain and may introduce the doubt that the central authority or some actor of the production chain can deny the free and complete access to all the desired information. A permissionless and pervasively diffuse blockchain, such as Ethereum, on the contrary gives the sensation that nothing is hidden and all the information on the products is freely accessible, leading to an increment of customer's trust.

In light of these considerations, we decide to use a permissionless platform supported by an additional access control layer and by an external database. The access control layer allows to supervise the read and write of data by licensed stakeholders, namely actors regularly accredited to perform a specific job. The external database contains both sensitive data and a large quantity of data such as those coming from IoT devices, which are too big to be stored in the blockchain. In fact, the data registration within a permissionless blockchain has a cost directly proportional to the data size.

All steps belonging to the supply chain are stored within the Ethereum blockchain by means of transactions. In order to demonstrate the integrity of data stored in the external database, we record in the ledger the hash code of the resource and the URL that points to that resource.

Summarizing, our platform design guarantees the access, the security and the integrity of data combined to the transparency of permissionless blockchain.

5.2 | Actors of the system

Following the ABCDE method, we identified the actors of the system and their interaction with smart contracts (see Figure 2). We report below a detailed description for each of them.

- *Authority* is the entry point of the system. It is a certified figure acknowledged by all participants within the chain. It is responsible for managing the reading and writing accesses in the system by verifying the identities of all actors. Each actor who wants to work into the system must be therefore authorized and certified. The authority also records information about every food product involved that will be certified and monitored by the system.

- *Producer* can record data and documents on a production batch and its shipment. It must communicate with the authority a list or a single food product which is authorized to produce. As explained in Section 4, each batch is physically described by a label and identified by an ID at any time.

- *Distributor/Retailer* adds information about ownership change when it receives the production batch, it can record data about a possible production batch split, moreover, it can record information about the delivery of a new production batch.

- *IoT network devices* monitor the integrity of the batch throughout the supply chain, namely, from the moment the producer records data about the batch until it reaches the final consumer. In particular, we consider as IoT devices a WSN to monitor temperature and humidity of the batch and a GPS integrated with a GIS to supervise its delivery. A single-board computer allow devices to interact with the system. The IoT devices are particularly suitable in a cold chain when the temperature monitoring is essential to guarantee the integrity of the food. Depending on the goods, sensors can be calibrated to control a temperature range. If the temperature does not respect the range the devices trigger an alert. The shipping and delivery of goods can be managed by GPS devices that can trace the path by verifying the correct delivery.

- *Certifier* can record certifications about products integrity during the different phases within the supply chain. Its reports become particularly important for the distribution of the products involved within the cold chain. The certifier is responsible for the product compliance, can check the product integrity by evaluating the alerts of the system. In general, it can decide about the withdrawal from the supply chain in all those cases in which the environment stress has compromised the batch integrity. Like any other actor, a Certifier has to be registered by the system administrator (Authority) within the system by providing its data and its professional trading.

- *Customer* can retrieve all information about the product history, in particular during the distribution chain. A customer by means of a QR code scan can check both the good provenance and the product integrity.

Each of these actors interact with the blockchain system by means of smart contracts to record information about a batch. As described in Section 4, a batch is characterized by its state, it can be "In Stock", "In Transit" or "Delivered". Every time a change from one state to another occurs, information about the batch is recorded within the blockchain. The state change takes place when an event occurs. Totally, three smart contracts manage the reading and the writing of data within our system as described in the next section.

5.3 | The Blockchain subsystem: smart contracts

According to the ABCDE methodology, we design a modified UML diagram, showing the structure of the required smart contracts of the agri-food supply chain system (see Figure 3).

We used some UML stereotypes introduced by the methodology such as «contract», «struct», «map[uint]».

We conceived three different smart contracts:

- ProductionChain, PC. It is responsible for the registration of a new producer and for the login. It contains information of all products and it also allows a producer to record data related to production batches before the delivery to Distributors/Retailers.

- DistributionChain, DC. It enables to read/write data related to the batch movement towards the distribution chain: split, owner change, delivery. In the case of batch anomaly, it will be possible to trace all its ancestors or its successors.

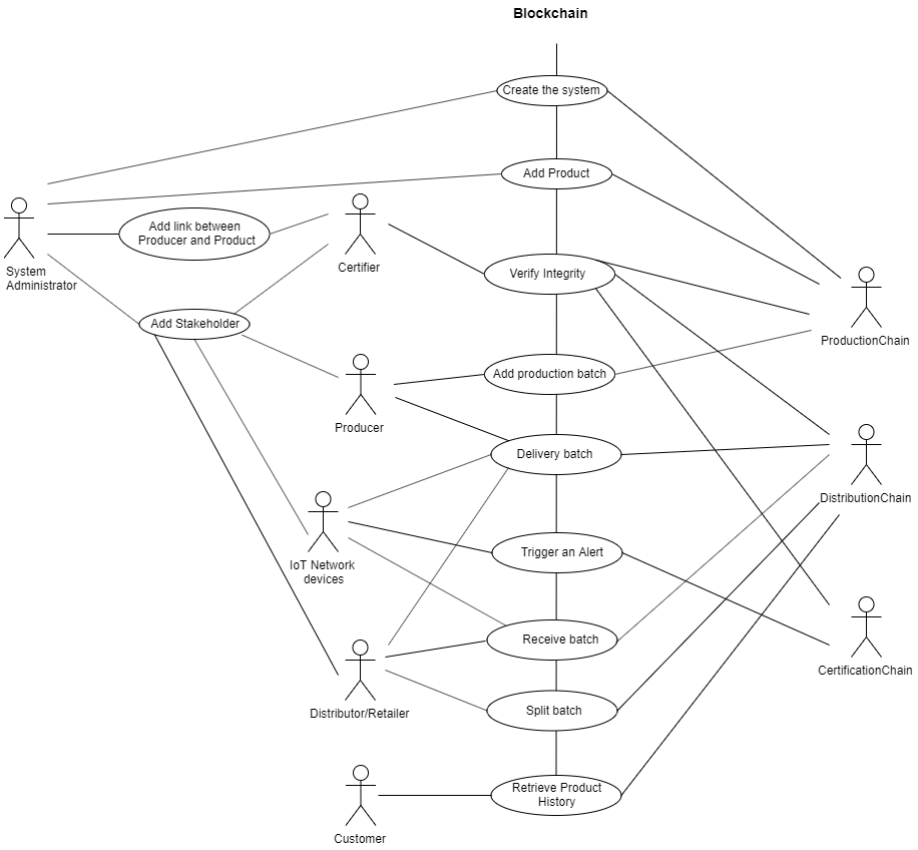


FIGURE 2 The UML Use cases Diagram

- CertificationChain, CC. It provides access to data recorded by IoT devices. A certifier can evaluate the recorded alert to verify the batch integrity by considering the principle of TTT, Time, Temperature Tolerance [40].

Smart contracts interact with each other and manage the access to read and write data to the different actors. The Figure 3 shows the structure of each smart contract.

As described before, each smart contract is responsible for the storage of a certain type of data, related to a specific batch. These data may concern production, distribution or certification phase. Therefore, corresponding data are recorded in the blockchain within data structures defined for each smart contract as shown in Figure 3.

In particular, data in PC are recorded within three main data structures: *Producer* containing information about all producers involved, *Product* and *ProductionBatch*. As mentioned above, we consider to monitor in detail the distribution phase of traditional products, therefore we record within the *Product* data structure information about production phase, processing and storage typical for that product without specifying any detail of raw material. We defined "production batch" a batch released by its producer for the first time within the distribution chain and its corresponding data structure will contain all relevant information about it.

DC contains two main data structures: *Distributor/Retailer*, namely all records related to distributors or retailers involved in the chain, and *Batch*, containing information about the batch subject to monitor.

Eventually, the CC contains information about certifiers and about IoT devices log files stored within *Certifier* and *LogHistory* data structure respectively.

As explained in Section 4, we consider the batch as the key element of the supply chain. The integrity of the batch and also its physical transfer are constantly monitored by means of IoT devices. As shown in Figure 3, each batch has a list of IoT devices linked to it (listIoTDevices). Whenever a new device is associated with a batch, this has to be added to the system by a system administrator (see Figure 2) and is uniquely identified by its own address. Moreover, it is automatically added to the list of devices associated to the batch.

Data detected by sensors as temperature or humidity are periodically written in a log file linked to the batch. During the shipment, in addition to previous data, we can have records coming from GPS devices that confirm the movement of the batch among two different places. All data recorded during the shipment are stored in the respective log files as soon as the batch is delivered.

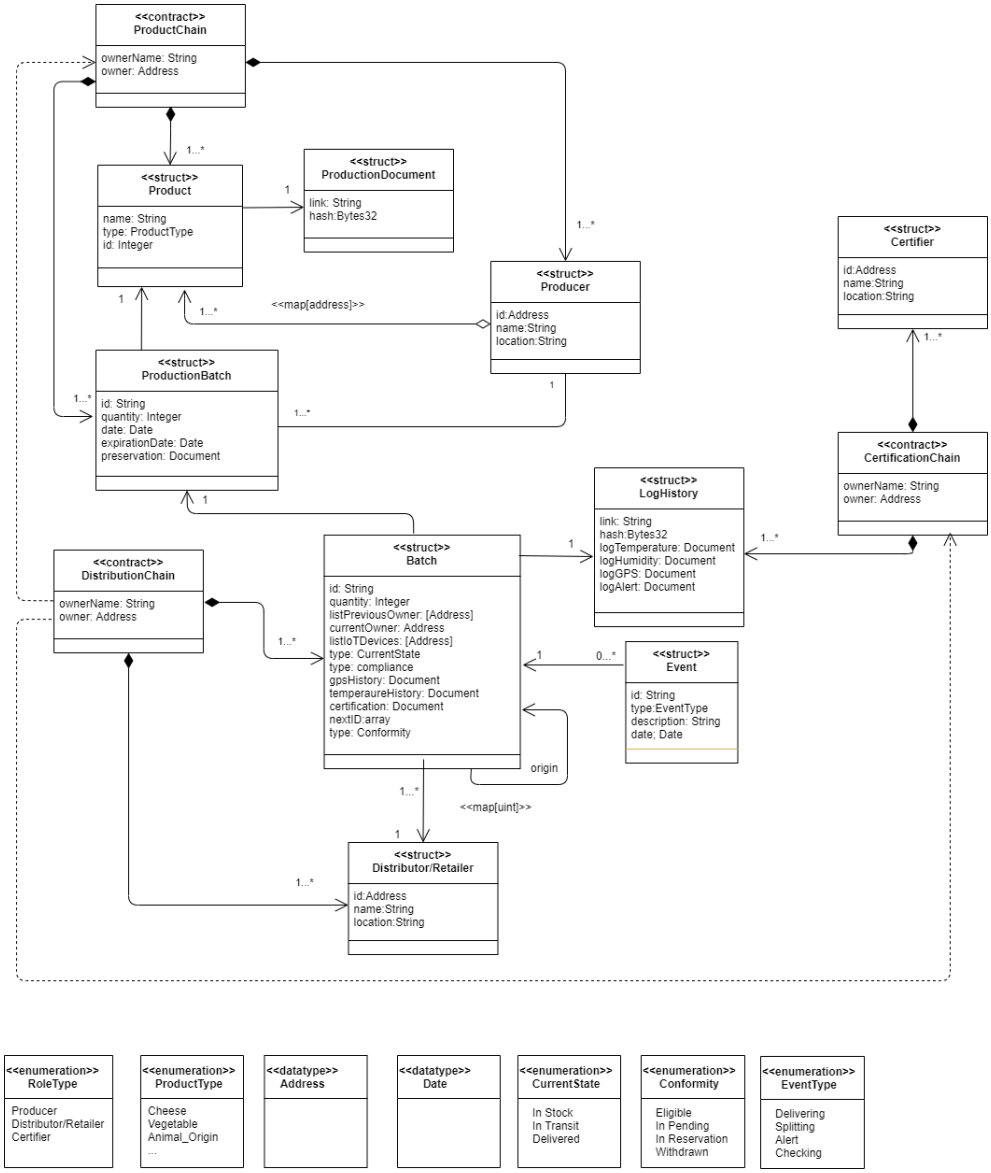


FIGURE 3 The UML of smart contracts and data structure required

In general, we assume to record data within the blockchain system whenever the batch undergoes a change of state or if an Alert event occurs. In any case, all IoT data measurement, recorded on log files and linked to a specific batch, are achievable in the blockchain system after their registration by means of the CC smart contract.

Each record stored in the Ethereum blockchain has a cost, also linked to the amount of saved data. Therefore, we decided to store large data, such as log files coming from IoT sensors, within an external database and to save in the blockchain (CC smart contract) the URL that points to these data, and the hash of the resource.

Whenever a data has to be stored in the blockchain, a new corresponding data structure instance is created by the associated smart contract. If the new instance is an updated information of a batch, a link to the previous one is added. Each smart contract will contain all instances of its data structures related to its corresponding phase: production, distribution or certification. Given a batch id, the DC smart contract that contains the *Batch* data structure is able to retrieve all its past information, since it directly access to its data structures instances and it interacts with the other two smart contracts.

The possible batch states are described by the data type "CurrentState" in Figure 3.

A batch in the "Delivered" state is considered to be old, it can not change its state so it can no longer generate new batches.

Each state change involves the creation of a new batch and the data related to the old batch are archived in the blockchain by means of the three smart contracts. Only the occurrence of an event can cause a change of the batch state. The possible events are described in Figure 3 by the data type "EventType". Moreover, a state change can be influenced by the Conformity condition. Only a batch "Eligible" or "In Reservation" can change its state by generating a new batch and continuing the chain. Instead, a batch "In Pending" or "Withdrawn" is excluded from the distribution chain.

We provide below a detailed description of operations that affect a batch when an event occurs.

Delivering Event.

At this event, an ID, a label, an owner and a link to the old batch are created for the new batch and recorded within the blockchain. Conversely, for the old batch, the dApp system records, in the blockchain, a link to the new batch and potential information coming from IoT devices (such as environmental conditions during the state or GPS data).

In addition, the dApp records in the blockchain all the information about the new batch ownership and associates it to the new ID. The conformity of id1 should not be equal to "In Pending" and its state should not be equal to "Delivered". When a batch transits from an owner to a new owner it creates a new batch with ID = id2. In details:

1. Begin delivering operations of the batch with ID = id1
   (a) The smart contract CC records environmental conditions in the LogHistory data structure for the batch with ID = id1
   (b) The smart contract DC generates a new batch with ID = id2 and it creates a link between id1 and id2. If the id1 was in "In Reservation" conformity also the id2 inherits this state. So, given id2 it will be possible to retrieve data related to id1 such as previous ownership, location and logHistory.
   (c) The smart contract DC changes the state of id1 in "Delivered" and create a link to id2.
   (d) The system prints a label for the id2.
   (e) Operators physically deliver the id2 batch. This operation includes the use of IoT devices, linked to the batch, to monitor the GPS positions in order to certify the delivery.
   (f) The smart contract DC changes the state of id2 in "In Transit" if delivered to a means of transport, or "In stock", if delivered to a warehouse.

Splitting Event.

A batch is divided into two or more batches of lower quantity of homogeneous product before a possible sale. When a batch splits into one or more batches it creates new batches IDs. The conformity of id1 should not be equal to "In Pending" or to "Withdrawn" and its state should be equal to "In Stock". In details:

1. Begin splitting operations of the batch with ID = id1
   (a) The current owner declares the number of new batches resulting after the splitting.
   (b) The smart contract DC creates a new ID for each new batch and it creates a link between the new id and id1. If the id1 was in "In Reservation" conformity, all new batches inherit this state. So, given the new id, it will be possible to retrieve data related to id1 such as previous ownership, location and logHistory.
   (c) The smart contract DC changes the state of id1 in "Delivered" and create a link with each new batches.
   (d) The system print a new label for each new batch.
   (e) An operator physically splits the batch. In case of delivery, this operation includes the use of IoT devices, linked to the new batch id in order to monitor the GPS positions and certify the delivery.
   (f) For each new batch, the smart contract DC changes the state of the new id as "In Transit", if delivered to a means of transport, or as "In stock" if delivered to a warehouse.

Alert Event.

When an IoT device, such as a sensor of a WSN, detects an anomaly in the environmental conditions around a batch, it triggers an alert. The conformity of the batch is modified by the system based on the type of anomaly. In details:

1. The WSN detects an anomaly in environmental conditions and triggers the controls for the affected batches.
2. The system elaborates anomalies by reading log files.

3. If the anomaly is minor or tolerable:
   (a) The smart contract CC records or upgrades within the blockchain the log data related to the anomaly and linked to the batch.
   (b) The smart contract DC sets the conformity of the batch to "In Reservation".
4. If the anomaly is major:
   (a) The smart contract CC records or upgrades within the blockchain the log data related to the anomaly and linked to the batch.
   (b) The smart contract DC sets the conformity of the batch to "In Pending".

Checking Event.
This event occurs when a certifier inspects the conformity of a batch. In details:

1. Given the ID batch, the certifier by means of smart contract DC reads log data recorded within the blockchain of current batch and its ancestors, and he triggers the appropriate controls.
2. If no anomalies are detected:
   (a) The smart contract CC records within the blockchain the data related to the check by linking them to the batch.
   (b) The smart contract DC sets the conformity of the batch to "Eligible".
3. If an anomaly is detected, (i.e. the batch has "In Pending" or "In Reservation" conformity):
   (a) The certifier inspects the batch to ensure its conformity to quality requirements.
   (b) The certifier, by means of CC, records the inspection results and evaluations in the HistoryBatch.
   (c) If quality control provides a compliance result:
      - The smart contract DC changes the conformity to "Eligible"
   (d) Otherwise:
      - The smart contract DC sets the conformity to "Withdraw" and the batch is definitively removed from the distribution chain.

Figure 4 summarizes the operations described above. In particular, we can see a detail of the interaction between actors and smart contracts.
The source code of smart contracts is available at the Bitbucket repository[1].

As described before, each batch is constantly monitored by IoT devices with their log history. All events affecting the batch state, including checking, are stored within the ledger. All certifiers actions, by means of CC, are back-trackable and referred to a specific batch. This implies that information can easily be retrieved to detect and analyse suspicious behaviour. For instance, given a certifier, the system administrator can do statistical analysis on the number of batches certified as "eligible" or "withdrawn" belonging to a specific producer and he can support its inquire by comparing IoT log files with inspection results. In the case of corruption, the administrator can close the certifier account and report the case to law enforcement.

To evaluate the system, during the implementation we conceived both unit tests to find vulnerabilities and bugs, and the acceptance tests in order to verify the consistency of smart contract implementation with the Use Case Diagram reported in Figure 2. As IDE, we used Remix, a browser-based tool to compile Ethereum smart contracts with Solidity language. Moreover we used the Ropsten test network (an Ethereum testnet) to test smart contracts behaviours referring to UML sequence diagram in Figure 4.

6 | THE CASE STUDY

As case study we consider to monitor a supply chain applied to traditional agri-food products coming from Sardinia, Italy. We call our system adapted to the case study as "Bertulas". We presented in detail this case study in the work of Baralla et al[41].

Compared to the previous work, we introduced several features to the blockchain system such as the certifier actor, a new smart contract, CertificationChain, the batch states, the conformity parameter, the events and the interaction with IoT devices to manage the cold chain. Furthermore, the entire system has been redesigned using the ABCDE methodology.

[1]https://bitbucket.org/AgileGroupUNICA/distribution-chain-traceabiltiy/src/master/

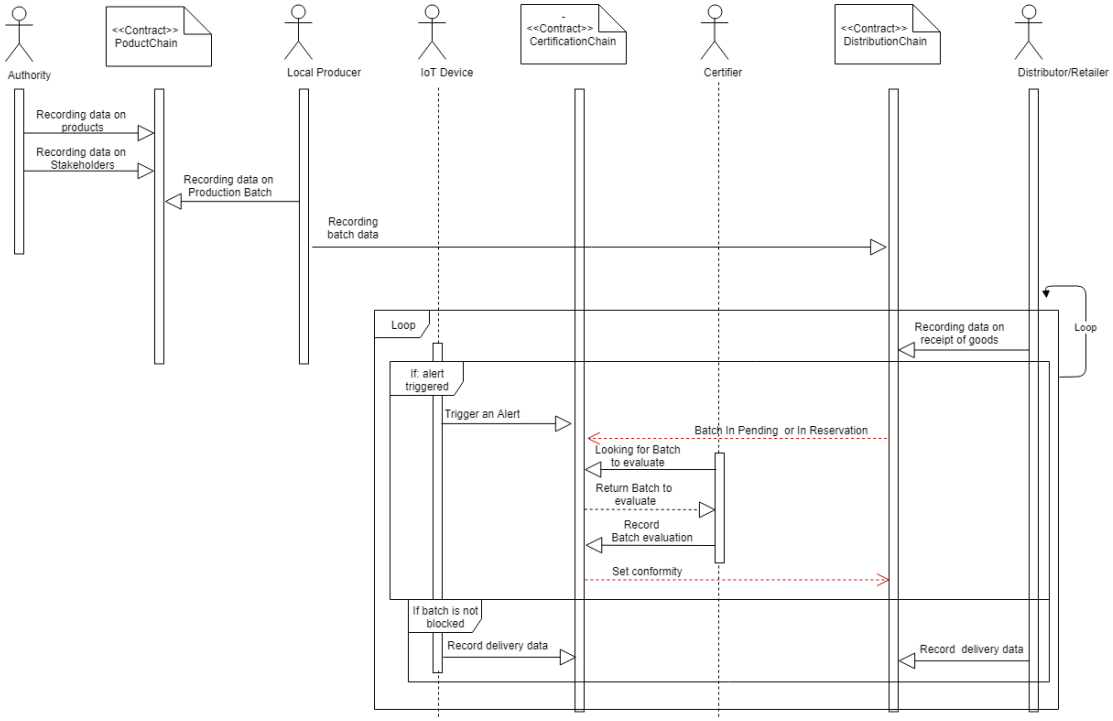


FIGURE 4 Batch Traceability in a Blockchain system: two use cases

Bertulas has been developed with the aim to increase the potential of Smart Tourism in the Sardinia Region through the creation of an innovative pop-up store system (POS), an interactive showcase of products for an effective contextual shopping that can improve the possibilities for tourists to discover the Sardinian food products. Pop-up stores are little local stores, run by an exhibitor, that will be positioned in places of particular touristic interest in order to get the attention of potential customers inviting tourists to live effective shopping experience, innovative and functional to specific needs. The exhibitor will be equipped with a tablet/laptop device connected to the network and channelled on a dedicated e-commerce site. Tourists will able to pay in a secure way, using cryptocurrencies or by credit cards, and can choose a specific method of delivery: at their temporary residence in Sardinia or at their own home in any part of the world. Each movement of products, from local producer to customer, is mapped in a blockchain that has a double role: the role of a public, transparent and immutable ledger, and the role of a control system which safeguards the originality of products. This latter role is implemented thanks to the computing resources available on the blockchain and will be explained later.

The stakeholders involved are:

- *authority* as the system administrator
- *local producers*
- *suppliers* identified as central or peripheral warehouses
- *retailers* identified as pop-up stores and the e-commerce application

The system administrator who provides the access permissions to the system is the public authority in the analyzed reality.

In our case study, we consider the Sardinia Region as the authority, namely the system administrator which inserts and monitors information about all the other stakeholders. Among its many roles, the administrator records data related to local products and about stakeholders involved. Each actor who wants to work into the system must be therefore authorized and certified.

According to the Sardinia Region [42], a total of 205 agri-food products are recognized as traditional. In Table 2 we report the general categories of these products.

Each product will be described by a file composed of 12 different fields: *product name; category; geographical name; synonym; production area; brief product description; traditional procedure, conservation and ageing description of processing the product material, special equipment for the preparation*

TABLE 2 Traditional agri-food products

General Category	Number of products
non-alcoholic beverages, distillates and liqueur	7
fresh meat (and offal) and preparation	16
condiments	1
cheese	20
fat	1
vegetable products in a fresh or processed state	49
fresh pasta, bakery products, biscuits, pastry-making and confectionery	76
gastronomy products	1
seafood preparations, crustaceans and molluscs	14
products of animal origin (honey, dairy products...)	20

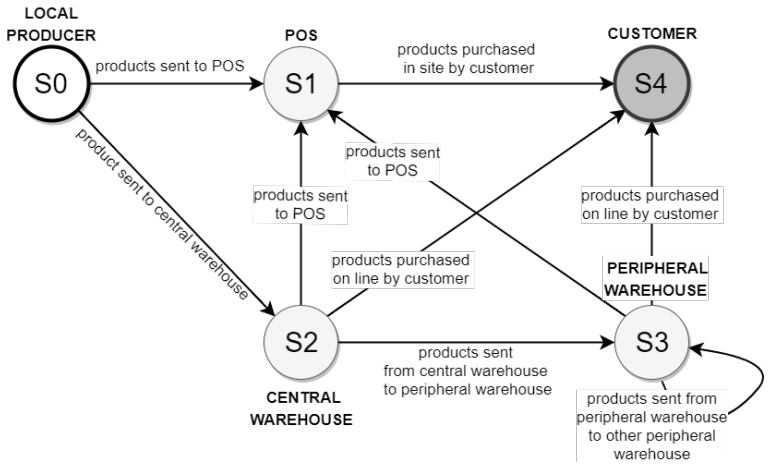


FIGURE 5 The state diagram describing products agri-food chain.

and the conditioning; workrooms description; evidence that the same procedure has been applied at least for 25 years; constancy of the manufacturing process for more than 25 years; exception request about health and hygiene laws.

Given the shelf life, only part of these products will be sold through the system. Currently, this information is public[43]. In addition, there are about ten additional agri-food products certified as traditional product by the Regione Sardegna[44], with a particular certification DOP or IGP in accordance to the Italian law which has a more detailed description and product specification. DOP or PDO have the Protected Designation of Origin, IGP or PGI products have the Protected Geographical Indication.

Figure 5 reports a state diagram describing the supply chain of the local agri-food products. A local producer places on the market the product (S0) that will be purchased at the end by the consumer (S4). A local producer can send the product both to a POS (S1) or to a Central Warehouse (S2). It is possible to have one or more peripheral warehouse (S3). We assume that a consumer can buy a product on site by a POS or online through the e-commerce website.

6.1 | Product Traceability

A consumer can buy a product through a pop-up store or through specialized e-commerce. He can obtain information about the production chain and the supply chain in order to check authenticity, goodness and provenance of the product. The entire system is designed to certify the local agri-food product in order to prevent fraud and to promote the economy in the geographical area. All information about a product is stored in the blockchain. For each product, the system recovers the information and shows it to the consumer who can verify the information by using a simple QR-code reader, or a specialized mobile app linked to the system.

The smartphone application retrieves the information about a product by connecting to DC smart contract (see Figure 2). Given a batch id the DC is able to backtrack to all ancestor batches it derives from.

The customer can also manually verify the product information integrity comparing the hashcode stored in the blockchain with the hash code of the information displayed on the web.

Our solution appears better than traditional solutions because all the infrastructure is already there and is the blockchain itself. There is no need to pay for cloud solutions or for service providers.

Furthermore, maintenance is avoided and customer's trust is maximized because all the infrastructure has not ownership. There are no actors able to manipulate data as it could be for owned or rented infrastructures.

In the specific case of the Sardinia Region, but this is true in general, our solution minimizes the role of the central authority increasing customer's trust. The authority is responsible only for actors and products accreditation, by using already existing infrastructures. After that, no intermediary is involved in the supply chain which is completely controlled through smart contracts in a completely transparent and freely accessible and immutable way. Moreover, in comparison with other public blockchain solutions, only hashed information is recorded into the system reducing Gas costs and payload.

7 | DISCUSSION AND LIMITATION

The blockchain platforms such as Bitcoin and Ethereum were designed to be public and the single distributed ledger is maintained by all participant of the network without any central authority mediation. By applying this technology in an enterprise context different problems can arise.

Even though the smart contracts implementation allows to step forward in the business solution applications, a platform such as Ethereum still presents important gaps linked to the privacy concept. Due to the public system, each company competitor can view data and verify all transactions within the ledger in a totally anonymous form, potentially causing economic damage.

Privacy is a fundamental requirement in the business applications, therefore, the transaction visibility and a data access only to authorized actors would be advisable. Usually, business blockchains tend to have proper authorizations to the accesses by means of the verification of the identity of participants. In this way, access is allowed only to verified users who have demonstrated their identity by using a digital signature or by means of a certificate. Some platforms allow anyone to join, delegating the transaction control to a specific group of authorities within the network recognized as reliable (pool). This solution provides a consensus mechanism more efficient in comparison to based economic incentives systems or on the resolution of computationally complex problems. The use of specific algorithms such as the zero-knowledge proof algorithm [45] allows overcoming the privacy problems. As an alternative, it is possible to choose an implementation based on a permissioned blockchain.

In addition to the privacy, other issues derive primarily from the PoW-based consensus algorithm which causes low throughput, demand for excessive computing power and huge energy consumption. It is possible to carry out a tuning of the main parameters such as block size and time for their generation, number of confirmations per block, mechanism propagation [46], etc., resulting in an increase in performance to the detriment of the security of the network.

Some studies have shown that it is not possible to use permissionless blockchain solutions for IoT applications due to the excessive amount of transactions to be processed, stored and managed [47]. This restriction applies to all possible applications that require a high tps. To overcome this problem it is possible to consider solutions based, for example, on the Bizantine Fault Tolerance and Proof-of-Stake consensus algorithms. In order to overcome these problems, the next Ethereum implementation called Casper will be based on the Proof-Of-Stake algorithm [48].

Also, the low throughput and the high transaction can deal with a private blockchain system but also in this case there are limitations about the management of permissions by a central authority.

Depending on the field applications it is, therefore, necessary to find the right balance between the limits and advantages of using blockchain platforms. Let us not forget that due to the early age of the technology, real and current applications in industrial cases are currently very limited so the technology in this sense is at the stage of its development.

By considering our case study, we decided to use the implemented system with two different levels. The first one as permissioned and supervised by a central authority (Sardinia Region): it allows managing governance rules such as add new products or add new stakeholders (producer, distributor or retailer). Only Sardinian traditional products can be stored within the system and only licensed stakeholders can join the network.

TABLE 3 Estimation of transaction costs to create a Production Batch in December 2019, according to ethgasstation.info.
In the time of the evaluation, 1 ETH = 147.5 USD

Gasprice	5 Gwei	10Gwei
Mean Time to Confirm (Blocks)	5	2
Mean Time to Confirm (Seconds)	63	25
Transaction fee (ETH)	0.00083	0.00166
Transaction fee (USD)	0.12201	0.24402

Such level also includes an external database containing sensitive information and a large quantity of data, such as those coming from IoT devices, too expensive to be clearly stored within the blockchain. The second layer is permissionless: it allows to share data, in terms of hash code, previously stored in the external resource.

Our approach, applied to guarantee the traceability of Sardinian traditional products, attempts to exploit the benefits of public DLT solution by adding some typical features of private DLT such as the access control and the security of sensitive data.

Bertulas is a pilot project, industrial research type and funded by Sardinia Region. We designed our system by considering to monitor the distribution of the traditional products by using the blockchain technology. At the moment no real actors such as producer, distributor or retailer have actually been involved. However, we plan in the next future, within an applied research project supported by local government, to engage local stakeholders to implement real use cases.

7.1 | Cost estimation

We implemented our system using the main net of the public blockchain Ethereum. We have to specify that this blockchain is not cost-less. In particular, every action that modifies the blockchain state implies a cost. In Ethereum, the transaction cost is computed as:

$$TC = GA * GP$$

where TC is the transaction cost, GA is the Gas amount and GP is the Gas price. The Gas amount is a value computed by the Ethereum system based on the data size and on the typology of operations required by the transaction execution. For instance, storage operations require more Gas than mathematical operations. Operations that don't change stored data, such as reading records, are free. The resulting transaction cost depends on the Gas price. The Gas price affects the validation speed. Validating nodes give higher priority to transactions having higher Gas price. Typically, the Gas price is expressed in Gwei (10^9 wei equal to 10^{-9} Eth)

We analyzed which one of the operations we implemented needs more gas. How could it be expected, the record of a production batch is the most expensive operation and requires about 166 thousand Gas unit to be executed.

Given this result, we evaluated a reasonable Gas price for our transactions. We used the tool offered by the ETH Gas Station and available online[2]. It suggests three Gas prices, based on the values currently used by Ethereum users. The three options are Fast (10 Gwei), Average (5 Gwei), and Cheap (3.1 Gwei). The main difference between the three options is the average time for the transaction confirmation. We computed the costs of our transactions considering the Average and the Fast options. Results are reported in Table 3.

On the base of these estimations, we can say that the additional cost of the use of the Ethereum blockchain is low in comparison with the value of the product batch, and the confirmation time is within one minute range.

It should be noted that the average Gas price is variable in the time, as well as the countervalue in fiat currency of one ether. A unit of Gas has a cost in fiat currency equal to the Gas price in ether multiplied per the countervalue of one ether. We examined two periods of time to evaluate the average transaction cost expressed in USD: the first covers the entire month of November 2019; the second covers one year, between December 1st 2018 and December 1st 2019. The average cost of recording a new production batch in the blockchain is 0.44 ($\sigma = 0.067$) USD in November 2019 and 0.50 ($\sigma = 0.57$) USD in the year between December 1st 2018 and December 1st 2019. We collect the Gas price time series from the available data in the website etherscan.io.

We also analyzed the problem of paying transaction costs. In fact, the sender of the transaction must pay for it. In our system, several actors send data to the blockchain: the system administrator, each producer, each distributor/retailer, and also the IoT devices which monitor the environment around the batch. Each of them has an Ethereum address. The cost of the transaction will be deducted from the address balance. For this reason, it is mandatory that address and device owners regularly check the balance of the accounts. These operations can be facilitated with the use of a specially developed web application. In our case study, it is possible that the Sardinia Region incentives the use of the system by taking on all the

[2]https://www.ethgasstation.info

costs of the transactions and sending with regularity a proper amount of ether to system operators' addresses. If there is no public administration covering transactions costs these must be supported by all stakeholders but, as reported in Table 3, these can be considered negligible and are balanced by many benefits. In fact the use of blockchain carries numerous benefits: less bureaucracy, lower costs with respect to a similar traditional system, no costs for the infrastructure which is already existing, data are shared almost instantly, transparency, security, trust and so on.

8 | CONCLUSIONS

The proposed system aims at increasing the tourism potential of a region through the enhancement of local products, able to tell, even with their taste, the uniqueness of the tradition and culture.

The system is based on the blockchain technology and uses the Ethereum platform to implement an agri-food distribution chain by means of smart contracts. We know in fact, that to reach the end consumer each product deals with a complex production and distribution network and in the most recent period the need of transparency for end users is increasing even more rapidly. Sometimes information about provenance exists, but the trustworthiness is often hard to verify. Currently, there is a strong need to rely on someone who can guarantee the integrity and provenance of goods and products. Moreover, given the complexity of the supply chain, it would be desirable to have specialized entities for each different process in the supply chain causing the increase of product price.

We proposed to solve the problem of traceability through the decentralized and reliable blockchain technology as a means of safeguarding the local foodstuffs with special characteristics and in order to create their digital identity card. By using smart contracts the platform guarantees provenance, integrity, transparency and trustworthiness.

The final consumer can verify the *provenance* by checking the product history from the introduction in the distribution chain to the end retailer. For example he can easily verify the producer from the information recorded in the Ethereum blockchain. The *integrity* of data can be proved by comparing the hash code stored in the public ledger with the hash code of the resource stored in the external database. *Transparency* is ensured by the use of a permissionless blockchain where all transactions are public and anyone can verify them. Eventually, *trustworthiness* is guaranteed by the use of a blockchain system where data are unchangeable once they are written within the system. Moreover, each stakeholder has to be authorized to write data related to the agri-food chain avoiding fraudulent access.

All involved actors can share data and information in a faster, cheaper and more efficient way with respect to traditional systems. In fact, everyone in the supply chain can track the ownership of the product and the location during all the time. Our system is also particularly suitable for cold chain management thanks to the use of IoT devices, such as temperature and humidity sensors to monitor the food preservation environment, and GPS to check goods delivery. The presence of certifiers allows evaluating the provenance and the food integrity during the entire distribution chain. In case of batch anomaly, it will be possible to trace all batch ancestors or its successors.

We designed our system by following the ABCDE method, an agile development process particularly useful to develop a higher blockchain system software quality applying the rules of software engineering.

We discuss a real case study for the supply chain management adapting our system to the protection of Made in Sardinia products food.

Lastly, the final consumer can be sure that the purchased product is original because he can retrieve detailed information, as for example the provenance from the distribution chain. We believe that this kind of system may encourage the purchase of typical products by increasing the local economy.

As future works, we are planning to extend our system to trace also the origin of raw materials. In this way, the platform will be applied to monitor a generic agri-food supply chain not necessarily oriented towards traditional products.

ACKNOWLEDGMENTS

Conflict of interest

The authors declare no potential conflict of interests.

References

1. Pinna A, Ibba S, Baralla G, Tonelli R, Marchesi M. A Massive Analysis of Ethereum Smart Contracts Empirical study and code metrics.. *IEEE Access* 2019: 1-1. doi: 10.1109/ACCESS.2019.2921936

2. Swan M. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc." . 2015.

3. Tapscott D, Tapscott A. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin . 2016.

4. European Commission . Policy - Blockchain Technologies. 2018. https://ec.europa.eu/digital-single-market/en/blockchain-technologies. Accessed June 10, 2019.

5. Tian F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: 13th international conference on service systems and service management (ICSSSM). IEEE. ; 2016: 1–6.

6. Caro MP, Ali MS, Vecchio M, Giaffreda R. Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In: IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), 2018. IEEE. ; 2018: 1–4.

7. Casado-Vara R, Prieto J, Prieta lFD, Corchado JM. How blockchain improves the supply chain: case study alimentary supply chain. *Procedia Computer Science* 2018; 134: 393 - 398. The 15th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2018) / The 13th International Conference on Future Networks and Communications (FNC-2018) / Affiliated Workshopsdoi: https://doi.org/10.1016/j.procs.2018.07.193

8. Galvez JF, Mejuto J, Simal-Gandara J. Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends in Analytical Chemistry* 2018.

9. Malik S, Kanhere SS, Jurdak R. ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains. In: 17th International Symposium on Network Computing and Applications (NCA). IEEE. ; 2018: 1–10.

10. Jeppsson A, Olsson O. Blockchains as a solution for traceability and transparency. 2017.

11. Time-Lapse D. https://diamonds.everledger.io. Accessed June 11, 2019.

12. Provenance . https://www.provenance.org/. Accessed June 11, 2019.

13. Blockverify . http://www.blockverify.io/. Accessed June 11, 2019.

14. Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. In: IEEE. ; 2016: 1392–1393.

15. Sun J, Yan J, Zhang KZ. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation* 2016; 2(1): 1–9.

16. Ibba S, Pinna A, Seu M, Pani FE. CitySense: blockchain-oriented smart cities. In: ; 2017: 1–5.

17. Dabbagh M, Kakavand M, Tahir M. Towards Integration of Blockchain and IoT: A Bibliometric Analysis of State-of-the-Art. In: Springer. ; 2019: 27–35.

18. Ali J, Ali T, Alsaawy Y, Khalid AS, Musa S. Blockchain-based Smart-IoT Trust Zone Measurement Architecture. In: ; 2019: 152–157.

19. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. *Ieee Access* 2016; 4: 2292–2303.

20. Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security* 2018; 78: 126–142.

21. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems* 2018; 82: 395–411.

22. Dorri A, Kanhere SS, Jurdak R. Blockchain in internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187* 2016.

23. Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. In: IEEE. ; 2017: 618–623.

24. Bahga A, Madisetti VK. Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications* 2016; 9(10): 533–546.

25. Hang L, Kim DH. Reliable Task Management Based on a Smart Contract for Runtime Verification of Sensing and Actuating Tasks in IoT Environments. *Sensors* 2020; 20(4): 1207.

26. Huh S, Cho S, Kim S. Managing IoT devices using blockchain platform. In: IEEE. ; 2017: 464–467.

27. Avila L. dA. Smart destinations: XXI century tourism. In: ENTER2015 conference on information and communication technologies in tourism, Lugano, Switzerland. ; 2015: 4–6.

28. Gretzel U, Sigala M, Xiang Z, Koo C. Smart tourism: foundations and developments. *Electronic Markets* 2015; 25(3): 179–188.

29. Buhalis D, Amaranggana A. Smart tourism destinations enhancing tourism experience through personalisation of services. In: Information and communication technologies in tourism 2015. Springer. 2015 (pp. 377–389).

30. Bateman AH. Tracking the value of traceability. *Supply Chain Manag. Rev* 2015; 9: 8–10.

31. Tian F. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In: International Conference on Service Systems and Service Management. IEEE. ; 2017: 1–6.

32. Toyoda K, Mathiopoulos PT, Sasase I, Ohtsuki T. A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access* 2017; 5: 17465–17477.

33. Baralla G, Pinna A, Corrias G. Ensure Traceability in European Food Supply Chain by using a blockchain System. 2019.

34. McConaghy T, Marques R, Müller A, et al. BigchainDB: a scalable blockchain database. *white paper, BigChainDB* 2016.

35. Kim HM. IoT and Blockchain Aware Ontologies for Supply Chain Provenance. SSRN 2818557, 2016.

36. Kim HM, Laskowski M. Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management* 2018; 25(1): 18-27. doi: 10.1002/isaf.1424

37. Porru S, Pinna A, Marchesi M, Tonelli R. Blockchain-Oriented Software Engineering: Challenges and New Directions. In: 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C). ; 2017: 169-171

38. Marchesi M, Marchesi L, Tonelli R. An Agile Software Engineering Method to Design Blockchain Applications. In: 14th Central and Eastern European Software Engineering Conference Russia. ACM. ; 2018: 3.

39. Etherscan . https://etherscan.io/. Accessed June 11, 2019.

40. FAO . Temperature-Time Tolerance. 2007. http://www.fao.org/3/V3630E/V3630E03.htm#2.7%20Time-Temperature%20Tolerance. Accessed June 10, 2019.

41. Baralla G, Ibba S, Marchesi M, Tonelli R, Missineo S. A Blockchain Based System to Ensure Transparency and Reliability in Food Supply Chain. In: European Conference on Parallel Processing. Springer. ; 2018: 379–391.

42. Regione Sardegna . Elenco nazionale prodotti agro-alimentari tradizionali della Regione Sardegna. https://www.regione.sardegna.it/documenti/1_850_20190418163507.pdf. Accessed June 11, 2019.

43. Regione Sardegna . Elenco dei prodotti tradizionali. https://www.regione.sardegna.it/j/v/25?s=3724&v=2&c=6&t=1. Accessed June 11, 2019.

44. Sardegna Agricoltura . DOP e IGP. http://www.sardegnaagricoltura.it/argomenti/prodottitipici/dop-igp/. Accessed June 11, 2019.

45. Li B, Wang Y. RZKPB: a privacy-preserving blockchain-based fair transaction method for sharing economy. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE. ; 2018: 1164–1169.

46. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the security and performance of proof of work blockchains. In: SIGSAC conference on computer and communications security. ACM. ; 2016: 3–16.

47. Conoscenti M, Vetro A, De Martin JC. Peer to Peer for Privacy and Decentralization in the Internet of Things. In: 39th International Conference on Software Engineering Companion (ICSE-C). IEEE. ; 2017: 288–290.

48. Buterin V. Proof of Stake FAQ. 2019. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ. Accessed June 10, 2019.

AUTHOR BIOGRAPHY

Gavina Baralla is a research fellow in Mathematics and Computer science at the University of Cagliari. She holds a Ph.D. in Electronic and Computer Engineering from the Department of Electrical and Electronic Engineering (DIEE) of the University of Cagliari in 2019 with a thesis entitled "Enabling technologies for the development of smart cities". Her research interests are focused on the study of the blockchain technology applied to different sectors such as e-health and agri-food chain management. Moreover, her studies concern the Knowledge Management referred to Semantic Web, use of taxonomies, ontologies and linked data.

Andrea Pinna received the Master degree in electronic engineering from the University of Cagliari in 2012 and the Ph.D. degree in Computer Engineering from the University of Cagliari in 2018. Since 2018 has been a research fellow at the University of Cagliari.

His research interests concerns the study of blockchain technology and its applications. His topics of interest include the study of smart contracts, the development of decentralized applications, and the enhancement of the software sustainability by using the blockchain technology. He also dealt with the study of data stored inside the blockchain, of network features and users' behaviors.

Roberto Tonelli received the Ph.D. degree in computer engineering and the Ph.D. degree in physics. He is currently a Temporary Researcher and a Professor with The University of Cagliari, Italy. The main topic of his research has been the study of power laws in software systems within the perspective of describing software quality. Since 2014, he has been extended his research interest to the Blockchain technology. His research interests are widespread and multidisciplinary.

Michele Marchesi has been Full Professor since 1994 at the Faculty of Engineering of the University of Cagliari. Since 2016 he is Full Professor at the Department of Mathematics and Computer Science of the University of Cagliari where he teaches the Software Engineering course. He is the author of over 200 international publications, including over 70 in the magazine. He was one of the first in Italy to deal with OOP, since 1986. He was founding member of TABOO, the Italian association on object-oriented techniques. He has also worked on object analysis and design, UML language and metrics for object-oriented systems since the introduction of these research themes. In 1998 he was the first in Italy to deal with "Extreme Programming" (XP) and agile methodologies for software production. He organized the first and most important world conferences on "Extreme Programming and Agile Processes in Software Engineering" in Sardinia in 2000, 2001 and 2002. Since 2014, being among the first in Italy, he has extended his research interest to blockchain technologies, obtaining significant results in the scientific community.

Simona Ibba received the B.S. and M.S. degrees in electronic engineering from the University of Cagliari and received the Ph.D. degree in Computer Engineering from the University of Cagliari in 2019.

Her scientific research activities are focused on the study of blockchain based software and in particular on the application of the Agile methodologies in blockchain software development. Her interests also include the Knowledge management development and in particular the knowledge representation design, strategies for knowledge management, and the study of taxonomies, folksonomies, Digital libraries, and scholarly literature.

How to cite this article: G. Baralla, A. Pinna, R. Tonelli, M. Marchesi, S. Ibba (2019), Ensuring transparency and traceability of food local products. A blockchain application to a Smart Tourism Region, *Concurrency and Computation, Special Issue on FPDAPP18, Future Perspectives on Decentralized Applications*, *2019;00:1–6*.