

# Using blockchain and IoT in food supply chains: an empirical study

*Pamela Danese*

*Department of Management and Engineering, University of Padova, Vicenza, Italy*

*Riccardo Mocellin (riccardo.mocellin.1@phd.unipd.it)*

*Department of Management and Engineering, University of Padova, Vicenza, Italy*

*Pietro Romano*

*Polytechnic Department of Engineering and Architecture, University of Udine, Italy*

## Abstract

Blockchain technology (BC) is gaining interest from both academics and practitioners that recognize its potential to face food safety, authenticity, and integrity issues. However, little is empirically known, and existing literature is dominated by conceptual studies highlighting the many promises of the technology. Following the calls for research aimed at learning from BC pioneers, we investigate an in-depth case study and derive insights on how BC combined with internet of things (IoT) can impact food supply chains. We adopted the agency theory as theoretical lens to better interpret empirical evidence.

**Keywords:** Blockchain, supply chain management, internet of things

## Introduction

Food supply chains are complex and vast ecosystems that involve a multitude of actors. Globalization, large reliance on paper records, and non-integrated information systems cause a lack of visibility and information asymmetry (Behnke and Janssen, In press).

A series of recent scandals (e.g. China's melamine milk powder, USA's salmonella in peanut butter) confirm the inadequacy of mechanisms currently used to ensure food safety, authenticity, and integrity (Ali *et al.*, 2017). Despite increasingly stringent regulations, about 420,000 people in the world die every year after eating contaminated food (World Health Organization, 2019). Moreover, food frauds cause huge losses in terms of revenues for producers and tax incomes for governments.

To explore the opportunities of BC in addressing these challenges, in the recent past, several BC-based pilot projects have been launched by start-ups and important organizations, such as Walmart, Nestle, and Carrefour (Kshetri, 2018).

Many researchers agree that BC technological qualities -specifically immutability, transparency, data security, and disintermediation- may significantly support food supply chains in addressing the above-mentioned problems (Bumblauskas *et al.*, 2020; George *et al.*, 2019). In particular, BC is considered especially appropriate for improving

coordination along the supply chain (SC) providing end-to-end traceability, thus fronting food frauds (Galvez *et al.*, 2018).

Some scholars stress the importance of complementing BC with IoT in traceability solutions to automatically collect data and feed the BC, hence, suggest considering their integration in future research (Kim *et al.*, 2018; Mondal, 2019).

Despite high expectations, implications of BC in the food sector are still under-investigated, and existing literature is mostly conceptual, based on literature review or anecdotal-descriptive (Wang *et al.*, 2019). There is a consensus among the research community that there have been few empirical and theoretically grounded investigations into BC application in the SC context with a particular focus on traceability (Kim and Laskowski, 2018; Hald and Kinra, 2019). Moreover, there is little research analyzing how the combined use of BC and IoT can leverage SC traceability (Kamble *et al.*, 2019).

Schmidt and Wagner (2019) encourage the application and validation of the agency theory to foster the topic of BC in the SC context quickly. In the same vein, several other scholars stressed the major importance of analyzing BC implications for SCs from the principal-agent (PA) relationship perspective, pointing out that it is an under-researched issue (Kshetri, 2018; Treiblmaier, 2018; Cole *et al.*, 2019). This theory has been previously used by operations management and supply chain management (SCM) researchers to describe the inter-organizational relationships between separated entities with conflicting interests, i.e. the principal -the entity who delegate certain task- and the agent -the party that is delegated (e.g. Halldórsson *et al.*, 2007; Shook *et al.*, 2009).

From the above, this study aims to address the following research question:

R.Q. – How companies can leverage BC in combination with IoT to face product safety, authenticity and integrity issues in the food industry?

This paper attempts to make two main contributions to literature by using an in-depth case study methodology to examine an initiative promoted by an Italian consortium of orange producers, which led several actors along the supply chain to adopt a traceability system based on BC and IoT technologies.

First, it seeks to contribute with empirical insights to the debate about how BC and IoT can impact food SCs and provide decision-makers with guidelines to decide how to properly configure and use BC-based solutions in the SC field.

Second, this study intends to understand how BC can affect the PA relationship in an uncommon context, where the principal -the consortium- also aims to maximize the benefits of some of its agents, specifically the orange producers belonging to the consortium. In particular, we use the agency theory to help the understating on how BC and IoT can be used to relegate the agency problem of *ex-post* opportunism, i.e. unfair practices driven by the self-interest of agents involved in a relationship (e.g. non-compliance with compulsory requirements of cultivation regulations), which is a crucial factor behind food safety, authenticity and integrity issues. As suggested by Wang *et al.* (2019), we also examine whether governance mechanisms employed by companies played an important role in supporting the developed system in the safeguard against opportunistic behaviors and, more generally, in reducing PA problems.

This investigation is valuable both from a managerial and theoretical perspective. From a theoretical point of view, it contributes to advance BC theory in the SC context, as most of the literature on this theme is merely descriptive. Moreover, it discusses the agency theory under a new technological paradigm. From a practical point of view, the analysis aims to understand why some choices have been taken in order to draw generalizable lessons and stimulate managers' reflection on how to properly configure BC-based solutions according to their specific needs.

## Theoretical background

### *Using BC with IoT to support SCM processes*

Several industries recognize the significant potential of BC for SCM (Abeyratne, 2016; Tian, 2016). Despite this, its development and diffusion outside the finance area are still largely experimental. The technology promises to change how SCs are managed and rethink inter-organizational business processes (Zhu and Zhu, 2016). Most applications in this domain are small scale and carried out by small and medium-sized companies (Gausdal *et al.*, 2018). However, a bunch of pilot projects launched by global organizations, such as Walmart, Unilever, and Maersk, suggests big benefits (Hackius and Petersen, 2017). There is a consensus among scholars that BC will bring a paradigm shift in SC activities in several types of industries, providing trust among suppliers, better efficiency, auditability and security, data integrity, and cost reduction (Heutger, 2018; Kim and Laskowski, 2018). Moreover, through self-executing smart contracts, it promises to lead higher automation and streamline processes (Wang *et al.*, 2019).

Nowadays, many SC actors use isolated IT systems, tracking and recording data without a shared standard, often relying on paper-based documentation (Brody, 2017; Yiannas, 2018). This causes several inefficiencies, such as information asymmetry, errors, and redundancies. On the other hand, BC promises to solve the lack of integration between network members by providing a single and shared version of truth about product flow and related digital assets, such as certifications, invoices, payments, etc. (Tijan *et al.*, 2019). This would enhance SC visibility, help to achieve end-to-end traceability, and strengthen trust in the network (Kshetri, 2018). Better visibility can enable companies to monitor the different SC actors' performance, boost customers' confidence toward brands, and reward producers who employ good production practices (Leong *et al.*, 2019). Moreover, it can make recall actions faster (Creydt and Fischer, 2019).

In general, the BC deployment within SCs entails several design decisions, such as the choice of the permission model (public or private), type of consensus mechanism, properties of blocks, use of smart contracts or token, etc. Moreover, as suggested by several studies, BC should be combined with other technological tools –such as radio-frequency identification (RFID), quick response (QR) codes, near field communication (NFC) tag, artificial intelligence, machine learning– in order to guarantee a durable coupling between physical goods and their digital representation while addressing product physical tempering, perform data exploitation and permit SC partner and final customers to interact with the solution easily (Toyoda *et al.*, 2017; Galvez *et al.*, 2018).

Special emphasis has been placed on using BC in combination with IoT sensors to allow automated, high-quality, and objective data capture (e.g. Zhao *et al.*, 2019). Their integration is considered a major trend by prior researchers, that will affect SCM and may revolutionize the food industry, by enabling real-time traceability of goods along the whole SC, while monitoring those environmental parameters (e.g. temperature, humidity) which can affect the final product quality (Kshetri, 2018; Schmidt and Wagner, 2019).

### *The agency theory*

Agency theory is one of the oldest theories in the literature of management and economics that examines the relationship between an entity, the principal, that delegates another entity, the agent, to work and take decisions on its behalf (Eisenhardt, 1989; Rungtusanatham *et al.*, 2007). According to the theory, if goal conflicts exist between the principal and the agent, the latter tends to act following its self-interest in two major ways, i.e. by misrepresenting its ability (*ex-ante* opportunism) or by hiding its true actions (*ex-post* opportunism) (Schmidt and Wagner, 2019).

A significant factor hindering PA relationship is information asymmetry, i.e. a situation when one party in the relationship has more or better information than the other. It is a factor that, according to the transaction cost theory, opens the way for opportunistic behaviors (Grover and Malhotra, 2003).

In order to resolve the agency problem in PA relationships, agency theory prescribes outcome-based and behavior-based mechanisms (Ekanayake, 2004). In both cases, the principal will seek to minimize the costs of monitoring (e.g. collecting information about agents' behavior) (Eisenhardt, 1989). As Fayezi *et al.* (2012) remark, for those actions that are difficult to observe there is a higher risk of opportunism.

The agency theory is well-established within operations and SCM and has been mainly used to describe governance conflicts between buyers-suppliers, investors-managers, and managers-employees dyadic relationships (Benton and Maloni, 2005) where each actor acts to maximize its convenience.

Various mechanisms can be used to align the behavior of the agents with the principal's interest, such as incentives or the use of information systems that make each party's behaviors more observable, hence reducing information asymmetry. In addition, agency theorists assert that governance mechanisms can help in limiting agency conflicts.

#### *Governance mechanisms on SCM*

Extant literature has shown that corporate governance practices, both relational and contractual, play a central role in safeguarding inter-organizational relationships against opportunism and, more generally, in reducing the PA problems in the SC context (Cao and Lumineau, 2015; Chedrawi and Howayeck, 2018).

Relational governance refers to the extent to which an inter-organizational relationship is governed by self-regulating mechanisms with informal structure. Three of the most known relational governance types are trust, brokered access, and shared goals (Poppo and Zenger, 2002). Trust has been widely recognized as a key factor influencing PA issues and refers to the extent to which a party, in a relationship, believes that another party is honest, i.e. will not exploit any adverse situation (Zaheer *et al.*, 1998).

Different from relational governance, contractual governance highlights the importance of formal contracts that stipulates the responsibilities, obligations, and rights of each party to perform particular actions in the future (Ryall and Sampson, 2009). Third-party bodies are usually involved to intervene if any violation of agreement occurs and therefore to solve the principal agent-dilemma.

#### **Methodology**

Considering the lack of research on this topic, an exploratory, qualitative approach was chosen as a valuable method for the study (Yin, 2017; Eisenhardt and Graebner, 2007). Several scholars stated that case-based research may be particularly useful to advance our knowledge on BC tangible benefits, implementation challenges, and contextual adaptations in the SC field (Treiblmaier, 2018; Cole *et al.*, 2019).

Given the scarcity of empirical prior research and the high complexity of the examined phenomenon, we decided to limit our investigation to a single in-depth case. According to Ridder (2017), single case studies allows answering the "how" question more easily as well as providing detailed descriptions of little-explored phenomena. In addition, they are valuable for explorative theory-building research since they allow investigating complex phenomena inside the real-world context in which they occur (Voss, 2010).

We conducted an empirical investigation involving an Italian consortium of orange producers and packers, comprehending more than 600 associates, that was a pioneer in the BC and IoT adoption as well as the orange producers, packers, and other downstream

actors of the SC. The names of the consortium and other actors involved in the study are not disclosed due to confidentiality issues. A long-term collaborative relationship between the research group and those actors allowed accessing rich data using a variety of data-gathering techniques. It is worth saying that, in this first pilot phase of the project, a total of 13 actors has been involved.

We chose semi-structured interviews with key managers and employees of SC participants as the primary data source. According to Eisenhardt and Graebner (2007), interviews are an efficient way to gather rich data. Each interview lasted on average from 45 to 90 minutes. In this first phase, we collaborated with the project consortium, two producers, and one processor. Besides, we interviewed the technology provider that developed the solution, asking for specific information and documentation, in order to clarify more technical aspects. In total, 10 interviews were conducted. Both the consortium and the technology provider provide us with useful information related to downstream actors that have not been interviewed in this phase.

As suggested by Eisenhardt and Graebner (2007), we complemented and triangulated primary data with secondary data sources, such as web resources or official documentation developed by companies related to the project. The use of different methods and sources of data guarantees the quality and reliability of the findings.

Most of the interviews were done face-to-face, but some were held via telephone or video calls due to logistical reasons. We recorded each interview, transcribed it, and share back our reports to key informants for improving accuracy and validity. We used a research protocol to cover the most relevant issues asking the same questions to different informants, but we also gain valuable data from informal conversation out of the predefined pattern.

Our study investigates the period between January 2019 -the time the project started- and March 2020. Our investigation mainly relied on real-time tracking of information in order to limit the reliance on historical data that usually leads to inaccuracies and biases. Since the project is still in its first phase and more actors will be involved, we plan to study future development.

### **Case description**

The consortium involved in this study, that represents one of the major Italian producers of oranges, is currently piloting a digital solution based on BC and IoT in a project that involves actors at the international level. Three main reasons push the consortium to promote the adoption of this solution. First, the desire to protect three different Protected Geographical Indication (PGI) orange varieties against counterfeiting. In fact, due to their unique characteristics (derived from the particular climatic conditions of the cultivation area) and the high export volume, they are usually subject to imitations. Second, the need to prevent opportunistic conducts of SC actors and ensure the observance of production/product requirements by its associates. Third, the desire to increase the brand reputation in Italian and foreign markets as well as costumers' confidence and loyalty.

The actors involved in this first phase of the project, which represent independent nodes in the BC network, are presented in Figure 1. The vision of the consortium is to involve all the producers and packers as well as other downstream SC actors. The reduced scale of the current project was justified by the need to develop the pilot fast.

Using the solution, each time a bag of oranges changes hands along the physical SC from the cultivation phase to end customer, a transaction with the relative data is recorded on the BC by the SC actor who receives and processes the products. Therefore, a permanent history of each bag is created. Large documents (e.g. certificates, photos in .pdf/.jpg format) are stored off-chain due to their large size.

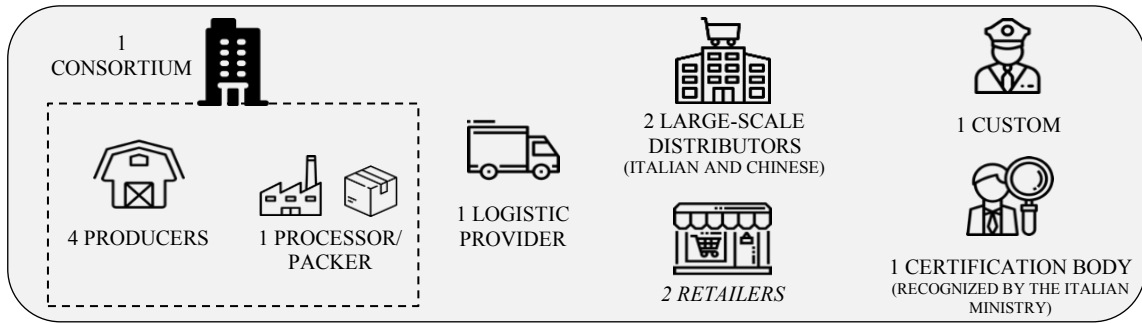







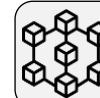





Figure 1 – Actors belonging to the BC network

However, the hash of each document is saved on-chain and works as a pointer that ensures the integrity of the off-chain files. Since transactions are digitally signed by the different SC entities, the latter is responsible for false declarations. The use of a public key infrastructure allows pairing each real-world actor with its digital identity (i.e. its BC public address).

Product-related information comes from three different sources, as shown in Table 1 and can be accessed by final customers by scanning a secure near-field communication (NFC) tag -containing the reference to information saved on BC- through a dedicated mobile application. For each bag carrying the oranges, customers can verify its origin, process steps, expiration date, characteristics, as well as its authenticity.

The system grants different levels of access to the different SC actors, i.e. some information is made visible to every stakeholder while other sensitive data is encrypted and accessible only to authorized actors (e.g. the number of oranges sold by GDOs and retailers can be accessed only by the consortium). Smart contracts are used in combination with IoT to automatically identify any out of tolerance measurement in the cultivation and transportation phase and send alerts to trigger corrective actions. For example, in the cultivation phase, alerts are sent to certification bodies when certain conditions (e.g. lack or excess of rain, high temperature) that could compromise the orange quality occur.

Table 1 – Data sources

1. THIRD-PARTY CERTIFICATION BODIES	2. INTERNAL COMPANIES STAFF	3. IOT SENSORS
 BLOCKCHAIN   CENTRALIZED SERVERS OF THE NATIONAL INFORMATION SYSTEMS   THIRD-PARTY CERTIFICATION BODIES	 BLOCKCHAIN   INTERNAL COMPANIES STAFF	 BLOCKCHAIN   IOT SENSORS
Data related to products (e.g. origin, process steps, etc.) are gathered by third-party certification bodies for regulatory concerns and firstly saved by the public administration in Italian national information systems before being synchronized on BC.	Data is manually uploaded on the BC by the administrative staff of the different SC actors by using a user-friendly interface installed on the devices already in use (e.g. days and kinds of pesticide or fertilizer treatments, date of harvesting, processing methods).	Data is gathered by IoT on a real-time basis during the cultivation and the logistic phases to monitor location, soil quality and environmental parameters, such as humidity levels and temperature, that are critical to guarantee the final products' quality.

At this first phase of the project, the use of IoT has been limited to cultivation and shipment processes but the consortium is evaluating the possibility of extending the IoT use in the future. The solution is based on the Ethereum BC but ensures interoperability with other BC platforms. This allows the involvement of customs and foreign actors, such as the Chinese large-scale distributor, that were already using a specific BC.

In general, the solution implementation does not require major investments, because it did not lead to substantial changes in processes, purchase of new hardware (except for the NFC tags and IoT for cultivation), and BC was simply integrated with existing IT architectures in a short time and with very limited coding requirements. All the expenses of this experimental phase have been covered by the consortium.

### Discussion and preliminary findings

From a preliminary analysis, our findings confirm that BC and IoT can help to address different food SCs issues, providing several of the benefits that are suggested by scholars (e.g. Bumblauskas *et al.*, 2020; George *et al.*, 2019), both for final customers and SC actors (Table 2).

Table 2 – Benefits of solution implementation

SOLUTION FEATURES	BENEFITS FOR FOOD SUPPLY CHAIN
<ul style="list-style-type: none"> <li>• End-to-end data recording from farm until sale</li> <li>• Information sharing between the different SC actors</li> <li>• Data integrity</li> </ul>	<p>FOOD SC TRANSPARENCY</p> <ul style="list-style-type: none"> <li>• Better SC traceability and visibility</li> <li>• Better auditability</li> <li>• Better customer relationship</li> </ul>
<ul style="list-style-type: none"> <li>• Interoperability between BC systems used by diverse actors</li> <li>• Complete transparency along the whole SC</li> <li>• Real-time data gathering through IoT</li> </ul>	<p>FOOD SC EFFICIENCY</p> <ul style="list-style-type: none"> <li>• Information asymmetry reduction</li> <li>• Better collaboration between all the SC actors</li> <li>• Higher speed in data gathering</li> <li>• More efficient export customs operations</li> <li>• Paper-based documents reduction</li> <li>• Faster verification of production requirements adherence</li> </ul>
<ul style="list-style-type: none"> <li>• Full history of the product</li> <li>• Real-time collection of critical environmental parameters</li> <li>• Smart contract to identity out of tolerance measurement</li> </ul>	<p>FOOD SAFETY</p> <ul style="list-style-type: none"> <li>• Better food safety guarantee</li> <li>• Faster and cheaper food recalls</li> <li>• Faster check on the compliance with legal requirements</li> </ul>
<ul style="list-style-type: none"> <li>• Data immutability</li> <li>• Information sharing between the different SC actors</li> <li>• Decentralized network architecture</li> <li>• Objective data gathering through IoT</li> <li>• Use of pre-certified data</li> <li>• Use of an NFC tag that prevents replicability</li> </ul>	<p>FOOD AUTHENTICITY</p> <ul style="list-style-type: none"> <li>• Prevention of opportunistic conducts</li> <li>• Guarantees on product provenance</li> <li>• Prevention of counterfeiting</li> <li>• Support for the brand reputation of honest producers</li> </ul>

From a B2C perspective, this study shows that the solution represents a marketing leverage that allows customers to verify the history, characteristics, and authenticity of each bag of oranges directly through their smartphones, hence increasing their confidence in the brand. Moreover, provided SC traceability, based on data integrity, in combination with the use of a secure and non-replicable NFC tag, help at protecting consumers from counterfeiting. The reliable coupling between the physical products and related information saved on BC is ensured by the decision to pack oranges on heat-sealed mesh bags that prevent any substitution. However, it is worth noting that the different types of data sources provide different guarantees to customers that uploaded data reflect reality.

From a B2B perspective, our findings suggest that the adopted system can substantially influence the PA relationship, by improving the direct vigilance of the consortium (the

principal) on the different SC actors (the agents), hence the detection and deterring of self-serving behavior of the latter. Information on the actions carried out by the different SC actors are permanently saved on BC transactions and, in agreement with what Xu *et al.* (2019) noticed in their study, can be checked at any time and with a minimum reading latency by each SC participant. BC auditability allows reducing information asymmetry, which is a leading cause of agency problems, and provides a solid base for performance evaluation. This finding is in accordance with previous research (Treiblmaier, 2018; Schmidt and Wagner, 2019), that suggests the ability of BC to elude agency issues, by reducing asymmetric information, and therefore to hinder opportunistic behaviors.

While in the SC context the principal generally has incomplete information about agents' behavior and therefore has to trust in their honest behavior to a certain extent (Treiblmaier, 2018), it could be stated that, as previously observed by Voshmgir (2017), BC system allows moving the trust from SC actors to the system itself. The trust in the technology (digital trust) has been recognized by several authors in the literature as a way to prevent SC actors from behaving unethically (Yan and Holtmanns, 2008; Hill *et al.*, 2009). However, compared to traditional digital systems, the trust in BC is higher due to its open-source nature (everyone can check the computer code which governs its functioning), fault-tolerant distributed architecture, and technical characteristics that ensure several qualities, such as the complete visibility and data integrity.

Some considerations regarding the real potential of BC in guaranteeing agents' honest behavior must be done since the degree of trust in the system seems to strongly depend on how data entry is performed that, as remarked by Creydt and Fischer (2019) and Schmidt and Wagner (2019) represents a critical factor in this type of applications.

For those transactions that are manually entered by SC actors, the consortium still needs to trust in the honest behavior of the person who is responsible for data-entry. In fact, manual entry results in data accuracy issues as it opens the possibility of data-entering mistakes or intentional false declarations (van Hoek, 2019). However, as noticed by Pearson *et al.* (2019), every company should theoretically be discouraged by making false statements since each transaction stored in BC is saved immutably and is non-repudiable. In fact, due to the decentralized architecture of the BC network -where each SC actor involved represents an independent node- each transaction is digitally signed and therefore can be attributed to a certain actor, that is responsible for false declarations. Consequently, any competitor could for example access the permanent record of past transactions of the company looking for false information or misbehaviors with the aim of damaging its reputation. From the above, it could be stated that BC alone can create system trust and theoretically prevent opportunistic behaviors only to a limited degree.

Instead, system trust is greater when information uploaded in BC are pre-certified by trusted third-party certification bodies. However, this choice seems incoherent with an important feature of BC, which is disintermediation, i.e. the possibility to execute and verify transactions without the need to rely on central authorities (Wang *et al.*, 2019).

The highest degree of system trust is reached in those phases along the SC where human interactions are eliminated by using IoT that automatically uploads data on BC after signing it, hence ensuring data accuracy (Surasak *et al.*, 2019). It is worth noting that unlike many existing applications, that firstly store data gathered by IoT sensors on centralized servers and subsequently upload a selected subset on BC, data in our case is directly sent to BC, hence avoiding any risk of human manipulation.

In light of these considerations, responding to the call of Wang *et al.* (2019) to examine whether BC can affect trust within companies relationships, it can thus be suggested that BC systems allow shifting the trust in the actors' honest behavior to the trust in the system and prevent agents' opportunism to varying degrees, based on the type of data entry that



is performed. In this regard, IoT sensors play a key role by ensuring that agents do not misrepresent reality.

In the future, the consortium could evaluate reducing human interaction to a different extent based on its trust in the agents, e.g. preferring a wider use of technological tools for automatic data-gathering for those less-trusted actors (e.g. external to the consortium).

In accordance with Ko *et al.* (2018), we also found that the solution can cut the “agency costs”. On the one hand, being used as an effective behavior-based control mechanism, it cuts the expenditures of surveillance carried out by the consortium to evaluate agents’ behavior. Beyond improving SC transparency, through the use of smart contracts the solution allows reducing the number of on-field audits carried out by the certification body to verify the adherence to pre-defined quality criteria. In fact, smart contracts, automatically suggest focusing inspections on those cases when the risk of quality problems is higher based on information gathered by IoT. This finding is in agreement with Wang *et al.* (2019) finding that smart contracts lead to process automation.

On the other hand, the examined system reduces the cost of reassurance of the principal-derived from agents’ willingness to assure they act in the best interest of the former- by digitizing several paper documents that producers were previously obliged to send to the consortium, hence improving the efficiency of information sharing, which also facilitates the compliance with legislation and food safety and quality requirements.

Beyond the increased transparency, empirical findings also demonstrate that the studied solution offers better efficiency in the export customs procedures and make the interaction with large-scale distributors more efficient by ensuring interoperability between BC systems used by diverse actors, thus providing the latter with reliable information on products characteristics and history. As remarked by Kamble *et al.* (2019), this point is of major importance since, to date, ensuring interoperability between different BC solutions represents a major challenge for BC diffusion.

This research also revealed the key role played by the consortium in addressing two well-known threats of BC adoption in a SC context, namely the difficulty to involve different SC participants (which could also be competitors benefiting from information asymmetries) (Kshetri, 2018; Schmidt and Wagner, 2019) and to overcome their resistance to share valued information (Queiroz and Wamba, 2019; Wang *et al.*, 2019).

The involvement of actors internal to the consortium has been favored by the existence of a strong interest alignment -i.e. the shared goals of promoting the product and improve the customer brand loyalty- as well as by the existing trust between them and the consortium, due to the long-term relational commitment. It is worth noting that the relational governance mechanisms of goals alignment and trust also support the restriction of *ex-post* opportunism by means of consortium’s producers/packer. The latter, in the same way as SC actors external to the consortium, may potentially disagree with the defined measures (e.g. stricter controls to assure consumers on product quality). This finding is in accordance with Norrman (2008), who stated that an effective way to deal with agency issues is the use of relational governance mechanisms.

As regards the other entities, the solution adoption by logistic providers and retailers was fostered by their desire to improve their relationship with the consortium by differentiating themselves from their competitors, whereas the adoption by customs, large-scale distributors and certification bodies has been facilitated by their desire to improve their internal processes efficiency due to the enhanced information sharing.

For all the actors, the consortium set precise rules on the use of BC (e.g. what data to be shared) and incentives their participation in the project by covering all the related expenses. Therefore, in this phase, the costs factor was not perceived as a barrier for BC adoption by SC actors, unlike several previous studies argue (e.g. Zhao *et al.*, 2019).

Some potential pitfalls that emerged from empirical evidence are the difficulties in convincing the SC actors external to the consortium to take part in the project, forcing IoT adoption to the carriers and the need for technical expertise within producers to program NFC tags. Moreover, several producers have not been able to participate since they do not have a reliable internet connection, being located in rural areas. As highlighted by Creydt and Fischer (2019), this represents a barrier for BC larger diffusion within SCs.

### **Conclusions**

By analyzing an in-depth case study through the lens of the agency theory, this study adds further insights to the limited amount of empirical research on BC potential in the SC context and contributes to a more theoretically grounded and less hyped discussion. In particular, we gained valuable insights on the potential of the combined use of BC and IoT in addressing product safety, authenticity, and integrity issues in the food industry.

The analysis shows that BC and IoT, beyond providing better assurances to final customers about product characteristics, history and authenticity, help to address the inter-organizational PA dilemma by reducing information asymmetry and therefore the risk of agents' opportunism, that can be at the origin of counterfeiting and food safety issues. The detailed SC visibility provided by BC, together with data immutability, improves the confidence of the consortium (the principal) on the honest behavior of the downstream SC actors (agents) and move the trust from the latter to the technology itself (digital trust) to different extents, depending on the adopted type of data entry. In particular, findings suggest that when data uploaded on BC is preliminarily checked by external certification bodies or collected by IoT sensors, trust in the BC system is higher and agents' opportunism can be better mitigated.

This study highlights the important role of smart contracts in reducing the agency costs of surveillance and automating processes, as well as that of interoperability between the different BCs already adopted by some actors that allow a better efficiency of export customs procedures and interaction between the consortium and large-scale distributors.

We advance that the consortium has major importance in overcoming two serious problems of BC adoption in the SCs, i.e. the necessity to involve the SC actors and their resistance to share internal private information. Besides, our study shows that solution adoption was also facilitated by the relational mechanism of goal alignment and existing trust between the consortium and some SC actors. We also underlined some potential weaknesses that can hinder BC potential in food SCs.

Our aim is to continue this study to learn more from SC actors that were not interviewed in this phase and follow the project's advance beyond its pilot phase to larger implementation, considering that difficulties in scaling up a BC project represent a significant barrier to BC diffusion in the SC context. Thus, beyond providing an overview of the challenges faced to scale up the project, we aim to gain a deeper understanding of (1) BC impacts on the PA relationship, (2) how BC further adoption by other SC actors will be encouraged, (3) whether different measures, in terms of incentives and technological tools, will be used by the consortium to control the agency conflict with those SC members that are not its associates, and (4) how IoT use will be extended to further processes.

### **Acknowledgments**

The research is funded by the Fondazione Cassa di Risparmio di Padova e Rovigo

### **References**

Available upon request.