Journal of Business Logistics

WILEY

ORIGINAL ARTICLE OPEN ACCESS

Blockchain Systems in Food Supply Chains: An Interpretation Through the Lens of Agency and Technology–Organization–Environment Theories

Pamela Danese[1] | Pietro Romano[2]

[1]Department of Management & Engineering, University of Padova, Padova, Italy | [2]Polytechnic Department of Management and Architecture (DPIA), University of Udine, Udine, Italy

Correspondence: Pamela Danese (pamela.danese@unipd.it)

Received: 26 August 2023 | **Revised:** 28 January 2025 | **Accepted:** 10 April 2025

Keywords: blockchain | case study research | food safety and quality | food supply chains | supply chain management

ABSTRACT

Blockchain (BC) systems are increasingly used by consortia to monitor ex-post opportunism in food supply chains. BC systems differ for BC technical characteristics, complementary technologies, and organizational tools. Yet, little is empirically known about the link between different BC system designs and the *context* where they are implemented and how contextual factors influence the adoption of each BC system. This study analyzed different BC systems in 11 principal–agent dyads within one food supply network. Each dyad is composed of a consortium of fruit producers and packers (the principal) and a supply network actor (the agent). Inspired by agency theory, this research associates BC system design choices with levels of system trust (trust in the technology) that are consistent with the risk level of ex-post opportunism. Compared to previous studies, a new studying perspective regarding the concept of 'BC trust' arises. Starting from technology–organization–environment (TOE) theory, this paper also offers an interpretation of how TOE factors intervene in the adoption of different BC systems by agents. By distinguishing between different BC systems, it offers a diverse perspective in grounding TOE in BC research. Together with relevant future research directions, these findings provide adopters and policymakers with important practical insights.

1 | Introduction

A series of scandals, frauds, and contamination incidents in the food sector—for example, the United States' *Escherichia coli* outbreaks, the European Union's (EU) horsemeat scandal, and China's pork mislabeling debacle—have caused serious impacts on public health, which raised concerns regarding food safety and quality (Astill et al. 2019; Chen et al. 2021). Despite the increasingly stringent standards and norms established by companies and governments (e.g., Good Manufacturing Practice, Hazard Analysis and Critical Control Point standards, EU directives), about 420,000 people worldwide die every year due to contaminated food (World Health Organization 2024). These incidents have received considerable attention from academics and practitioners, intensifying the debate on finding adequate solutions to ensure food safety and quality (Thangamayan et al. 2023).

Food supply chains (SCs) are complex, fragmented, and vast ecosystems involving a multitude of actors, from growers to retailers (Stranieri et al. 2021; Cao et al. 2022; Li et al. 2023). Accidents undermining product safety and quality may occur at any stage of the SC—from product cultivation, processing, packaging to distribution, or sale—and can be due to unverified diseases in plants, product contaminations or manipulations, non-compliance with temperature or humidity during storage or transportation, etc. (Kamble et al. 2019; Köhler and Pizzol 2020). In recent decades, the probability of such outbreaks has been increasing due to several factors, such as globalization, growing SC complexity, a large reliance on paper records, and non-integrated information systems, which have exacerbated information asymmetry across the SC (Behnke and Janssen 2020).

Many protection food consortia have been established worldwide to monitor the compliance of pre-established cultivation, production, and distribution rules (Caldarelli et al. 2020). They are generally supported by public funding and associated with legal marks issued by the European Union—such as Protected Designation of Origin (PDO), Protected Geographical Indication (PGI), or Geographical Indication (GI)—or with registered certification marks issued by different US state agencies. Consortia play an institutional role in contrasting illegal practices that can negatively impact the state budget by compromising, on the one hand, the competitiveness of honest companies (and therefore the state revenue through taxes) and, on the other, the public health (and therefore the state expenditure). Consortia associates are typically subject to audits conducted by an external certification authority selected by the consortium that supervises and certifies SC processes. They can also establish contracts with other actors in the SC up to the delivery of products to the final market (e.g., transporters, importers, and large-scale distributors). Associates and supply network members act as agents of the consortium in guaranteeing compliance with pre-established SC practices and rules. However, their actions may sometimes depart from what is agreed upon (*ex-post opportunism*) (Zu and Kaynak 2012), as the two parties can have divergent interests, and the actions of the agents are not easy to verify. According to the agency theory (AT) perspective, it can be argued that an agency problem can arise between the consortium (i.e., the *principal* who delegates certain tasks) and its associates or the other supply network members (i.e., the *agents* who are delegated).

Several researchers identify in blockchain (BC) a technology whose ability to trace activities and increase visibility over various SC processes offers to principals unprecedented possibilities to effectively monitor the agents' behavior and limit ex-post opportunism (Gligor et al. 2022; Xu et al. 2021). For this reason, previous studies have encouraged grounding BC research on AT (Cole et al. 2019; Schmidt and Wagner 2019; Zhu et al. 2022). At its most basic level, BC can be seen as a digital, distributed, and decentralized data structure composed of "blocks" that contain transactions added in chronological order with the goal of creating permanent and tamperproof records (Treiblmaier 2018). Its combination of unique intrinsic characteristics—such as a cryptographic system to ensure data immutability, the use of a consensus mechanism to validate transactions, and a distributed ledger system to make SC transactions accessible to authorized actors—helps preserve data security while enhancing transparency (Schmidt and Wagner 2019; Dutta et al. 2020; Falcone et al. 2021; Richey and Davis-Sramek 2021; Xu et al. 2021; Budler et al. 2024). Given its characteristics and functioning, BC is seen as a trust generator (a 'trust machine'), which can substitute trust between actors with trust in the technology (Falcone et al. 2021; Xu et al. 2021) by reducing information asymmetry and thus ex-post opportunism.

In the food sector, BC is expected to play a crucial role in the next years in guaranteeing product quality and safety and although BC adoption is not yet mandatory, some countries and jurisdictions may decide to mandate the use of BC for food traceability, given the increased risks related to food safety and the globalization of SCs (Bradshaw 2023; Duong 2024). Thus, a growing, yet limited, number of consortia are launching BC projects—such as the Spanish cooperative Conde de Benalúa (Cao et al. 2022), the consortium of Parmigiano Reggiano PDO in Italy (Agnihotri and Bhattacharya 2025), and the Grass Roots Farmers Cooperative in San Francisco (Kamilaris et al. 2019).

On-field BC pilot projects, not only in the food sector, are numerous and exhibit considerable variability in terms of BC configurations (e.g., Galvez et al. 2018; Kamilaris et al. 2019; Dutta et al. 2020; Danese et al. 2021; Köhler and Pizzol 2020; Bai and Sarkis 2022; Zhu et al. 2022). They differ not only for the technical characteristics of the BC technology (e.g., the type of permission model) but also for complementary technologies supporting BC data reading, writing, and analysis—such as internet of things (IoT), near field communication (NFC), or artificial intelligence (AI)—and for organizational tools supporting BC functioning (e.g., the involvement of auditors). For this reason, in the following, we will refer to *BC systems* (i.e., the BC technology plus the complementary technologies and organizational tools supporting BC data reading, writing, and analysis) and *BC system design choices* (e.g., using an NFC tag rather than a QR code to allow access to data stored in BC). The *BC system configuration* is the result of a certain combination of BC system design choices. The *BC system trust* is the trust generated by the whole BC system.

Previous literature in the fields of supply chain management (SCM) (van Hoek 2019; Danese et al. 2021) and Information Management (Kamble et al. 2019; Bumblauskas et al. 2020) has discussed the pros and cons of BC system design choices. Yet, there are no empirical studies that compare different BC system configurations in relation to the *context* where they are implemented. For example, the well-known BC system implemented by Walmart is built on the Hyperledger Fabric permissioned BC, characterized by a data entry that is both manual and IoT-supported, and does not make use of third-party certification bodies (TPCBs) or digital tokens (Leong et al. 2019). Danese et al. (2021) analyze five pilot projects of wine companies using BC to prevent counterfeiting. While all the companies adopt public permissioned BCs (Etherum and VeChain Thor), the BC configurations differ in terms of data entry method, use of TPCBs, and data reading technologies (e.g., QR codes and NFC tags). Why do SC actors design BC systems in different ways across different pilot projects? What is the link between BC system design configurations and the context in which the SC actors are embedded? A fundamental assumption of AT, which inspired the present research, is that monitoring and control mechanisms should be designed in accordance with the potential risk of ex-post opportunism to be addressed. Specifically, the greater this risk in each relationship, the more resources must be allocated to monitoring and control (Wathne and Heide 2000). Extending this perspective to BC, it can be inferred that the different BC system configurations should be designed in alignment with the specific context in which they are implemented, contingent upon the levels of ex-post opportunism risk in the supply chain.

In a food SC, the risk of ex-post opportunism differs significantly depending on the SC actor and the tier considered. It can be argued that different BC system configurations are more or less effective in addressing this risk. A food consortium that needs to monitor its SC member agents' behavior must understand which BC system configuration is most appropriate. More generally, there is a need to better comprehend the reasons behind a particular *BC system design configuration* to guide future applications.

This leads to our first research question:

RQ1: Which BC system design configurations are appropriate for addressing the different levels of ex-post opportunism of supply chain members?

Contextual factors also influence technology adoption. Previous BC studies have identified the contextual factors that drive and enable companies to adopt the BC technology (Clohessy et al. 2019; Orji et al. 2020; Falcone et al. 2021; Sternberg et al. 2021). Treiblmaier and Rejeb (2023) advocate for a shift in investigative perspective, directing attention away from the *general* contextual factors affecting BC adoption to focus on the perceptions of SC member agents regarding *specific* BC systems and their inclination to adapt the design to the *specific* context in which they operate. In the context of a food consortium, it is crucial from a principal's viewpoint that its agents are predisposed to adopt the proposed BC system throughout the SC. However, various factors, including knowledge of BC technology, the financial and process change investments required, and the regulatory environment, can significantly impact the willingness of SC actors to adopt. An exploration of the perceptions of different SC member agents towards various configurations of BC systems can elucidate the circumstances under which and the manner in which BC system design needs to be tailored to both adopters and the context in which they are embedded to promote adoption. Addressing these issues is critical, as the majority of existing BC-based applications remain small-scale (Dutta et al. 2020; Cao et al. 2022) and a deeper understanding of SC member agents' perceptions of different BC systems could be instrumental in enhancing the spread of BC adoption. In a recent research note, Lumineau et al. (2025) endorse this view and encourage scholars to move from the question of whether the use of BC provides distinct advantages to SC members to an exploration of the conditions under which BC confers such advantages.

This leads to our second research question:

RQ2: What contextual factors influence the use of different BC systems by supply chain member agents?

This research is guided by a priori theoretical considerations based on AT and technology–organization–environment (TOE) theory (Tornatzky and Fleischer 1990), which have been previously used to interpret BC adoption and implementation (Zhu et al. 2022). These general theories are applied to approach the empirical context to address RQ1 and RQ2 (Ketokivi and Choi 2014). AT guided the analysis of the appropriateness of different BC systems to address the agency problem, depending on the risk level of agents' ex-post opportunism. TOE theory was adopted to investigate the contextual factors that can influence agents' BC use.

This study analyzed multiple units of analysis, that is, different principal–agent dyads, within one case study of BC implementation in a food SC, considering the consortium as the principal who needs to monitor potential SC member agents' opportunistic conduct and the companies in the supply network as its agents.

The core contribution of this research is a model that guides researchers and practitioners towards understanding (a) the consistency between BC system design choices and the level of ex-post opportunism of SC members to be addressed and (b) the relevant contextual factors that can affect the final BC system use by SC members. Overall, this study provides relevant and original implications for research and practice. This research offers a novel study perspective about the topic of 'BC and trust' by extending the concept of trust at the BC *system level* and analyzing the *fit* between some important BC system design choices and the level of ex-post opportunism to be addressed. Thanks to its systemic perspective, this study originally discusses the integration of the BC technology with other agents' monitoring mechanisms, opening new and compelling directions for future research. Regarding BC adoption, compared to previous BC studies, this research concludes that it is not a question of 'yes or no', and identifies those TOE factors that jointly determine the adoption of different BC systems by SC members. This analysis allows a better reflection of reality, in which BC design is adapted to agents to favor its adoption. Overall, this research contributes to the debate on potential implications of BC adoption and future scenarios in fruit and vegetable SCs.

The rest of the paper is organized as follows. In the next section, literature on BC in food SCs is reviewed with a focus on the different possible choices in designing a BC system. Then, AT and TOE theory are introduced by discussing their basic assumptions and how they are used in this research, BC studies grounded on AT, BC studies using the TOE framework, and barriers to BC adoption, both in general and specifically in food SCs. The research methodology is then described, followed by within- and cross-case analyses. Subsequently, the discussion section reports the model proposed in this research to address RQ1 and RQ2, together with the theoretical and practical implications. The research limitations and future research are discussed in the final section.

2 | Literature Review and Theoretical Background

2.1 | BC in Food Supply Chains to Address Quality and Safety Issues

Many BC studies in the field of operations and SCM focus on the food sector (Dutta et al. 2020; Li et al. 2023), and among the actual BC applications in this industry, most are in the food safety and quality areas (Kamilaris et al. 2019). Previous works (Rogerson and Parry 2020; Gligor et al. 2022; Mangla et al. 2021) and case studies in food SCs (Table 1) show how BC reduces information asymmetry, and thus the risk of ex-post opportunism undermining food quality and safety, by

TABLE 1 | BC cases in the food sector.

Case	BC platform	BC use	Network involved
Bumble Bee Foods	SAP	Traceability of yellowfin tuna from the Indonesian ocean to the stores.	Bumble Bee Foods is a food producer. The BC is designed to involve: fishers, packagers, transporters, distributors and retailers in Bumble Bee Foods tuna supply chain.
Cargill (RWA chicken products)	CAFA platform and VeChain	Traceability of product origin and production of chicken food. Data registered regards: hatchery, farm, production and environment data, poultry not treated with antibiotics, etc.	Cargill is a global food company. The BC project involves its chicken supply chain in Chuzhou (China), Sun Valley's flagship stores on Tmall and JD.COM.
Conde de Benalua	IBM	Traceability of cultivation and olive oil production processes. Data registered regards: the groves where the olives were grown, mills where they were processed into oil, etc.	Conde de Benalua is a cooperative in Spain made up of more than 2000 farmers, and producers of olive oils. The BC project involves its associates.
Grass Roots Farmer Cooperative	Provenance	Traceability of meat to certify the source of food (where the meat came from and how the animals were raised).	Grass Roots Farmer Cooperative is a consortium of Arkansas livestock small farmers in San Francisco. The BC project involves its associates.
Nestlè	IBM	Traceability of Mousline *purée* from Nestlé factory in the north of France to Carrefour stores. Data registered regards: production date, quality control parameters, storage times and location of warehouses, information on suppliers of potatoes.	The BC project involves Nestlé production factory in France and Carrefour stores.
Parmigiano Reggiano Consortium (early stage project)	—	Traceability of product origin through an innovative microchip. Data registered regards: cheese producers, date of production, ripening conditions, etc.	The BC project (which is at a design and testing phase) is designed to involve producers of parmesan cheese, which are associates of the consortium.
San Daniele ham (early stage project)	—	Traceability of products from the birth of piglet, up to breeding, slaughter, seasoning.	The BC project (which is at a design and testing phase) is designed to involve producers, which are associates of San Daniele consortium.
Tyson	IBM	Traceability of meat supply chain from farms to Tyson production facilities.	The BC project involves Tyson production facilities and its farmers.
Unilever	SAP	Traceability of palm oil chain production to assure the respect of planet.	The BC involves Unilever's global palm oil supply chain.
Walmart (leafy green)	IBM	Traceability of the production of each bag of leafy green.	Walmart and farms supplying fresh, leafy greens to Walmart's stores.

providing stakeholders with reliable data/information on product provenance/authenticity and SC activities. In food SCs, large, well-known retailers, consortia, and processors of agricultural products have launched promising pilot projects (Table 1). They focus on the transparency of SC processes. For example, Cargill traces the production of chicken food, and the Grass Roots Farmer Cooperative traces the origin of meat. Bumble Bee Foods's or Nestlè's BCs are designed to trace the complete product journey from upstream to downstream. Gligor et al. (2022) employ the resource orchestration theory to elucidate how SC transparency can be attained through the structuring, bundling, and leveraging of processes. They conduct an analysis of a case study involving a small roaster and producer of distinctive blends of coffee beans sourced from remote regions of the world. This company has achieved SC transparency enabled by BC, allowing end customers to scan a QR code to verify traceability and provenance. The objective is to showcase the artisanal craftsmanship involved in the coffee production process and the authenticity of the materials utilized. The study advances theory on SC transparency that is enabled by BC traceability capability.

In the food industry, institutions, governments, and consortia see in BC a tangible opportunity to realize various benefits associated with the certification of food provenance and SC transparency. For example, in Italy, the government finances BC projects as a strategy to enhance the reputation of Made-in-Italy products through certified product quality (ISMEA 2023; Agenzia ICE 2024). As pointed out by Ahmed et al. (2022), supporting compliance with standards and regulations constitutes a potential application area for BC, with the added prospect of developing a cross-country regulatory framework for future advancements in certifications.

2.1.1 | Differences in BC Systems in Food SCs

Table 2 provides an overview of the different possible choices for designing a BC system mentioned in the literature on food SCs.

Hyperledger Sawtooth (for both permissioned and permissionless BC networks) facilitates traceability of the seafood SC and uses sensory equipment to record information about fish location and storing conditions (Kamilaris et al. 2019). By contrast, the Beefledger project is based on the Ethereum public BC and makes use of digital tokens, whereas Provenance leverages TPCBs to increase BC data reliability but does not rely on IoT sensors. Thus, in addition to BC technical differences, BC systems can differ for complementing technologies. Compared to traditional traceability measures, data in BC is immutable, shared, and validated, and, as such, data reliability is considered higher (Lumineau et al. 2021; Xu et al. 2021; Tiwari et al. 2023). Yet, the veracity of input data is still a challenge (Babich and Hilary 2020; Chod et al. 2020; Dutta et al. 2020; Sternberg et al. 2021). To assure the accuracy of the information before uploading in BC, this should be combined with other advanced complementing technologies, such as IoT, RFID, or sensors, to automatically upload real-time data without human intervention (Cao et al. 2022). In particular, Torky and Hassanein (2020) discuss the importance of integrating IoT and BC and analyze the challenges of adopting IoT in precision agriculture. As an example, ZetoChain performs environmental monitoring at every link of the cold chain, based on IoT devices (Kamilaris et al. 2019).

BC can also be integrated with smart contracts, which are used in the food sector to assure product quality and safety and to reduce the counterparty risk. Keskin et al. (2023) analyze the case of smart contracts enabling automated trade, as long as the food supplied is sufficiently fresh, and examine the value of such smart contracts for a retailer.

Danese et al. (2021) emphasize the importance of the organizational dimension in designing BC systems. In this regard, a critical and debated issue concerns the use of TPCBs combined with BC. BC eliminates the need for a central entity by validating and storing transactions through distributed consensus (Dutta et al. 2020; Zhao et al. 2022). However, current regulations require that food consortia coordinate mandatory audits conducted by an external certification authority to certify SC processes. In some BC pilots in the food sector, TPCBs are used to certify data reliability before uploading in BC, as in the Provenance case study (Leong et al. 2019) or in the wine industry (Danese et al. 2021). In addition to this, a challenge in BC implementation in food SCs is that the so-called hardware *oracles* (e.g., IoTs) are not always appropriate to measure all the needed parameters, which are sometimes difficult to assess and audit (Kamilaris et al. 2019).

2.2 | Grounding BC Research in the Agency Theory

AT is one of the central theories in the literature on management and economics dealing with problems that arise when an entity, the principal, delegates another entity, the agent, to perform certain tasks on its behalf (Eisenhardt 1989). Ex post opportunism arises when the agent hides its real actions that diverge from the expected conduct. This is aggravated by information asymmetry, that is, when the principal has no information to verify whether the agent has properly performed its task, which also depends on the nature of the task and the degree of measurability of its outcomes (Zu and Kaynak 2012; Ellram and Tate 2021). AT has been broadly used across different disciplines, including in the operations and SCM field, to analyze dyadic relationships between buyers and suppliers, investors and managers, and managers and employees where conflicts may occur (Fayezi et al. 2012). The aim of these studies was to suggest appropriate mechanisms to reduce the likelihood of agents' ex post opportunism.

In a dyadic relationship between a principal and an agent, BC represents a promising behavior-based monitoring mechanism that allows the principal to effectively detect and deter any agent's' self-serving conduct by reducing information asymmetry and, in turn, the risk of ex-post opportunism (Stranieri et al. 2021; Sterberg et al. 2021; Zhu et al. 2022). For this reason, many studies (e.g., Kshetri 2018; Treiblmaier 2018; Cole et al. 2019) have called for the use of AT as a theoretical lens to study BC. A recent review of the literature on BC by Zhu et al. (2022) reveals that AT is one of the theories most used in BC studies to interpret its adoption.

AT assumes that the effectiveness of an agent's behavior monitoring tool depends on its ability to reduce information asymmetry (Whipple and Roh 2010). Previous works show how BC reduces information asymmetry by enhancing traceability regarding the history of products and visibility about SC activities (Morgan et al. 2018; Fosso Wamba et al. 2020; Hastig and Sodhi 2020; Rao et al. 2021; Xu et al. 2021). According to Xu et al. (2021), the same BC features that ensure better data integrity (i.e., data quality), data availability, and confidentiality also foster traceability and visibility, which are both closely related to transparency. Similarly, Stranieri et al. (2021) assess the positive impact of the BC in food SCs in terms of improved transparency—e.g., through better data accuracy, accessibility/availability, and real-time information updating. Many studies in the food sector (Antonucci et al. 2019; Rogerson and Parry 2020; Gligor et al. 2022; Mangla et al. 2021; Ahmed et al. 2022; Treiblmaier

TABLE 2 | Blockchain systems.

Configuration choice	Definition	Options
Permission model	Property of BC systems that determines who can become a node of the BC, thus can read, write, and verify information saved on the ledger. It determines the degree of information immutability (Chang et al. 2019; Dutta et al. 2020; Pandey et al. 2022)	• Public: (e.g., Bitcoin) Purely peer-to-peer, decentralized and permissioned. It allows anyone to join the network without authorization, read/write transactions and participate in the consensus process. It provides high guarantees of data immutability. • Private: (e.g., Hyperledger Fabric) Permissioned and controlled by a central authority. It allows only a limited number of pre-authorized nodes to join the network, read/write transactions and participate in the consensus process. It provides lower guarantees of data immutability compared to public ones. • Hybrid: Make use of both public and private BCs. Public BC is used for data that requires a high immutability level, while private BC is generally used for sensitive data.
Data entry	A way by which data is collected and entered on BC (Creydt and Fischer 2019; Kamble et al. 2019; van Hoek 2019; Bumblauskas et al. 2020; Torky and Hassanein 2020).	• Human: Data is collected, handled, and entered manually on BC by human operators by using a frontend interface that is installed on their digital devices. It can lead to poor, incorrect, or incomplete information, as well as delays. • Internet of Things: Data is collected, handled, and uploaded to BC by IoT devices (e.g., sensors, scanners, cameras) without any kind of human interaction, lowering the risk of poor, incorrect, or incomplete information as well as time delays.
Consensus mechanisms	The consensus method that is used to approve the contents of a ledger (Kamilaris et al. 2019; Pandey et al. 2022).	• Type of consensus mechanisms, such as proof of work, proof of stack, proof of activity, etc.
Data veracity control measures	Controls and methods aimed at reducing the risk that the data saved on the BC has been subject to unintentional errors or intentional manipulations (Galvez et al. 2018; Kamble et al. 2019; Kamilaris et al. 2019; Kshetri 2018; Creydt and Fischer 2019; Leong et al. 2019; Schmidt and Wagner 2019; van Hoek 2019; Bumblauskas et al. 2020; Danese et al. 2021).	• No control: No data veracity control measure is used. • Artificial intelligence: Algorithms designed to analyze data saved on BC, searching for potential mismatches that may indicate that reality has been altered. • Third-party certification bodies (TPCBs): Independent, neutral actors that conduct on-field audits to certify the trustworthiness of the data collected and saved on BC.
Data-entry frequency	Parameter that specifies how often the collected data is entered into BC (Danese et al. 2021).	• Real-time: Collected data is uploaded to BC in real-time. It allows for supporting real-time decision-making. • Periodical: Collected data is first grouped and then uploaded on BC after a time interval that can vary based on the user's requirements.
Smart labels	Flat physical identifiers affixed to real-life objects that link them with the related digital information saved on BC (Leong et al. 2019; Danese et al. 2021).	• Common tagging techniques (e.g., barcodes, serial numbers, QR codes): Printed codes that can be easily read with the camera of a mobile device that automatically redirects to the product information. They are vulnerable to cloning. • More sophisticated tagging techniques (e.g., RFID, NFC with data encryption): Microchips embedded in stickers or wristbands that store a reference to the product information and are generally read using a dedicated application installed on a mobile device. They can use specific security mechanisms that prevent their cloning.

(Continues)

TABLE 2 | (Continued)

Configuration choice	Definition	Options
Customer communication channels	Types of channels adopted to enable final users to access the product-related information (Creydt and Fischer 2019; Leong et al. 2019; Danese et al. 2021).	• Website: Collection of static web pages that can be accessed using a desktop or mobile web browser. • Mobile application: A software application that is downloaded and installed on users' mobile devices.
Proportion of accessible data that is saved on-chain	Proportion of the data accessible by consumers (through a web page or a mobile application) that is immutably saved on-chain (Leong et al. 2019; Danese et al. 2021).	• From 0% to 100%: The portion of the information presented to consumers that is also saved on-chain is generally variable. The higher its value, the higher the guarantee that data has not been subject to manipulations.
Smart contracts	Computer software that executes pre-defined actions (e.g., alerts) when certain conditions are met (Kim and Laskowski 2018; Keskin et al. 2023).	• No: Smart contracts are not used. • Yes: Smart contracts are used to monitor environmental conditions (e.g., temperature, humidity, light exposure, sudden fall) and automatically signal when any violation occurs.
Tokens	Digital representation of real-world assets (e.g., raw materials, semi-finished or finished products) on BC (Leong et al. 2019; Caldarelli et al. 2020).	• No: Tokens are not used. • Fungible (ERC20): Tokens that cannot be distinguished. They represent interchangeable goods, such as crude oil, wine, or currency. • Non-fungible (ERC721): Tokens that can be distinguished. They represent non-interchangeable goods, such as different cars.
Traceable resource unit	Object of traceability (Kim and Laskowski 2018; Kamilaris et al. 2019; Leong et al. 2019; Bumblauskas et al. 2020).	• Single product: Trade unit. • Multiple product: Unit that comprehends multiple products. It can be a logistic unit (e.g., pallet or container) or a production unit (e.g., a production batch).

and Rejeb 2023) discuss the value of BC for improving SC visibility and traceability.

Thanks to this, BC engenders *trust*, as the actors are confident that the SC members consistently execute the expected actions and report accurate information (Falcone et al. 2021; Xu et al. 2021). The concept of BC as a 'trust machine' in the BC literature is widely discussed (Durach et al. 2021; Falcone et al. 2021; Xu et al. 2021), and a general claim is that BC substitutes trust between individuals with trust in the technology. Yet, this concept is not straightforward, and the debate is open. On the one hand, BC reduces information asymmetry thanks to better data quality, availability, immutability, or confidentiality, but, on the other hand, BC cannot guarantee that correct data are entered into the ledger or are updated (Kurpjuweit et al. 2021; Sternberg et al. 2021). Thus, BC would need trust between actors, but an SC of trusted actors does not need BC, which is a paradox (Sternberg et al. 2021). This perspective suggests, when studying BC trust and the issue of information asymmetry, the need to take into account the whole BC system and all its configuration choices (e.g., technologies supporting BC data input). For this reason, we will use the term 'BC system trust' to refer to the trust generated by the whole BC system, that, in line with the AT, is determined by the BC system's overall capability to reduce information asymmetry (Whipple and Roh 2010).

Current BC research lacks studies that compare the different BC systems in terms of trust, considering not only the characteristics of the BC technology itself, but also the complementary technologies and organizational tools supporting BC, and that link the different BC systems to the *context* in which they are implemented.

2.3 | TOE Framework and Barriers to BC Adoption

According to TOE theory, the propensity of a firm to implement new technologies is influenced by three different aspects: its technological, organizational, and environmental contexts (Tornatzky and Fleischer 1990). The first includes the characteristics of the innovation under consideration, the adopter's perception of its attributes, and the technological tools already used. The organizational context concerns the adopter's characteristics and internal resources. The environmental context refers to the environment in which the adopter operates (e.g., regulatory, governmental, industrial).

Some scholars have used TOE as a theoretical foundation to analyze incentives or constraints to BC adoption (e.g., Clohessy and Acton 2019; Kouhizadeh et al. 2020; Orji et al. 2020; Kurpjuweit et al. 2021). This investigation is of pivotal importance considering the lower-than-expected BC adoption rates in many sectors (Kouhizadeh et al. 2020; Durach et al. 2021). Although the terminology the authors used and the level of detail vary, by comparing prior BC studies using TOE and those outlining significant TOE factors, Table 3 summarizes the most cited factors for each category of the TOE framework.

TABLE 3 | Blockchain TOE adoption factors.

Dimensions	Factors	References
Technological	Technology complexity	Clohessy and Acton (2019), Clohessy et al. (2019), Kamilaris et al. (2019), Köhler and Pizzol (2020), Lansiti and Lakhani (2017), Morabito (2017), Pandey et al. (2022), Pilkington (2016), Woodside et al. (2017), Vu et al. (2021), Zamani and Giaglis (2018).
	Relative advantage	Chen et al. (2021), Clohessy and Acton (2019), Crosby et al. (2016), Kamilaris et al. (2019), Lansiti and Lakhani (2017), Morabito (2017), Pilkington (2016), Sternberg et al. (2021), Tapscott and Tapscott (2016), Vu et al. (2021), Woodside et al. (2017), Zamani and Giaglis (2018).
	Compatibility with existing technology	Clohessy and Acton (2019), Chen et al. (2021), Kamilaris et al. (2019), Köhler and Pizzol (2020), Lansiti and Lakhani (2017), Morabito (2017), Pandey et al. (2022), Pilkington (2016), Vu et al. (2021), Woodside et al. (2017).
	Technology maturity	Biswas and Gupta (2019), Chen et al. (2021), Clohessy and Acton (2019), Dutta et al. (2020), Kamble et al. (2019), Kamilaris et al. (2019), Kurpjuweit et al. (2021), Lansiti and Lakhani (2017), Morabito (2017), Orij et al. (2020), Pilkington (2016), Tapscott and Tapscott (2016).
Organizational	Organizational size	Clohessy and Acton (2019), Clohessy et al. (2019), Crosby et al. (2016), Lansiti and Lakhani (2017), Morabito (2017), Pilkington (2016), Tapscott and Tapscott (2016), Zamani and Giaglis (2018).
	Top management support	Clohessy et al. (2019), Clohessy and Acton (2019), Crosby et al. (2016), Lansiti and Lakhani (2017), Morabito (2017), Pilkington (2016), Zamani and Giaglis (2018).
	Organizational readiness	Clohessy and Acton (2019), Clohessy et al. (2019), Crosby et al. (2016), Morabito (2017), Sternberg et al. (2021), Tapscott and Tapscott (2016), Zamani and Giaglis (2018).
Environmental	Governmental incentives	Biswas and Gupta (2019), Clohessy and Acton (2019), Crosby et al. (2016), Morabito (2017), Kamble et al. (2019), Saberi et al. (2019), Sternberg et al. (2021), Tapscott and Tapscott (2016).
	Regulatory environment	Chen et al. (2021), Clohessy and Acton (2019), Clohessy et al. (2019), Crosby et al. (2016), Dutta et al. (2020), Kamilaris et al. (2019), Köhler and Pizzol (2020), Kurpjuweit et al. (2021), Lansiti and Lakhani (2017), Morabito (2017), Orjі et al. (2020), Pandey et al. (2022), Tapscott and Tapscott (2016), Vu et al. (2021), Woodside et al. (2017), Zamani and Giaglis (2018).
	Industry pressure	Clohessy and Acton (2019), Clohessy et al. (2019), Crosby et al. (2016), Lansiti and Lakhani (2017), Pilkington (2016), Stenberg et al. (2021).

Some studies (Kamilaris et al. 2019; Köhler and Pizzol 2020; Vu et al. 2021; Pandey et al. 2022) focused on BC adoption in food SCs and related barriers. A big challenge mentioned is technology accessibility, which is exacerbated by the increasingly complex digital technology linked to BC (e.g., sophisticated sensors), the information infrastructure needed, and a general lack of skills in BC, also due to the small size of farmers as well as the immaturity of BC technology (Kamilaris et al. 2019). Consequently, SC actors often perceive BC technology complexity as a major barrier. A further obstacle cited is the uncertainty surrounding BC sustainability and its long-term impact (Kamilaris et al. 2019; Vu et al. 2021). It is difficult to evaluate the relative advantage of its adoption, given the high implementation costs and efforts BC entails, and without a clear understanding of its actual need (Vu et al. 2021). The lack of regulations/standards and technical limits (scalability, interoperability/fragmentation, and privacy issues) are also discussed in BC papers in the food sector (Kamilaris et al. 2019; Köhler and Pizzol 2020; Vu et al. 2021; Pandey et al. 2022), as well as in other industries (Babich and Hilary 2020; Dutta et al. 2020; Orji et al. 2020; Balci and Surucu-Balci 2021; Kurpjuweit et al. 2021), revealing the scarce level of BC technology maturity.

We can find similar findings in the framework developed by Chen et al. (2021). By reviewing literature on BC in food SCs, they apply TOE to investigate barriers to BC adoption. They classify them into five major challenges: (a) the complexity of integrating data, systems, and users (e.g., due to different BC platforms or multiple types of data); (b) the immature implementation of BC, which leads to low familiarity, a labor and skill shortage, and low users' acceptance; (c) BC technology characteristics (e.g., scalability, privacy, transaction capability); (d) high investments in BC systems; (e) the absence of regulation and standards. Kurpjuweit et al. (2021) apply TOE to investigate BC adoption in additive manufacturing and, although the context is different, some recurring results can be found. For instance, they identify developing and integrating a compatible BC solution as the greatest technological barrier in terms of BC integration in the existing information structure, BC-related technologies (e.g., sensors), interoperability, and lack of standards between different BCs. Among the most relevant organizational barriers, they also mention the high implementation costs, and linked to this, the lack of top management support. Again, one of the most relevant environmental barriers is the absence of a common regulation, as regulatory conditions depend on national legislation.

These studies offer a rich overview of the numerous reasons that can deter companies from adopting BC. Yet, within this stream, some significant research directions are proposed to advance knowledge further. A major research gap regards the paucity of studies that differentiate between different BC systems when studying the link between BC adoption and contextual/TOE factors, although many works suggest that this is fundamental. For instance, different BC-complementing technologies (e.g., IoTs) can determine different levels of technology complexity perceived by potential adopters, which can influence adoption decision (Chen et al. 2021; Kurpjuweit et al. 2021). Other studies (Falcone et al. 2021; Xu et al. 2021) posit that exposure to different technological design features can affect the willingness to adopt and use a new technology and analyze how some specific BC features influence managers' perceptions and willingness to adopt. Sternberg et al. (2021) develop a model for BC adoption, based on tensions between drivers in favor of and against BC, for example between the perceived benefits (e.g., enhanced product traceability) and additional data input costs for infrastructural and workload investments; or between the use of BC as a 'trust machine' and the need to rely on trusted partners for data input. It is evident that different BC systems can exacerbate or ease these tensions, facilitating or hindering BC adoption. Finally, Treiblmaier and Rejeb (2023) recommend to not treat BC as a black box with assumed properties, but to differentiate between different BC systems when analyzing acceptance and adoption.

This perspective moves attention from the contextual factors influencing the willingness to adopt a BC solution to the need to consider the perceptions of agents towards different BC systems and, when required, adapt a BC system design to the adopters' needs and the context in which they are embedded.

3 | Research Methodology

This research is based on a BC project promoted by one of the major Italian consortia of fruit producers and packers. The units of analysis investigated are the principal–agent dyads, where the principal is the consortium that aims to control for any opportunistic conduct that may compromise product quality and safety, and the agents are the diverse companies in the supply network, from food cultivation to distribution and retail. This approach was judged appropriate given the research aim (see RQ1 and 2). Analyzing different dyads within the same supply network while keeping the principal constant provides the necessary variability to examine influencing key variables while avoiding potential confounding effects that might undermine the study's validity (e.g., different principals can use BC for different purposes).

In this research, some general theories (AT and TOE) were identified to approach the empirical context, with an emphasis on abductive reasoning. TOE theory and AT, together with existing literature on BC, provided researchers with a priori theoretical considerations to deduce the various elements that characterize the different BC systems used to control agents' behavior and what contextual variables influence BC systems proposed by the principal and BC used by the agents. Figure 1 summarizes the research process, the main steps of which are detailed below.

3.1 | Case Selection and Sample of Principal–Agent Dyads

A BC implementation case was searched that met the following criteria: shows a certain complexity in terms of the diversity of actors in the supply network involved in BC use and concerning the diversity of BC systems; is relevant for safety and health risk in the food sector; and where the BC system is in use (not at a conceptual stage). Initially, three potential cases were identified at conferences and workshops dedicated to BC and by gathering information from the Internet and newspapers. The first case concerned BC application in the tomato industry, but it was excluded because the only supply network actors involved in the project were farmers and packers who implemented the same BC system. The second case was in the wine industry and involved a major Italian consortium. However, the involved companies were all fully integrated and again lacked sufficient diversity in the BC systems adopted.

The chosen case, which met the selection criteria, involves an Italian consortium of fruit producers and packers with more than 500 associates. This consortium is responsible for assuring the quality and origin of fruits produced in a specific area of an Italian region (that accounts for more than 50% of national production), which the European Union decided to promote and protect with the PGI label because of the microclimate and soil organoleptic characteristics that determine the fruits' unique quality. Only the consortium associates can benefit from the PGI brand, which is a guarantee of quality for final consumers.

The main role of the consortium is the supervision and protection of the brand from abuse, acts of unfair competition, counterfeiting, improper use of the PGI label, and non-compliance with PGI specifications. Examples of opportunistic behaviors are the use of pesticides or fungicides not permitted by the PGI specifications; the inclusion in the packaging of fruits not coming from the PGI area; packagers or retailers not communicating the real sold quantities; the selling of fruits with anthocyanin levels lower than a threshold limit (product quality assurance); and the failure to comply with temperature and humidity conditions during transportation and storage. To guarantee both consumers and associates (i.e., producers and packers) about the adherence to the PGI specifications, the consortium decided to equip itself with a product traceability system and, in 2019, launched a project to explore the efficacy of BC to monitor actors' conduct along the supply network. This BC project was judged particularly interesting for the present study as it was at a pilot (not conceptual) stage and was designed to involve over time many actors in different supply network tiers (i.e., growers, packers, transporters, importers, customs, large-scale distributors, neighborhood fruit markets, and fruit stores) (Figure 2), which is a fundamental selection criterion in this research. At

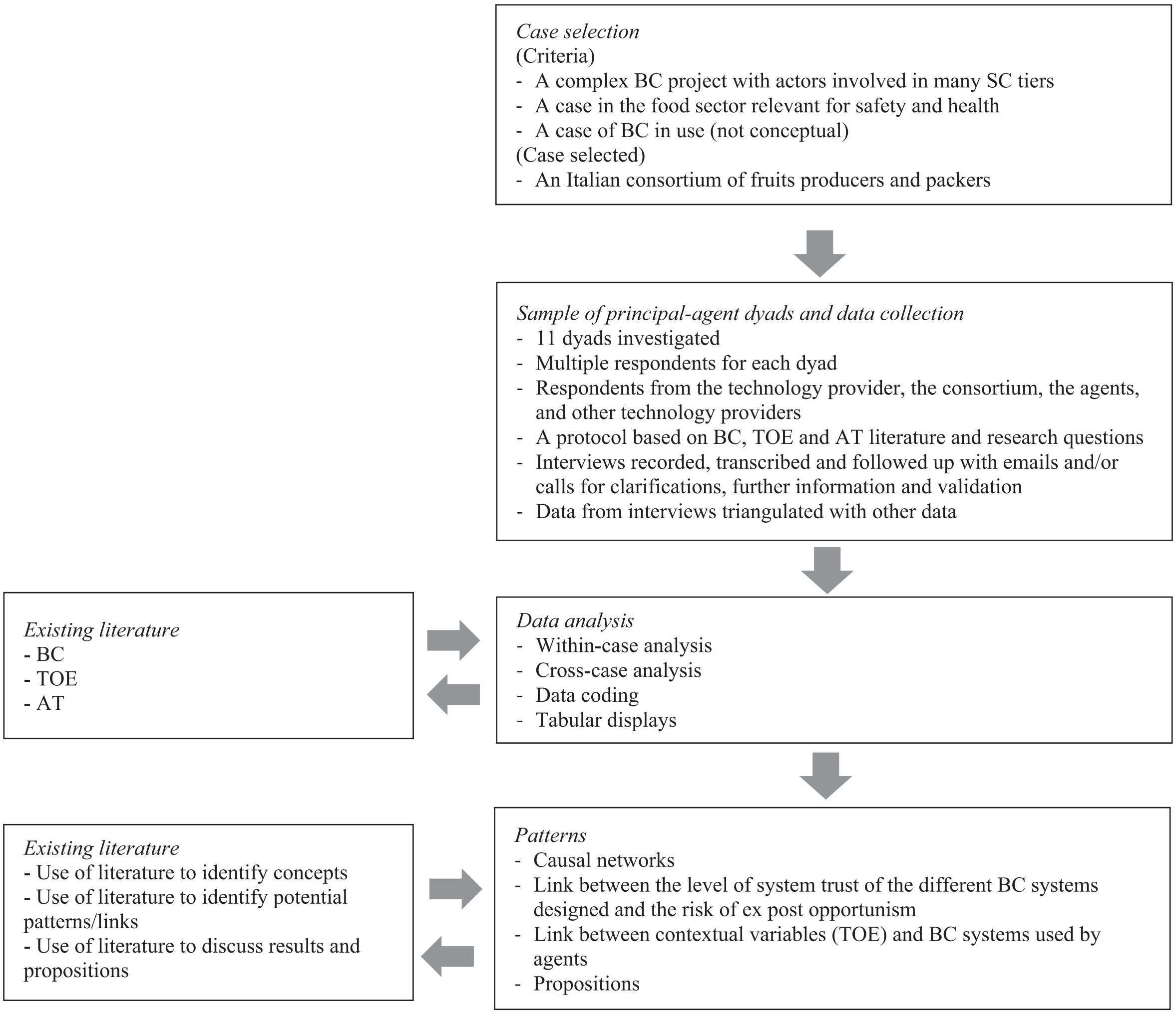


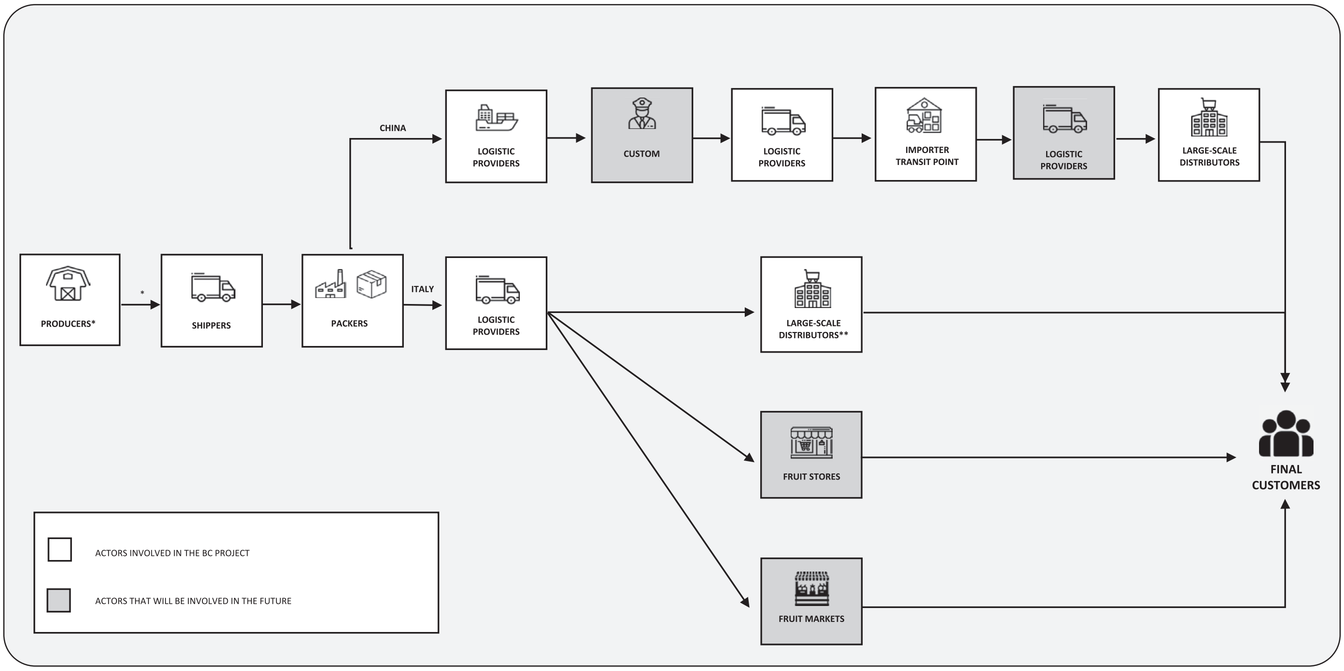
FIGURE 1 | The research process.

the time of this writing, the project includes seven consortium associates (i.e., five producers, two packers), two shippers, two logistics providers, one Italian large retail chain, and one importer, who acted as facilitator in coordinating the BC project in the Chinese part of the distribution/retail network (i.e., including one logistic provider and one large retail chain). Being a BC pilot project, only a portion of the consortium associates was involved; however, the participants covered almost all the supply network tiers, excluding the customs, neighborhood fruit markets, and small family-owned fruit stores, which will be involved in the future. The consortium's monitoring of the activities of these actors is of paramount importance because, in each production and distribution phase, the behavior of a single actor could compromise product safety and quality, jeopardizing the high-quality product image.

After verifying the willingness of the consortium and the BC technological provider (TP) to participate in this research project, an agreement was reached on how to select and contact the potential agents in this study. The aim was to choose principal–agent dyads following literal and theoretical replication, searching for cases presenting similarities and differences along the dimensions of interest, namely, the BC systems (e.g., type of permission model, data entry, etc.) and the context (e.g., agent's supply network tier, size, and nationality) (Yin 2017). The consortium provided researchers with information about the pioneer associates involved in the BC project since its conception (i.e., two producers and one packer). They were contacted and provided with a brief introduction of the team, the study's objectives, and were asked for their willingness to take part in this research. All the pioneers agreed to participate in this study, as well as two shippers, two logistics providers, one importer, and one Italian large-scale distributor. They would remain anonymous and receive the final study report. To include in the analysis dyads across all the supply network tiers, the design and use of BC in the Chinese portion of the supply network was investigated thanks to the involvement of a key informant working for the importer, a consultant who was part of the BC project team since the beginning and acted as a facilitator of BC adoption in the Chinese distribution network. In total, 11 principal–agent dyads were analyzed (Table 4).

3.2 | The BC Project

At the BC project kick-off, the consortium declared the desired benefits: to contrast counterfeiting, to enhance the brand (especially in the Chinese market), to facilitate control activities, to



Notes: BC project evolves fast, and this is the situation at the time of writing, *Producers can sell goods directly to final customers; **Transhipment between the Italian large-scale distributor and the fruit market may occur.

FIGURE 2 | Supply network involved in the BC project. BC project evolves fast, and this is the situation at the time of writing, *Producers can sell goods directly to final customers; **Transhipment between the Italian large-scale distributor and the fruit market may occur.

simplify bureaucracy and reduce paper, to lean processes and speed throughput (very important for perishable food, like fruit), to reduce errors in data entry, to facilitate customs clearance, and to monitor the fruit status and temperature during transportation. The consortium intended to implement a BC-based product traceability system to guarantee the fruit's origin and integrity. The reasons were, on the one hand, to protect consumers from the opportunistic conduct of unfair competitors that use fake PGI labels and, on the other hand, to safeguard consumers, customers, and associates about full compliance with PGI specifications, such as harvesting location and date, quality control types and timing, storage, and transportation conditions. Product tracking started in the 2019–20 winter harvesting season with the support of a digital platform based on BC technology created *ad hoc* by the TP, inspired by previous experiences in the wine and olive oil SCs.

By scanning an NFC tag affixed to the fruit crate or net, a mobile application with a BC backend presents users with the most relevant information for their context. All project partners are enabled to upload data to BC using their signatures. This is a differentiating element compared to previous projects in which the TP had been involved, in which it was delegated for data entry. Decentralization was intended to speed up the BC update and make the SC actors more committed to regular and truthful data entry. For on-site audits, the consortium delegates a TPCB, recognized by the Ministry of Agriculture but different from the one that carries out the checks for the Ministry. To comply with the legal provisions, data gathered during such controls is first saved on the Italian national agricultural information systems and then synchronized on the BC. The same applies also for data concerning the localization of each fruit grove in the PGI area, documents related to the Ministerial Certification Body audits, and data related to weather conditions during the fruit growth and harvesting season (monitored by sensors of the regional network of weather stations). The use of data related to product traceability stored in the BC creates the condition for a profound simplification, improvement, and speeding up of control activities because it is no longer necessary to employ dozens of people for paper controls and is instead possible to divert the personnel of the certification bodies to on-site audits. The NFC tag connected to the BC system guarantees, on the one hand, the certain provenience of the data, based on information coming from companies linked to the consortium or the public administration, and, on the other hand, the correct link with the certified and immutable history of the product (e.g., origin, controls, transactional data along the different actors of the supply chain). The BC stores both data visible to the consumer and data encrypted with appropriate keys, which are made accessible only to some actors (e.g., consortium, certification bodies, project partners). Each actor can decide which data to make public (unencrypted). Based on the level of confidentiality, data is stored on the Ethereum public BC or the private Enterprise Ethereum BC, which grants different levels of accessibility to SC actors. This hybrid BC solution is also open, as it can always be integrated by new partners who can join without changing their BC platform. This feature was designed with the aim of extending the system to foreign importers and distributors.

TABLE 4 | Overview of the cases.

Case	Members of the dyad	Agents		
		No. of full-time employees	Location	Relationship with the consortium
A	Fruit consortium, Company A (fruit producer)	10–15	Italy	Associate of the consortium.
B	Fruit consortium, Company B (fruit producer)	10–15	Italy	Associate of the consortium.
C	Fruit consortium, Company C (shipper)	10–15	Italy	Company C is a local shipper, working for long time for the food consortium.
D	Fruit consortium, Company D (shipper)	10–15	Italy	Company D is a local shipper, working for long time for the food consortium.
E	Fruit consortium, Company E (packer)	25–49	Italy	Associate of the consortium.
F	Fruit consortium, Company F (logistic provider)	150–200	Italy	Company F manages national shipments in Italy by trucks. It maintains a long-time relationship with the consortium.
G	Fruit consortium, Company G (large-scale distributor)	> 500	Italy	Company G is an Italian supermarket chain, costumer of the consortium for a long time.
H	Fruit consortium, Company H (logistic provider)	250–300	Italy	Company H is the international logistic provider which manages the international transport to China by ship (till the custom). China represents for the consortium a new market.
I	Fruit consortium, Company I (logistic provider)	100–150	China	Company I is a Chinese logistic provider which manages shipments within China. It is in direct contact with the importer J.
J	Fruit consortium, Company J (importer)	50–100	China	Importer J works closely with the consortium to develop the Chinese market and had a primary role in the BC project.
K	Fruit consortium, Company K (large-scale distributor)	> 500	China	Company K is a Chinese supermarket chain. China represents for the consortium a new market. It is in direct contact with the importer J.

3.2.1 | The Context of Distribution Channels

Analyzing the characteristics of the various distribution channels is essential for the present case study. This helps to better understand why neighborhood fruit markets and small family-owned fruit stores were excluded by this BC pilot project and, more generally, to consider the potential implications of BC in the fruit and vegetable trade.

The decision of the food consortium to initially focus the pilot project on the large-scale retailer channel was driven by several reasons. First, this channel is by far the most significant distribution channel for the fruit. Second, due to its characteristics (i.e., high water content), the fruit has a strong export potential, and the only distribution channel outside of Italy is large-scale retailers. Third, although the consortium contemplates this possibility, involving neighborhood fruit markets and small family-owned fruit stores in a BC pilot project is more challenging, as these are typically micro- and small businesses with very limited resources and staff.

The 2024 Italian report by ISTAT—the Italian National Institute of Statistics—indicates that large-scale retailers remain the dominant distribution channel for fruits and vegetables, while small shops and fruit markets are experiencing a decline (ISTAT 2024). These latter channels have lower margins compared to large-scale retailers, as they lack the capacity to achieve cost reductions through bulk purchasing. Their gradual contraction began years ago, driven by broader changes in consumer purchasing habits and consumption patterns (Autorità Garante della Concorrenza e del Mercato [AGCM] 2007). To survive, these businesses have specialized in specific niche segments, focusing on so-called "zero-kilometer" products, which refer to locally sourced items. Neighborhood fruit markets exhibit flexibility in their product offerings, adjusting to the seasonality of local produce and selling products in small quantities. They thrive in fragmented supply contexts, particularly for those products for which large-scale retailers are unable to identify one or a few large producers or consortia from whom to source.

Thus, neighborhood fruit markets and small fruit shops operate under a business model and within an SC, which is very different from those of large-scale retailers.

They rely on very short SCs, as producers are geographically concentrated in a nearby area, whereas large-scale retailers sell food from various sources, including imported items, purchased in large quantities. The SCs of the latter are long and complex, often involving intercontinental shipping. In addition, consumers of neighborhood fruit markets and small shops are well-acquainted with the products they purchase (e.g., their appearance, flavor, etc.), as well as the area where local producers cultivate them. Consequently, the risk of purchasing counterfeited products is minimal in comparison with goods sold by large-scale retailers. Additionally, food is replenished frequently and in small quantities, mitigating concerns related to food spoilage.

Although neighborhood fruit markets and small family-owned fruit stores were not included in the present case study, potential implications of BC and future scenarios on BC adoption are discussed in Section 5 to provide a broader perspective on BC use in the fruit and vegetable SCs.

3.3 | Data Collection

Data collection was conducted in the period between January 2019 and October 2022. The investigation relied on both a real-time collection of information and retrospective reconstructions.

Semi-structured interviews were chosen as the primary data source because they represent a highly efficient way to gather rich and empirical data (Voss et al. 2002). In total, we collected 27 interviews. A first set of informants was selected from the TP and food consortium. We interviewed three senior managers from the TP (i.e., the BC Solutions Architect, the Head of Blockchain and Distributed Ledger Function, and the Head of the Healthcare, Agriculture & Environment Service). The BC Solutions Architect had a deep knowledge of all technical features of the BC solutions designed and applied in the BC project, as well as of BC technology in general and its application in the food sector. Together with the Head of Blockchain and distributed ledger function, he had been responsible for analyzing the supply network (Figure 2) (e.g., peculiarities, the flow of materials and information/documents, etc.) and organizing appropriate support and training for all actors interested in participating. The Head of the Healthcare, Agriculture & Environment Service was part of the BC project team and was informed about how the BC project evolved over time and its expected impact. We also interviewed the President and the Vice-President of the food consortium. They were experts in the sector and the supply network. They knew very well the characteristics of the associates, transporters, importers, and stores in the network, existing/potential markets, as well as the monitoring mechanisms, standards, and regulations in place. They were also aware of opportunistic behaviors, already occurred in the past or were potential. Together with TP managers, they set the goals and timing of the project, searched for external funding, and monitored it by documenting details, decisions, and any changes that occurred during the BC design and implementation. These informants provided us with useful written material and reports.

A further set of key informants came from the agents in the supply network involved in the BC project (i.e., CEOs, IT managers, or operations managers); in particular, from the fruit producers A and B, shippers C and D, packer E, logistics providers F and H, large-scale distributor G, and the Chinese importer J. They were informed about the BC project (e.g., reasons leading to its adoption, expected results, BC functionalities) and the role of their company in the supply network. They provided us with useful details on their immediate network. Since A–E were small companies, CEOs played operational roles (e.g., as agronomists in the fruit producers) and thus knew very well the operational processes of their company. In addition, we interviewed a consultant working for the importer J as 'import–export specialist'. His knowledge of the Chinese market and regulations, as well as of possible opportunistic behaviors of actors involved in fruit distribution in China, was very useful. In addition, he provided us with information on the large-scale distributor K and the Chinese logistics provider I.

Finally, a further set of key informants comes from four technology providers (not involved in this BC project), experts in BC design and use for food traceability, operating also in sectors different from agri-food. Two were global professional services, one was an Italian start-up, and one was a Swiss software house. Their involvement was fundamental to assessing the technical features of BC systems, their strengths and weaknesses, and thus the level of system trust of BC systems.

The interview with each respondent lasted between 45 and 120 min and was conducted by two researchers who had previously conducted other studies in the BC field to reduce potential observers' bias, enhance convergence of observations, and, therefore, increase confidence in the findings (Yin 2017). For all dyads, multiple perspectives were considered by asking, when appropriate, respondents from the consortium, the TP, and the company acting as agent the same questions. The interviews followed a case research protocol with a common structure (Appendix 1: Table A1), although the set of questions was tailored accordingly to the different interviewees (Yin 2017). The questions for the consortium and the TP focused on general information about the implementation of the BC project in the supply network, the design of the BC system, and specific information on each dyad. The questions for agents focused on the BC implementation, specifically within the dyad. The protocol was developed based on the prior theoretical underpinnings of BC, TOE theory, AT, and our research questions. Interviewees were encouraged to provide any additional information besides the pre-defined questions of the protocol, and valuable data was gained from informal conversations. To improve data reliability and internal validity, each interview was recorded with the express consent of the respondents and subsequently transcribed verbatim. Interviews were followed up with emails and/or calls with the interviewees for clarifications, to gather further information, or to confirm the correctness of our interpretations (Yin 2017).

To cross-check information and complement any missing data, the research team triangulated information/data derived from the interviews, official documentation related to the BC project, and any additional insights from other secondary data sources, such as company websites and press releases. In addition, the researchers learned what documents and information were exchanged through BC and the methods used for BC data input and reading across the supply network. All the gathered data were stored and organized in a case study database for subsequent analyses.

3.4 | Data Analysis

Data analysis was based on abductive reasoning (Ketokivi and Choi 2014). BC literature, TOE theory, and AT provided researchers with an a priori view of possible concepts and links, which were refined as the empirical data analysis progressed. It included a within- and cross-case analysis and was based on three steps: (a) data reduction, (b) data display, and (c) conclusion drawing/verification (Miles and Huberman 1994).

The within-case analysis began by writing up a detailed case narrative for each of the observed dyads. The large amount of raw data collected for each case (interview transcripts, direct observation, documentation, and secondary data) was converted into text files and analyzed, organized, and coded (see a coding example in Data S3). Major themes were first identified based on the research questions (open coding), namely, 'BC systems' and 'contextual factors'. Subthemes emerged by analyzing and comparing data across cases and based on the literature (axial and selective coding). The BC literature helped to identify relevant variables to characterize and differentiate BC systems. AT guided our attention towards the risk of agents' ex-post opportunism and TOE theory towards some factors characterizing the agents. The data for each case was then summarized into tabular displays, including a synthetic case description broken down into the relevant variables and the corresponding rating of each variable (Appendix 2: Tables B1 and B2) (Yin 2017).

Afterwards, cases were compared to isolate patterns or linkages between variables emerging from the data and to detect commonalities and differences (Voss et al. 2002). To this end, causal network analysis was adopted (Miles and Huberman 1994). An initial version of causal networks was produced by focusing on the variables that covaried, that is, seemed to have some kind of causal relationship. Each identified relationship was evaluated by all researchers until consensus was achieved and described through analytic text. Finally, the results of our analyses were discussed with interviewees to corroborate the validity of the relations identified in causal networks (Miles and Huberman 1994). They were summarized in the form of propositions.

4 | Analysis and Results

4.1 | Within-Case Analysis

After data collection, cases were broken down, examined, and compared to identify commonalities and differences in the BC systems designed and proposed by the principal and used by SC actors. The analysis differentiated between the BC system designed and considered the 'ideal' solution by the consortium, given its need for monitoring each specific agent, and the BC system effectively used by the agent, which in some cases differed to facilitate the agent's adoption based on its needs. Each dyad was then characterized based on context, considering both the risk level of an agent's ex-post opportunism, as suggested by AT, and TOE factors considered in the related literature. In line with Zsidisin and Ellram (2003), the risk of the agent's ex-post opportunism was rated as high, medium, or low. The risk matrix used to assess agent's ex-post opportunism considers the likelihood that an opportunistic behavior occurs—depending on absence/presence of monitoring mechanisms that discourage misconduct, outcome measurability, and convenience to cheat (e.g., the damage to brand reputation in case of quality and safety issues)—as well as potential detrimental consequences on product quality and safety (Figure 3). TOE factors refer to the agents' contexts, as the aim was to understand the factors influencing their use of different BC systems (RQ2). Detailed information for each dyad is provided in Tables 5–8.

				Degree of detrimental consequences		
				Based on the nature of the process carried out by the agent and on its potential negative impact on product quality and safety		
				Minor impact on food quality and safety	*Modest impact on food quality and safety*	*Severe impact on food quality and safety*
				Marginal	***Moderate***	***Critical***
Likelihood	Likelihood that the agent acts opportunistically	*Expected to occur at some time*	***Likely***	Medium risk	High risk (C, D)	High risk
		May occur	***Possible***	Low risk	Medium risk	High risk (A, B, F, H, I)
		Difficult to occur	***Unlikely***	Low risk (G, J)	Low risk	Medium risk (E, K)

FIGURE 3 | Risk of ex-post opportunism.

4.2 | Cross-Case Analysis

4.2.1 | Level of System Trust of BC Systems and Risk of Ex-Post Opportunism

BC systems observed in the different dyads were compared and assessed. For each BC system, the researchers identified an overall level of system trust, considering its capability to reduce information asymmetry in terms of data availability, data immutability, data veracity, and responsiveness, which are crucial dimensions in measuring transparency (Stranieri et al. 2021; Xu et al. 2021). Data availability refers to the degree to which stakeholders (e.g., food operators; in our case, the principal) have access to information; data immutability and veracity are fundamental components of data quality/integrity; responsiveness refers to the ability to share real-time information in a synchronized way along the SC. This assessment was based on information provided by the interviewees, mainly from the TPs involved in this BC project, as well as the additional TPs interviewed (not part of this BC project), triangulated with technical information on the functioning of each BC configuration choice.

By comparing the dyads and rating BCs according to their level of system trust, four distinct clusters of BC systems emerged (Table 9).

In some cases (Cluster 1), since the permission model was private, data was manually entered into BC without any use of IoT or inspection by a TPCB, and smart contracts were not used, system trust was assessed at a *minimum* level. Similarly, in Cluster 2, data entry was manual, IoT and smart contracts were not used, and no TPCB was involved. However, the level of system trust was slightly higher (at a *low* level) than in Cluster 1, as the permission model was hybrid, and this suggests that the principal could access information publicly saved on BC by the agent, which assured better data visibility, immutability, and veracity. Cluster 3 differed from the latter, as a TPCB was also involved in verifying data veracity, which offers a higher guarantee of system trust than in Cluster 2 (classified as *medium* level). Finally, in Cluster 4, system trust was considered at a *high* level since (a) the permission model was hybrid; (b) data was collected and uploaded on BC in real-time by IoTs, previously verified and calibrated by a TPCB, and, when this was not possible, they were manually collected and uploaded into BC after being checked by the TPCB; and (c) smart contracts were used to alert SC actors to anomalous situations. Taken together, these characteristics guaranteed a higher data veracity and responsiveness compared to the other BC systems, in addition to a high data visibility and immutability.

These four clusters of BC systems do not represent all possible BC configurations. However, they reflect different levels of system trust, which is the focus of this study. An important point of discussion raised with BC experts, the TPs, and the consortium was whether a BC system based on a private permission model could be helpful as a monitoring tool for the consortium, which had no visibility on data registered in the private BC. On the one hand, the fact that a portion of the supply network used a BC to register data represented a guarantee for the consortium that a control measure of downstream actors' activities was in place. On the other hand, the fact that data was not shared limited the possibility of monitoring, and thus the level of system trust was assessed at a minimum level. In fact, a private permission model reduces not only data visibility but also data immutability and veracity. The TP was studying possible solutions that would allow connecting heterogeneous BC systems so that data could be shared upstream with the consortium.

Grounded on AT, a basic a priori argument of this study is that different BC systems should be designed based on context, particularly depending on the risk of ex-post opportunism. The analysis revealed that the designed BC systems had a level of system trust consistent with the risk of an agent's ex-post opportunism; namely, the higher the risk of ex-post opportunism, the higher the level of system trust that the BC system needed to guarantee (this visual pattern is illustrated in the Data).

Interviews were useful in understanding why and how different BC systems were designed for different agents. The President of the consortium said: "Monitoring production and cultivation phases is crucial because these could have a tremendous impact on food quality and safety. The number of activities to control is impressive, and some fraudulent behaviors, such as the improper use of pesticides, are very difficult to detect. Although on-site and documental audits conducted by our certification body can deter unfair conducts, my feeling is that the risk

TABLE 5 | BC systems use (within-case analysis).

Dyad	Description	Variable	Rating
A (Consortium—Company A/Fruit producer)	For each production batch, company A collects different data on harvested fruits (e.g., quantity, variety, organoleptic characteristics) and cultivation processes (e.g., climatic conditions, farming location, days and kinds of insecticide or pesticides treatments, irrigation, date of harvesting, compliance with quality standards, etc.) and records it on BC, together with company A's general information. Based on the level of confidentiality, data are stored on the Ethereum public BC or the private Enterprise Ethereum BC, which grants different levels of accessibility to SC actors. For example, growing parameters are stored publicly and can be accessed by anyone, while the quantity of harvested fruits is saved privately and made accessible only to authorized SC actors.	Permission model	Hybrid
	Data entry is twofold: Most information is manually entered onto the BC by the company's administrative staff using a user-friendly software interface implemented on the technological devices already in use (e.g., smartphones, personal computers). IoT sensors are also used to automatically measure critical environmental conditions during the cultivation phase, namely the temperature, soil moisture, and quality.	Data entry	Human + IoT
	An independent third-party certification body is delegated by the consortium to verify the adherence of data on BC with real-world occurrences as well as the correct functioning of IoT devices. Data gathered during the on-site audits are first saved on the Italian national information systems for regulatory concerns and then synchronized on the BC.	TPCB	Yes
	Smart contracts are used to automatically trigger alerts when certain parameters detected by IoT sensors exceed the pre-defined thresholds in order to stimulate plant-health checks and prevent quality issues. In particular, they signal a lack or excess of water and a too low or high temperature, which can alter fruit characteristics. Moreover, the occurrence of specific conditions of temperature and soil moisture may encourage the development of plant diseases.	Smart contracts	Yes
B (Consortium—Company B/Fruit producer)	Ethereum public BC and Enterprise Ethereum private BC are jointly used to store farm-, product- and process-related data. Company B can decide which uploaded information will be publicly accessible and which ones will be only open to a few selected members who have permission to avoid the disclosure of sensitive information to competitors.	Permission model	Hybrid
	IoT sensors complement BC to create transparent, immutable and auditable records of: ambient temperature and relative humidity in the cultivation phase. These data are collected automatically and in real-time with a pre-defined sampling frequency, and directly transmitted to BC without requiring manual entry, to ensure integrity. The remaining information is still inserted manually by internal workers.	Data entry	Human + IoT
	As in case A, data uploaded on BC are certified by a third-party certification body, which also verifies the functioning and calibration of IoT sensors. These data are also stored in the Italian national agricultural system for reasons of compliance with government regulations.	TPCB	Yes
	Smart contracts perform self-check on environmental conditions and automatically notify the company when any potentially dangerous violation of default tolerances occurs in order to foster timely phytosanitary inspections.	Smart contracts	Yes

(Continues)

TABLE 5 | (Continued)

Dyad	Description	Variable	Rating
C (Consortium—Company C/ Italian shipper)	For each production batch that is shipped by the carrier, many details are recorded on BC about transportation, such as goods arrival and departure, temperature and humidity storage conditions as well as general information about the logistic provider (e.g., name, location, etc.). The platform allows the company to decide whether to save the data publicly on the Ethereum BC or on the Enterprise Ethereum BC to restrict access. Product information that is useful for all SC actors is saved publicly (e.g., data related to final product quality).	Permission model	Hybrid
	BC is supported by IoT devices to accurately monitor geographical location during transportation as well as shipping conditions that are critical for preserving fruits quality and freshness, namely the temperature and humidity parameters that can favor the formation of mildew. Data captured by sensors are transmitted in real-time to the BC.	Data entry	IoT
	IoT sensors are installed on the transport vehicle and verified by a third-party certification body to ensure their correct functioning and therefore the validity of data entry on BC.	TPCB	Yes
	In order to mitigate potential quality deteriorations, smart contracts execute real-time temperature and humidity controls and automatically trigger in-transit notifications to the consortium and carrier whenever any violations to pre-defined limits occur.	Smart contracts	Yes
D (Consortium—Company D/ Italian shipper)	The carrier records data about the goods transported (e.g., quantity, number of production batch), transport conditions and the time information on arrival and departure. Data can be saved on the Ethereum BC or kept private on the Enterprise Ethereum BC, based on the carrier decision. The shipper currently shares all the data publicly.	Permission model	Hybrid
	As in case C, IoT sensors are used to automatically update and transmit real-time data on temperature, humidity and geographical location.	Data entry	IoT
	As in case C, a trusted third-party certification body supervises and certifies the functioning of IoT sensors installed on the vehicles.	TPCB	Yes
	As in case C, smart contracts verify the respect of temperature and humidity tolerances.	Smart contracts	Yes
E (Consortium—Company E/ Italian packer)	During the packing phase, the records that Company E uploads on BC concern the dates of fruits receipt and dispatch, conformity of processed products and packaging procedures. Data are at the lot level. The hybrid nature of the adopted BC, which combines Ethereum public BC and the private Enterprise Ethereum BC, addresses the specific company's need to limit access to certain confidential information.	Permission model	Hybrid
	Data are manually communicated to the BC by the company internal staff through a dedicated mobile application installed on mobile phones that were already in use.	Data entry	Human
	The accuracy of information gathered from the real-world is ensured by the involvement of third-party intermediaries with specific on-field audits.	TPCB	Yes
	Smart contracts are not used.	Smart contracts	No

(Continues)

remains high." Interviewees agreed that the producers operate in a context characterized by a high risk of ex-post opportunism. In cases F, H, and I, the agents were logistics providers; again, the risk of ex-post opportunism was considered high. The Vice-President of the consortium commented: "In the absence of any monitoring of temperature and humidity during transportation by ships or trucks, the products deteriorate, compromising food quality and safety. Control is essential because no carrier

Dyad	Description	Variable	Rating
F (Consortium—Company F/ Italian logistic service provider)	By using the web-based platform accessible with existing digital devices, Company F uploads information about firm characteristics, type of vehicle used for transportation, bill of landing, departure and arrival date. The company combines the use of Ethereum BC and Enterprise Ethereum BC. Thus, certain information that is saved can be accessed by anyone, whereas a more sensitive one is intentionally kept private.	Permission model	Hybrid
	Data upload into BC is enabled by a standardized software user interface. Internal staff is delegated to manually upload the information associated with each processed production batch.	Data entry	Human
	No audits are performed by external bodies to verify the accuracy and veracity of data declared on BC.	TPCB	No
	Smart contracts are not used.	Smart contracts	No
G (Consortium—Company G/ Italian large-scale distributor)	Company G shares information on the arrival of goods (i.e., the date, quantity and the related suppliers), and on the total number of fruits sold. External access to some sensitive data, such as quantities sold, is kept restricted to the consortium and third-party certification body. Ethereum and Enterprise Ethereum BCs are used to manage the privacy of uploaded data.	Permission model	Hybrid
	The data collection is based on manual recording and transmission on BC, whose activities are performed by delegated internal workers.	Data entry	Human
	Records are uploaded on BC without a data validation based on audits by external third-party authorities.	TPCB	No
	Smart contracts are not used.	Smart contracts	No
H (Consortium—Company H/ Italian logistic provider)	The use of a hybrid BC, that combine Ethereum and Enterprise Ethereum BCs, allows Company H to save data publicly or privately. Information on BC regards company name and location and shipping details (e.g., departure of goods and arrival time, amount and weight of transported goods, storage conditions, etc.). To facilitate custom control, the company uploads on BC a digital copy of the bill of landing and a certificate to prove that the cold treatment process was carried out in accordance with Chinese regulations, since products are delivered in China.	Permission model	Hybrid
	A company's employee within the administrative staff is responsible for the manual entry of data on BC. Despite the logistic provider monitors shipment conditions using temperature and humidity sensors, they operate offline and therefore are not connected to BC.	Data entry	Human
	Third parties are not involved in the processes of data collection and data entry.	TPCB	No
	Smart contracts are not used. In general, the driver does not receive any automatic notifications when out-of-tolerance values about storage conditions occur.	Smart contracts	No
I (Consortium—Company I/Chinese logistic provider)	Truck drivers of company I write information on the Chinese national private BC concerning: firm characteristics, departure and arrival of the vehicles, routings, bill of landing, storage conditions of the transported goods. The consortium has no visibility on that information whose access is restricted to Chinese companies, that is, Company I and its downstream players.	Permission model	Private

(Continues)

TABLE 5 | (Continued)

Dyad	Description	Variable	Rating
	All data are manually written on BC by the truck driver who interacts with the platform using a dedicated application that is installed on his/her smartphone.	Data entry	Human
	No external trusted auditors verify the reliability of the data that is uploaded on BC by truck drivers.	TPCB	No
	Smart contracts are not used.	Smart contracts	No
J (Consortium—Company J/ Chinese importer)	As in case I, Company J uses the national private BC to register information about the firm, the date of the receipt and dispatch of imported fruits, quantity received, etc. Access to this information is restricted to Chinese actors.	Permission model	Private
	The company's workers are responsible to manually recording data on BC by using a specific software user interface that is installed on the computers already in use by the company.	Data entry	Human
	Data collection and entry activities are not monitored by any external third-party authority.	TPCB	No
	Smart contracts are not used.	Smart contracts	No
K (Consortium—Company K/ Chinese large-scale distributor)	Through the web-based platform developed by the technology provider, Company K saves information concerning the date of goods arrival, quantity received, and the number of fruits sold. As in cases I and J, because this information is saved on the private national Chinese BC, SC actors located in Italy have no visibility on data.	Permission model	Private
	Data are manually entered into the platform by Company K's internal accounting staff, using the frontend user interface that is installed on company's devices.	Data entry	Human
	Data inserted on the system are not validated by audits carried out by certification bodies.	TPCB	No
	Smart contracts are not used.	Smart contracts	No

will ever proactively confess that they were unable to meet temperature or humidity limits." The risk of ex-post opportunism and the need for monitoring were also perceived as high in cases C and D, although agents were Italian shippers and fruits were stored in trucks for a short time with a moderate impact on food quality and safety. The Vice-President of the consortium argued: "Paradoxically, monitoring transport activities is even more important when the logistics route is short, as in the case of domestic transport. In this situation it is more difficult to detect through visual inspection if the product has deteriorated during transport, and even if the fruit is apparently delivered in perfect conditions, the travel could have partially compromised its quality and reduced its shelf-life."

In all the above-cited cases, given their need to strictly monitor agents' behaviors, the principal designed and proposed a BC system with a high level of system trust.

Instead, in cases E and K, agents' opportunistic behaviors were unlikely. The CEO of the packer E explained: "Overall, monitoring packaging activities is less complex than cultivation and harvesting activities. These activities take place in a relatively narrow and circumscribed area: a dedicated line or equipment in a production plant. National directives define clear responsibilities and set out strict rules with which packers must comply. Controls are very frequent and severe. Packers are less numerous than producers and this is an additional facilitation in control activities." As regards the case K, the import–export specialist said: "Grocers in China interested in commercializing this high-quality fruit, such as company K differentiates from other grocers for the high investments in store quality, the selection of foreign high-quality products, and a special attention to customer. This competitive positioning and the fear of potential damage to brand reputation in the case of quality/safety issues are the strongest deterrents of any unfair conduct. [...] the guarantee of product origin for Italian goods is fundamental [...] food counterfeiting is a severe issue and selling fruit that has been subjected to out-of-control pesticide treatments can seriously harm consumers' health." To sum up, in cases E and K the consequences of opportunistic behaviors could be severe for food quality and safety (e.g., counterfeiting, contaminations during packaging), but such behaviors are unlikely; thus, the resulting risk of ex-post opportunism was classified as medium. A BC system with a medium level of system trust was proposed, that is, one that was not integrated with the use of IoTs to collect data or smart contracts but still involved a TPCB to verify data veracity.

TABLE 6 | Cases with differences in the BC systems designed and used (within-case analysis).

Dyad	Description (BC systems designed vs used)	Variables and ratings (differences)
F and H (Consortium –Companies F, H: Italian logistic providers)	The intention of the consortium, in general, for all the dyads, was to apply a BC with a hybrid permission model, to increase data visibility. In cases F and H, this was judged feasible, and a hybrid permission model is currently in use.	Permission model: Hybrid (as designed)
	As in dyads C and D, given the need to monitor temperature and humidity during transportation, the consortium proposed to install IoTs on vehicles to monitor and transmit real-time data to BC. TPCB should have checked the functioning of the IoTs. The consortium also proposed applying smart contracts through IoT use to automatically notify any violations of temperature and humidity limits. Overall, this solution was perceived as too complex by Companies F and H due to excessive costs. The current data entry on BC was manual, TPCBs were not used to verify BC data, and smart contracts were not currently in use.	Data entry: Human (instead of IoT) TPCB: No (instead of 'Yes') Smart contracts: No (instead of 'Yes')
I (Consortium – Company I: Chinese logistic provider)	The consortium would prefer to use a hybrid permission model to increase data visibility. Instead, company I decided to use the private national Chinese BC, which restricted data access to only some companies in the supply network.	Permission model: Private (instead of 'Hybrid')
	As in cases F and H, the consortium considered using IoTs to upload data into BC important, given that monitoring temperature and humidity during transportation is crucial. For the same reason, it also proposed using TPCBs to verify IoT functioning and linking smart contracts to IoT. Similar to companies F and H, this solution was judged too complex and expensive by Company I.	Data entry: Human (instead of IoT) TPCB: No (instead of 'Yes') Smart contracts: No (instead of 'Yes')
J (Consortium— Company J/Chinese importer)	As in case I, company J decided to use the private national Chinese BC, although the consortium aimed to adopt a BC with a hybrid permission model for all agents.	Permission model: Private (instead of 'Hybrid')
	The consortium did not need to strictly monitor the activities in this supply network tier (as in cases F, H or I), due to the very short storage, and as a consequence, the BC system design proposed included a manual data entry, no TPCBs involved and no use of smart contracts. The BC in use meets these features.	Data entry: Human (as designed) TPCB: No (as designed) Smart contracts: No (as designed)
K (Consortium – Company K: Chinese large-scale distributor)	The intention of the consortium was to use a BC with a hybrid permission model for all the dyads. As in case I and J, company K instead preferred to use the national Chinese BC.	Permission model: Private (instead of 'Hybrid')
	In this case, the consortium did not consider crucial to adopt IoTs and, linked to these, smart contracts to monitor storing conditions in the supermarket, or register other types of data. Instead, it judged it appropriate that BC data (e.g., date of goods arrival, fruits sold, etc.) be validated by an external certification body (TPCB) to assure data veracity. This last proposal was infeasible for Company K, given the additional costs that would be required for an external certification body.	Data entry: Human (as designed) TPCB: No (instead of 'Yes') Smart contracts: No (as designed)

Finally, in cases G and J, the risk of ex-post opportunism was judged low (see Table 7) because opportunistic behaviors were unlikely (due to the strict control measures already in place) and had a marginal detrimental effect on food quality and safety (in case G, because (a) products were stocked within a supermarket with a low variation in temperature/humidity; (b) customer knew the product and was able to visually identify quality problems; (c) fruit counterfeiting is rather uncommon; in case J, due to a

TABLE 7 | Risk of ex-post opportunism (within-case analysis).

Case	Description	Variable	Rating
A and B Consortium – Companies A and B (Italian fruit producers)	Type of opportunistic behavior: Non-compliance with regulations regarding cultivation (e.g., fruit variety and characteristics, density per hectare, type of harvest, improper use of pesticides, fungicides, fertilizers, etc.). Likelihood (Possible): Specific external audits by the certification body designated by the consortium mitigate potential misconducts. However, identifying a potential misconduct in the cultivation phase only through visual inspections is difficult. Degree of detrimental consequences (Critical): Misconducts in this phase can seriously compromise product safety and quality.	Risk of agent's ex-post opportunism	High
C and D Consortium – Companies C and D (Italian shippers)	Type of opportunistic behavior: Lack of observance of temperature and humidity ranges during transportation in order to preserve fruits. Likelihood (Likely): Considering the short distance between companies C or D and the packer, the non-respect for temperature and humidity thresholds is difficult to detect by visual inspections of products received by the packer. Degree of detrimental consequences (Moderate): Due to short shipment time, any out-of-tolerance temperature or humidity condition has a moderate impact on final product quality/safety.	Risk of agent's ex-post opportunism	High
E Consortium—Company E (Italian packer)	Type of opportunistic behavior: Packaging of non-PGI products or of PGI products that do not meet the specifications described in the production regulation (e.g., minimum diameter). Likelihood (Unlikely): The packaging process is strictly controlled by a third-party certification body, and any inappropriate behavior is easily detectable through monitoring of product inbound and outbound deliveries. Degree of detrimental consequences (Critical): The commercialization of low-quality products labeled PGI may compromise the quality and authenticity of final products.	Risk of agent's ex-post opportunism	Medium
F, H and I Consortium – Companies F, H (Italian logistic providers), and I (Chinese logistic provider)	Type of opportunistic behavior: Non-compliance with the defined transport temperature or humidity. Likelihood (Possible): Data eventually registered or monitored during transportation are not shared with the consortium. The journey can last some days or weeks (company F manages national shipments in Italy and Company I shipments in China, both by trucks) or some months (company H manages shipments from Italy to China by ship). If the right transport conditions are not met, the product deteriorates, and this can be identifiable by visual inspections. Degree of detrimental consequences (Critical): Inappropriate storage conditions during transportation (usually temperature or humidity abuses) cause safety/quality hazards. This problem is also exacerbated when the agreed shipping time is not respected.	Risk of agent's ex-post opportunism	High

(Continues)

very short food stock storage in the transit point of the Chinese importer (agent J). A basic BC system was proposed without the use of IoT, smart contracts, or the involvement of a TPCB, although with a hybrid permission model to make the saved data publicly visible, tamperproof, and guarantee a greater level of veracity.

Based on this evidence, the following propositions are here advanced:

P1. *Different BC systems choices assure different degrees of system trust and thus provide the principal with different capabilities to monitor the agents' behavior*:

TABLE 7 | (Continued)

Case	Description	Variable	Rating
G Consortium – Company G (Italian large-scale distributor)	Type of opportunistic behavior: Sale of products that remain on the shelves of supermarket for a long time. Likelihood (Unlikely): Products on the shelf are subject to controls by the Italian surveillance bodies and the department of the central inspectorate for fraud repression and quality. These bodies conduct several severe controls, taking photos of the products being sold, asking for bills of lading, etc. Company G is highly committed to delivering fresh fruits to customers, perceived as high-quality products, to maintain a certain brand image. Italian final customers are typically familiar with these products and expect distinctive features (e.g., dimension and color). Degree of detrimental consequences (Marginal): The consequences of opportunistic behaviors in this phase marginally influence PGI products quality/safety since temperature and humidity conditions in a supermarket are usually stable, which guarantees a long shelf-life and mitigates quality and safety deteriorations.	Risk of agent's ex-post opportunism	Low
J Consortium – Company J (Chinese importer)	Type of opportunistic behavior: Non-compliance with the defined storage temperature and humidity. Likelihood (Unlikely): Company J is committed to preserving the quality and safety of the product sent to the large-scale distributor, as this latter adopts a strict verification and acceptance procedure to ensure final customers about product quality, safety, and authenticity. Fruits are stored by the importer for a short time in the transit point. Degree of detrimental consequences (Marginal): Due to the very short storage, any out-of-tolerance temperature or humidity conditions has a marginal impact on the final product quality/safety.	Risk of agent's ex-post opportunism	Low
K Consortium – Company K (Chinese large-scale distributor)	Type of opportunistic behavior: Sale of low-quality and non-PGI products generally using a similar packaging that shows a sort of PGI label (counterfeiting). The issue of products that remain on the shelves of the supermarket for a long time is considered of secondary importance by the consortium compared to counterfeiting. Although it is possible that this occurs, since there is no surveillance body similar to that in Case G, and customers are less familiar with this product, fruits in supermarkets are usually stored in appropriate conditions. The impact on product quality and safety would be marginal, determining a low risk of ex-post opportunism. For this reason, the subsequent analysis focuses on the major issue of counterfeiting. Likelihood (Unlikely): In general, a higher risk of counterfeiting in China potentially exists with non-original PGI products sold using a similar packaging or name, misleading the consumer who is not used to distinguishing the original fruit. However, company K chose to sell distinctive high-quality products (Made in Italy) in its store, and its brand image would suffer enormously from scandals linked to the sale of non-authentic products or low-quality products. Degree of detrimental consequences (Critical): Counterfeiting has a strong impact on product quality and safety.	Risk of agent's ex-post opportunism	Medium

TABLE 8 | TOE factors (within-case analysis).

	Organizational variables		Technological variables		Environmental variables	
Case	Organizational size	Top management support	Technology complexity	Relative advantage	Government or contractual incentives	Regulatory environment
A	Small	High	High[a]	High	Yes[c]	Italy
B	Small	High	High[a]	High	Yes[c]	Italy
C	Small	High	High[a]	High	Yes[c]	Italy
D	Small	High	High[a]	High	Yes[c]	Italy
E	Small	High	Medium[b]	High	Yes[c]	Italy
F	Medium	Low	High[a]	Low	No	Italy
G	Large	High	Low	High	No	Italy
H	Large	Low	High[a]	Low	No	Italy
I	Medium	Low	High[a]	Low	No	China
J	Medium	High	Low	High	No	China
K	Large	Low	Medium[b]	Low	No	China

[a]Since the BC system design required additional measures integrated with the BC technology, such as TPCBs, smart contracts, and IoTs, the technological complexity of the system was perceived as high due to the excessive costs and resources that would have been required by the company.
[b]The technology complexity was perceived as medium, as TPCBs were recommended to increase data veracity.
[c]These agents could benefit from resources granted by the Italian government to the consortium for BC implementation (governmental incentives). When needed, they could also use TPCB services by contract for free (contractual incentives).

P1a: *In a principal-agent dyad, BC system choices characterized by hybrid permission model, a data entry supported by IoT, the use of a TPCB and of smart contracts are associated with a high level of BC system trust.*

P1b: *In a principal-agent dyad, BC system choices characterized by hybrid permission model, a human data entry and the use of a TPCB are associated with a medium level of BC system trust.*

P1c: *In a principal-agent dyad, BC system choices characterized by hybrid permission model, a human data entry and the use of a TPCB are associated with a low level of BC system trust.*

P2. *In a principal–agent dyad, the risk of a supply chain member agent's ex-post opportunism is positively related to the level of system trust of the BC system designed.*

4.2.2 | Factors Influencing the BC Systems Used by Supply Chain Member Agents

For the different agents, the consortium, in collaboration with the TP, designed BC systems with a level of system trust that increased with the risk of ex-post opportunism. However, in some cases (F, H, I, J, and K), the BC systems adopted differed from those designed for various reasons. Causal network analysis was important to understand how the risk of ex-post opportunism, together with TOE factors, influenced the BC systems adopted. (Data S1 reports the causal network analysis applied to each dyad and by grouping dyads with high, medium, and low risks of ex-post opportunism).

An important premise in this analysis regards some similarities among the agents that emerged. In particular, all the agents shared common traits in terms of: (a) organizational readiness for BC implementation—that is, the availability of skilled employees to support the adoption of the technology and an information technology infrastructure that enables BC implementation; and (b) compatibility of their enterprise information systems and business processes with BC implementation, which are contextual factors usually contemplated in BC studies that use TOE (Table 2). In this BC project, financed by the Italian government, the TP was responsible for supporting adopters with specific training and solving specific issues that could have been found about system interoperability. All the agents were also all equipped with an internet connection and digital devices (e.g., PCs or smartphones/tablets) needed to interact with the BC system, although none of the actors had previously implemented IoT. For all the companies involved, the TP, together with the consortium, analyzed current processes and integrated the information systems in use with BC. In general, agents were not concerned about technical problems such as the BC standard proposed (e.g., Ethereum vs. other BC platforms) or the level of maturity of BC technology (e.g., transaction capability issues) because, as stated by the CEO of the producer A: "All operational problems and integration with current processes were appropriately addressed by [the TP] and the consortium. [The TP] has a long experience in BC implementation in food and our consortium is one of the most important in Italy for food. We are confident that they are great experts of blockchain [...] We are small producers and need to rely on their competence." Thus, moving beyond the traditional barriers mentioned in the literature (Table 2), such as compatibility with existing systems and BC maturity level, a major issue regarded the configuration of BC systems, which determined a different perceived technology complexity. In the dyads in which the risk of ex-post opportunism was

TABLE 9 | Level of BC system trust.

Level of BC system trust

Clusters	BC systems designed	BC system used	BC systems variables	Degree of data visibility, data immutability, data veracity, and responsiveness	Level of BC system trust
1	Dyads: none	Dyads: I, K, J	Permission model: Private Data entry: Human TPCB: No Smart contracts: No	Degree of data availability: Null. Private permission model does not permit the principal to access information that is digitally saved on BC by the agent. Degree of data immutability: Low. Private permission provides low guarantees against data tampering, since data is saved on a private BC, whose intrinsic characteristics do not ensure the principal that data uploaded by the agent has not been subsequently modified. Degree of data veracity: Null. Human data entry without additional controls by a TPCB potentially makes data prone to quality issues. Degree of responsiveness: Low. The absence of smart contracts and IoT real-time data uploading does not allow the availability of timely information and alerts.	Minimum
2	Dyads: G, J	Dyads: G, F, H	Permission model: Hybrid Data entry: Human TPCB: No Smart contracts: No	Degree of data availability: High. Hybrid permission model allows the principal to access information that is publicly saved on BC by the agent. Degree of data immutability: High. Hybrid permission provides high guarantees against data tampering, since the hashes of the uploaded information are saved on a public BC. This ensures the principal that the data uploaded by the agent has not been subsequently modified. Degree of data veracity: Low. Human data entry without any additional control by a TPCB can lead to data quality issues. However, false statements are discouraged, since data is publicly saved. Degree of responsiveness: Low. As in the BC systems of Cluster 1.	Low

(Continues)

TABLE 9 | (Continued)

Level of BC system trust					
Clusters	**BC systems designed**	**BC system used**	**BC systems variables**	**Degree of data visibility, data immutability, data veracity, and responsiveness**	**Level of BC system trust**
3	Dyads: E, K	Dyad: E	Permission model: Hybrid Data entry: Human TPCB: Yes Smart contracts: No	Degree of data availability: High. As in the BC systems of Cluster 2. Degree of data immutability: High. As in the BC systems of Cluster 2. Degree of data veracity: Medium. As in the BC systems of Cluster 2, false statements are discouraged since data is publicly saved. In addition, manually uploaded data are checked by a TPCB to ensure accuracy and prevent intentional manipulations. However, non-intentional errors in the data input phase can still occur. Degree of responsiveness: Low. As in BC systems of Clusters 1 and 2.	Medium
4	Dyads: A, B, C, D, F, H, I	Dyads: A, B, C, D	Permission model: Hybrid Data entry: Human + IoT or IoT TPCB: Yes Smart contracts: Yes	Degree of data availability: High. As in BC systems of the Clusters 2 and 3. Degree of data immutability: High. As in BC systems of the Clusters 2 and 3. Degree of data veracity: High. Some data is automatically collected and uploaded on BC in real-time by IoT sensors, which have been previously verified and calibrated by a TPCB. Data accuracy improves compared to BC systems 3. However, non-intentional errors can still occur for data manually uploaded on BC after being verified by a TPCB. Degree of responsiveness: High. The use of smart contracts and IoT real-time data uploading allows for the availability of timely information and alerts.	High

judged high (A, B, C, D, F, H, and I), the principal designed a BC system with a high level of system trust, integrated with the use of IoT and smart contracts, involving a TPCB, and always based on a hybrid permission model. The technological complexity of the BC system designed was perceived as high due to the costs and resources that would have been required to the agents. The operations manager of the logistics provider F considered the requests of the BC project too demanding: “Operators are required to dedicate their time to entering data in the BC; the company is required to invest in temperature/humidity sensors and to accept an intensification of controls by certification bodies, which requires additional time from our operators. What is the return on this significant investment in time and money? Increased monitoring of our activities and a smart contract that punishes us if we don't respect the temperature range. I believe that supply chain visibility is important, but I'm also skeptical about this approach.”

Despite the perception of high technological complexity, in cases A, B, C, and D, the top management supported the initiative, judging the relative advantage as high due to contractual and governmental incentives. The CEO of producer B said: “This project required both a significant cultural change and an investment in terms of time, money, and human resources. However, as a producer, I benefited from a governmental incentive granted to the consortium for BC implementation. All the consortium associates could also use the certification body services for free as part of a general agreement with the consortium. We were grateful to the consortium for such opportunities and economic support, and did our best to implement the BC as proposed.”

By contrast, in other cases (F and H), in which adopters had no access to governmental or contractual incentives, the relative advantage of implementing this BC system was perceived as low due to the high costs and efforts required. The companies were not motivated to use IoTs and smart contracts integrated with BC or to involve a TPCB for BC data validation. This led to the use of a simplified BC system that was able to guarantee a low level of system trust, according to the taxonomy in Table 9. The same applies to the logistics provider I, but a fundamental difference here is the regulatory environment. In general, in all the dyads in which agents were in China (I, K, and J), the BC systems used guaranteed a minimum level of system trust, regardless of the risk of ex-post opportunism. Chinese companies usually adopt the national BC, and the TP considers the task of opening a node of the hybrid BC in China, although technically feasible, an expensive and time-consuming process. Thus, in addition to not using a TPCB or lacking IoTs and smart contracts integrated with the BC, the logistics provider I relied on a BC based on a private permission model, a feature that determined a minimum level of BC system trust for the consortium.

In dyads in which the risk of ex-post opportunism was judged medium (E and K), the proposed BC system required a TPCB for data verification in addition to using a hybrid permission model. As in dyads A–D, the CEO of packer E explained that governmental and contractual incentives and the Italian regulatory environment (where there was no national private BC) led to BC use consistent with the BC design. On the contrary, similarly to the dyads involving Chinese agents, the large-scale distributor K adopted a private permission model BC that lacked TPCB (i.e., with a minimum level of system trust) due to the peculiarity of the Chinese regulatory environment and the lack of any incentive.

Finally, in dyads characterized by low risk (G and J), the consortium proposed a BC system with a hybrid permission model without integrated IoTs or smart contracts and without any TPCB. Since the agents perceived this BC system as not technologically complex, even in the absence of any governmental and contractual incentives, the relative advantage was judged high; consequently, top management support was also high. In dyad G, the proposed BC system was adopted. Instead, given that J was a Chinese company, a national private BC was preferred.

It is worth noting that the contextual variable ‘organizational size’ was not included in any causal network analysis, as it was not influential. In summary, the following propositions are advanced:

P3. *Technological, organizational, and environmental factors influence the level of system trust of the BC system adopted by supply chain member agents.*

P3a: *The relative advantage of implementing a proposed BC system as perceived by the agent, in turn influenced by its technological complexity and governmental and contractual incentives, determines the agent's top management support.*

P3b: *Low support from an agent's top management limits the level of system trust of an adopted BC system to a low level by discouraging agent's adoption of IoTs, smart contracts, and TPCBs. BC systems with a high or medium level of system trust require high top management support.*

P3c: *A regulatory environment which favors the use of a private rather than a hybrid permission model limits the level of system trust of the adopted BC system to a minimum level.*

5 | Discussion

5.1 | Summary of the Theoretical Model

Building on AT and TOE frameworks, this study develops a model to interpret BC system design choices and the relevant contextual factors that can influence the final BC system use (Figure 4). Grounding AT and its assumptions in the BC context led us to extend the concept of BC trust to encompass the entire BC system (i.e., BC system trust) in order to study the fit between some important BC system design choices and the level of ex-post opportunism to be addressed. The overall model then intersects concepts from the AT and TOE theories to provide explanations about the determinants of BC system use. The overarching interpretation of the results is that the level of system trust of the BC system designed and proposed by the consortium depends on the risk level of agents' ex-post opportunism. The BC system designed, in turn, shapes the agent's perception of the technology complexity, which, along with other TOE factors, influences the BC system effectively used. Specifically, BC systems can be configured in different ways, ensuring varying levels of system trust. When the risk of ex-post opportunism

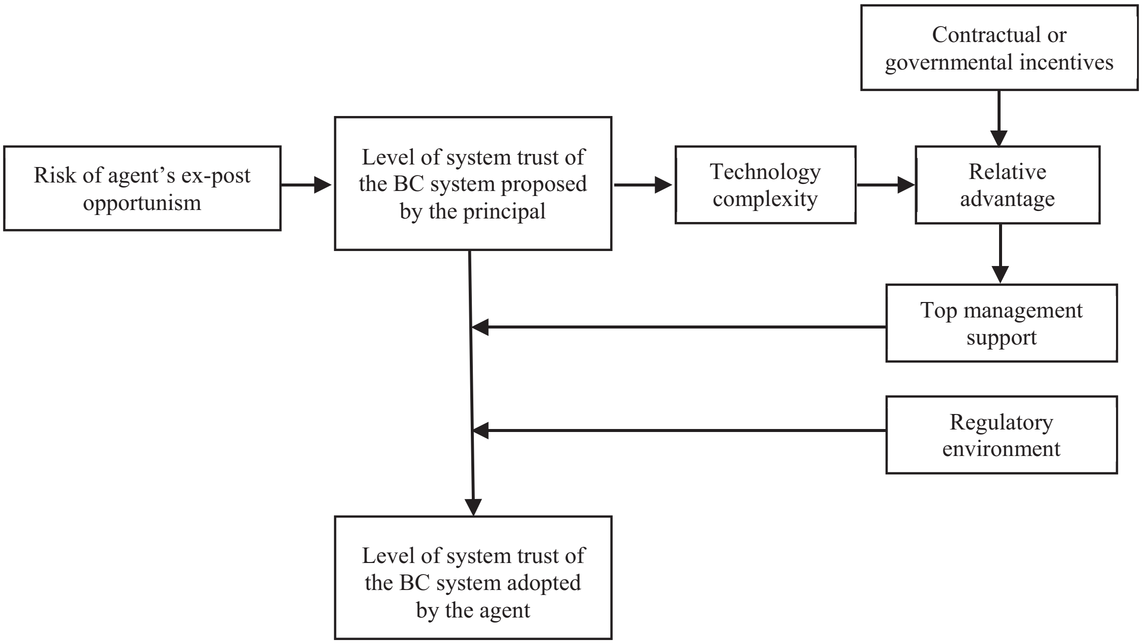


FIGURE 4 | Theoretical model.

is high, the principal designs and proposes BC systems to the agents that are more powerful in reducing information asymmetry. However, an agent's willingness to adopt the BC system designed depends on a set of interconnected TOE factors that can cause a mismatch between the level of system trust of the BC system designed and that effectively used, as summarized in proposition 3.

5.2 | Theoretical Contributions

A first analysis of this research regards the appropriateness of the different BC system's design choices for addressing different levels of risk of ex-post opportunism. On the one hand, this investigation fills a relevant gap in BC literature concerning the comparison of different BC systems in relation to the SC context where they are implemented. On the other hand, it integrates BC research in the SCM field in different ways.

First, this research reveals the need to extend the concept of 'BC trust' and measure it at a system level when comparing and assessing different BC implementations, as both differences in the BC technology as well as in the BC-integrated technological and organizational tools count. Previous research analyzed in detail the impact of specific technical features of BC (i.e., cryptography system, decentralized consensus, and distributed ledger) on SC transparency (i.e., traceability and visibility), thus guaranteeing trust in the BC technology (Durach et al. 2021; Falcone et al. 2021; Xu et al. 2021). Our research, instead, following an approach similar to Gligor et al. (2022), takes a systemic perspective. While in Gligor et al. (2022) the systemic view concerns the intra- and inter-organizational orchestration of structuring, bundling, and leveraging of processes to achieve SC transparency through BC, the present study introduces the notion of 'BC system trust'. It posits that different BC system configurations determine different levels of system trust based on their degree of data availability, immutability, veracity, and responsiveness (Stranieri et al. 2021), and thus on their ability to reduce information asymmetry (Whipple and Roh 2010). Compared to other studies, such as Xu et al. (2021), the investigation is wider as it also contemplates the use of technologies integrated with the BC for data entry, in contrast to manual entry, as well as the use of TPCB integrated with BC. This research concludes that a data entry supported by IoTs, the use of TPCBs to validate data and calibrate IoTs, as well as smart contracts to signal data alerts represent a mix of configuration choices that offers a better guarantee of data veracity and responsiveness, increasing trust, compared to a date entry mode based on a human data entry associated with TPCB checks, which however guarantees better data veracity compared to simple human data entry. The BC permission model also counts, as public or hybrid BCs can offer a further guarantee of data immutability compared to private ones (Chang et al. 2019; Dutta et al. 2020; Pandey et al. 2022). Moreover, for a stakeholder or a principal who needs to monitor SC actors' behaviors, data availability is fundamental, and this means being connected to the BC through a node.

Second, this research proposes a new study perspective regarding the concept of 'trust', establishing a link between BC system trust and the level of risk of ex-post opportunism. Consistent with Treiblmaier and Rejeb (2023) and Lumineau et al. (2025) who advocate for exploring the specific conditions under which BC operates, the present study advances that BC configurations should not be assessed in *absolute terms*. Rather, what counts in designing a BC system is the *fit* between its level of system trust and the risk of ex-post opportunism by SC member agents. This is in accordance with the AT view that the higher the risk of opportunism in a relationship, the more resources that must be spent on control and monitoring (Wathne and Heide 2000). This perspective, together with the need to extend the concept of trust to the whole BC system, enriches the debate on the tensions underlying Sternberg et al.'s (2021) paradox that BC implementations require trusted actors, because if input data are false the benefit of using BC is vanishing. On the one hand, the present research reveals that these tensions depend on the system trust guaranteed by the whole BC system design, and not only by the BC technology itself. In general, BC systems characterized by high level of system trust -such as those integrated with IoTs and smart contracts and involving TPCBs for data validation- reduce the need for trusted actors. On the other hand, this tension between the use of BC and the need for trusted SC actors depends on the SC context. Where misconduct is unlikely to occur (e.g., situations in which the lack of quality of a food is easily detectable, or controls are severe and frequent), even BC systems characterized by a lower level of system trust are sufficient to guarantee food quality and safety, and Sternberg et al.'s (2021) paradox is less relevant.

Third, thanks to its systemic perspective, this research offers novel evidence of the integration of BC technology with other agents' monitoring mechanisms to appropriately address ex-post opportunism. In particular, the present pilot case study represents an example of how using TPCBs combined with BC technology to design a BC system that guarantees an appropriate level of trust, in line with a few prior studies in the food sector (Leong et al. 2019; Danese et al. 2021). TPCBs are used to validate IoT calibration and certify BC data veracity. This research found that this role is especially critical when the risk of ex-post opportunism is high. Future research could further elaborate on the integration of BC with other monitoring mechanisms, trying to depict possible future scenarios in the food sector. Literature generally agrees that BC will replace traditional traceability technologies (Danese et al. 2021); however, further research and industry advancements are necessary to better understand how its use will align with industry standards and, consequently, whether and how these standards will need to evolve with the diffusion of BC adoption. For instance, some studies (Durach et al. 2021; Kurpjuweit et al. 2021) examine BC potential in digitalizing the activities of third parties during audits by certification authorities selected by food consortia as well as by national surveillance bodies.

Finally, a further contribution is the analysis of contextual factors that influence the use of different BC systems by agents, determining (or not) a widespread adoption in the supply network. Many conventional contingencies highlighted in BC's previous research in food SCs were found to be relevant (Kamilaris et al. 2019; Köhler and Pizzol 2020; Chen et al. 2021; Kurpjuweit et al. 2021; Vu et al. 2021; Pandey et al. 2022) (Figure 4). However, a more fundamental insight here is that BC adoption for agents is not a question of “yes or no” as a BC system design should be adapted, at least initially, to consider SC member agents' needs, thus ensuring a widespread BC adoption. In fact, compared to the above-mentioned studies and in general to existing research on BC and TOE theory (e.g., Clohessy et al. 2019; Kouhizadeh et al. 2020; Chen et al. 2021), the present research offers precise insights on the link between TOE factors and different BC systems adopted. This new line of inquiry is suggested by those studies providing evidence that differentiating between various BC systems is fundamental when analyzing BC adoption (Chen et al. 2021; Falcone et al. 2021; Kurpjuweit et al. 2021; Sternberg et al. 2021; Xu et al. 2021; Treiblmaier and Rejeb 2023). A further distinctive trait of this study compared to the literature on BC and TOE is that TOE factors emerged as strictly interconnected, exerting a joint effect on BC adoption, as suggested by Zhu et al. (2022).

This new perspective led to a richer interpretation of how some TOE factors, traditionally considered relevant, can influence BC adoption in food SCs. This study confirms that the ‘technology complexity’ perceived by agents (Chen et al. 2021)—also referred to as accessibility (Kamilaris et al. 2019; Köhler and Pizzol 2020; Vu et al. 2021; Pandey et al. 2022)—is an influential factor. Yet, it also advances that it is linked to the characteristics of BC systems (e.g., the use of IoTs, smart contracts, TPCB, etc.), which can determine a diverse perceived complexity as they require a different effort in terms of supporting technologies and processes. This confirms Kurpjuweit et al.'s (2021) finding that integrating BC systems into the company's information infrastructure can be perceived as a big challenge, which depends on BC-related technologies (e.g., sensors), and on what is required to collect and prepare input data (e.g., TPCB checks). For this reason, adapting BC systems to agents' needs, at least initially, can determine a wider adoption. Also, the perceived ‘relative advantage’ of applying a BC system was found to be relevant, in line with Chen et al. (2021) and many other studies emphasizing the high costs of BC implementation (Kamilaris et al. 2019; Köhler and Pizzol 2020; Kurpjuweit et al. 2021; Sternberg et al. 2021; Vu et al. 2021; Pandey et al. 2022). Being the perceived relative advantage in turn linked to the perceived technology complexity, we again conclude here that it depends on the different BC systems proposed.

These factors are linked together, and the perceived relative advantage is also influenced by the presence of governmental or contractual incentives. As a result, ‘technology complexity’ cannot be considered simply an inhibitor of BC adoption, as the presence of governmental or contractual incentives can reduce the efforts required for the technology implementation and thus increase the relative advantage as perceived by potential adopters and, in turn, top management support, which was identified as a major organizational issue (Kurpjuweit et al. 2021).

As regards the absence of regulations and standards, which is a further environmental factor considered in the food sector (Kamilaris et al. 2019; Köhler and Pizzol 2020; Chen et al. 2021; Vu et al. 2021; Pandey et al. 2022), it represents here again a variable influencing the type of BC system finally used rather than an inhibitor of BC adoption. It played a fundamental role in determining the BC system adopted by the Chinese partners in the supply network, which was based on a private permission model. This result is in line with Kurpjuweit et al. (2021), who maintain that differences in regulations and standards leading to national BC solutions represent one major barrier to BC implementation in international supply networks.

This research instead does not offer novel evidence about further barriers usually contemplated, such as the immature implementation of BC or its technological limits (e.g., scalability, privacy, and transaction capability) (Chen et al. 2021). The role of the technology provider was fundamental to support and train partners. In addition, it worked synergistically with all the participants in the BC project to address in advance potential technological limits, which, however, will become more critical once the project is extended to several other partners, as planned. This evidence supports the findings of Gligor et al. (2022), who discuss a case within a coffee supply chain where the development of BC-enabled SC traceability necessitated the bundling of resources from various SC actors and the BC technology provider. This process involved both exploratory learning and the integration of supply chain information with the technology platform.

Overall, the findings discussed above inform and suggest a broader debate on the potential implications and benefits of BC adoption, as well as future scenarios regarding its diffusion in fruit and vegetable SCs. In this way, the present study contributes to the body of research that identifies areas of BC application in SCM (Durach et al. 2021; Ahmed et al. 2022), with a specific focus on the food context.

First of all, the link found between the risk of ex-post opportunism and BC system design suggests the need to distinguish between different food distribution channels. Large-scale retailers, neighborhood fruit markets, and small shops significantly differ in their business models and in the risk of opportunistic conduct by upstream (e.g., producers, packers) or downstream SC members (e.g., logistics service providers, retailers). For instance, focusing on the context examined here, in Italy, neighborhood fruit markets and small shops rely on very short SCs, where misconduct is unlikely. Overall, the risk of ex-post opportunism by SC members is very low. Thus, although the investigated food consortium declares that its BC project may eventually include fruit shops and markets in the future, at present, BC is seen as especially beneficial in the distribution channel of large-scale retailers and thus in the context of complex food SCs. This confirms Ahmed et al. (2022) and Behnke and Janssen (2020). As regards the involvement of neighborhood fruit markets and small shops in BC adoption, future developments could assess the real need for BC in terms of reduced risk of ex-post opportunism, as well as the opportunity to consider the adoption of less complex BC systems.

The research also reveals that future scenarios and developments regarding BC adoption in food SCs cannot be evaluated solely in the light of current consumer awareness of food quality or consumer demand for food traceability. The food consortium investigated plays an institutional role in assuring food quality to many interested stakeholders, such as Chinese importers or institutions promoting Made-In-Italy exports (e.g., the National Foreign Trade Agency). From this case study, it emerged that, unlike the promoters of BC projects—such as food consortia—companies in food SCs are sometimes not equally committed to BC adoption. This is primarily because they perceive a low relative advantage in its adoption and are uncertain about consumer behavior, as well as future requirements in terms of standards and regulations. Simultaneously, they may perceive BC adoption as technologically complex due to the high costs and resources required, especially when BC systems demand integrated technologies and organizational tools. Yet, it is crucial for food consortia that SC actors be willing to adopt the proposed BC system across the SC and participate in BC pilot projects. Even if companies do not perceive an immediate benefit, it is essential for them to be prepared for future changes in the food sector. In this regard, the original perspective applied in this study in grounding TOE in BC research gives the opportunity to understand how a BC system can be initially adapted to the SC member agents' needs, to favor adoption, in line with theories of technology acceptance (Liao et al. 2009; Momani and Jamous 2017). The latter state that a technology user's attitude, in turn determined by its perceived usefulness (here, relative advantage), is fundamental for initial acceptance of a new technology. In the subsequent phases of adoption, attitude changes as a function of the initial attitude itself and satisfaction in technology use (dis/confirmation) and determines the user's intention to continue to adopt it. The present study suggests that engaging users in the initial adoption of BC, even modifying its design, could be relevant to trigger a virtual cycle of increased positive attitude and BC continued use, with the opportunity to subsequently redesign the technology towards the desired BC systems. This research highlights the importance of engaging SC members in the initial adoption of BC through contractual or governmental incentives or by reducing the perceived technology complexity. The investigation into the use of BC in the phases following the pilot testing (e.g., scaling and sustainability) represents an emerging avenue for future research, particularly through longitudinal studies on the evolution of BC adoption within supply networks.

5.3 | Managerial Contributions

The results obtained provide valuable practical insights for companies/consortia aiming to implement a BC project within their supply networks as well as for policymakers seeking to foster BC adoption.

First, for an organization acting as a principal responsible for monitoring the behavior of its agents, our findings offer guidance on how to assess the potential of various BC systems in terms of system trust. Additionally, we suggest how to design and recommend the adoption of BC systems that fit with the organization's requirements for monitoring and control. The risk matrix proposed in this study (Figure 3) could be used to assess the risk of ex-post opportunism of agents in the different supply network tiers to consistently design and propose diverse BC systems along the supply network. For instance, during transportation, IoTs or smart contracts integrated with BC can be instrumental in monitoring temperature and humidity thresholds. Instead, given that large-scale Italian food distributors are mandatory subjects to strict control by surveillance bodies and food is typically stored under appropriate conditions, a less complex BC system can be judged sufficiently adequate for monitoring their behaviors. Furthermore, the relationships illustrated in Figure 4 may prove useful in interpreting the potential influence of context on BC adoption, as well as in understanding the broader implications for the BC project. This theoretical model may increase the principal's awareness that, even when the risk of ex-post opportunism is high, given certain contextual conditions (e.g., when the top management support is low due to a low perceived relative advantage or when the regulatory environment favors the implementation of a private permission model), it can be necessary to adapt the designed BC systems to these contingencies, at least initially, to spread BC adoption. As contextual conditions evolve, the principal may, if necessary, consider enhancing the level of system trust in the BC systems adopted by agents, in alignment with the assessed risk level of ex-post opportunism. A major criticality for the principal that this study recommends solving regards the limit of relying on a BC with a private permission model in a portion of the supply network without being connected through a node, as this severely limits information transparency.

This research warns organizations acting as principals in promoting BC adoption, such as policymakers or food consortia, that the level of commitment to participating in a BC project may differ significantly between the organizations in the food SC and the BC promoter. Some SC members may not initially perceive a high relative advantage, as they may assume that consumers are not interested in the innovation or may not feel the need to proactively safeguard against future food regulations and standards. Instead, the food consortium investigated in this research, which works in collaboration with policymakers, sees in BC an opportunity to guarantee food quality to many stakeholders for different reasons. It judges BC pilot projects and experimentations essential to anticipate future export regulations that may make the use of BC mandatory, as well as to protect reliable and ethical SC members from unfair competition, such as the counterfeit of Made-in-Italy products. This is especially beneficial within the distribution channel of large-scale distributors that, unlike small family-owned fruit stores or neighborhood markets, are embedded in complex and international food SCs. Yet, for a successful BC experimentation on field, it is fundamental that SC members join BC pilot projects. On the one hand, the present research suggests to policymakers and food consortia that to increase SC members' perceived relative advantage, governmental or contractual incentives are fundamental, especially when the technology is considered overly complex. On the other hand, it recommends that BC systems (including complementary technologies and organizational tools) be designed with a clear understanding of the specific contextual needs, particularly in terms of the risk of ex-post opportunism, in order to avoid proposing too complex BC systems when simpler configurations would suffice.

Finally, this research suggests that food SC members should not underestimate the potential of BC in fostering a trustworthy reputation. The risk of ex-post opportunism, as perceived by stakeholders, is not solely dependent on whether an organization or a supply chain behaves reliably and maintains a strong reputation for food quality that has been built over time. Rather, it is influenced by the characteristics of the SC tiers and the activities performed (e.g., cultivation versus transportation), as well as the specific attributes of the actors involved (e.g., location). For instance, in the case of international SCs, where importers or foreign consumers may not be familiar with the products, or where potential misconducts are difficult to detect (as in the cultivation phase), the risk of ex-post opportunism is perceived to be high. In these contexts, BC can play a crucial role in safeguarding honest and reliable actors, as those who strictly adhere to guidelines and regulations are protected from unfair competition, and their commitment to public health is valued through a tool that demonstrates their integrity (Pun et al. 2021). Durach et al. (2021), albeit focusing on a different sector, identify 'product quality certification' as the most promising area for BC in terms of the likelihood of BC implementation.

6 | Conclusions, Limitations, and Future Research

Grounded on AT and TOE theories and based on the analysis of eleven principal–agent dyads, where the principal is a food consortium and its agents are the companies in the different supply network tiers, this study proposes a theoretical model (Figure 4) to interpret: Which BC system design configurations are appropriate for addressing the different levels of ex-post opportunism of supply chain members? (RQ1), and what contextual factors influence the use of different BC systems by supply chain member agents? (RQ2).

One important limitation of this study is that the model in Figure 4 does not consider the influence of some contextual variables mentioned in the literature on BC and TOE theory (Table 3). The agents selected in this study showed some common traits, which set precise boundaries for the present study (see Section 4.2.2). However, in general, contextual variables—such as organizational readiness, agents' perceptions of technology maturity, or compatibility with a company's existing technologies—can affect BC adoption and should be investigated in future studies. Another area for further research is to understand whether the focus on other sectors and countries might highlight different influencing variables (e.g., mimetic pressure or technological barriers as Internet connection).

In addition, the BC systems investigated do not represent all the possible existing BC systems. Future research could extend the analysis on the level of system trust of BC systems by considering further differentiating features, such as the use of AI.

A further limitation relates to the nature of the ex-post opportunism issue (Lumineau and Oliveira 2020). During the interview process, the president and vice president of the consortium discussed the likelihood that an opportunistic event would occur and its consequences and provided the researchers with past examples of agents' opportunistic behaviors. The discussion with all agents focused on understanding where some potential opportunistic behaviors could potentially occur in their activities and in the SC and the monitoring mechanisms that were already in place (e.g., certifications, audits by a surveillance body). However, agents obviously did not disclose any intention to game the system or that there was a conflict between their goals and those of the consortium regarding food safety and quality.

Moreover, dyads and the BC project were observed until a certain point in time, and it would be interesting to explore how the BC use could evolve over time to reach the ideal BC system initially designed. In some dyads, this is challenging, as changes in the regulatory environment can take a long time. In other cases, such evolution could be observed in scenarios in which the principal incentivizes actors who are reluctant to use IoTs or smart contracts. Future longitudinal case studies are also required to understand the dynamics in BC system adoption evolution. On the one hand, the flexibility of adapting a BC system to agents' needs can facilitate its adoption, as the present research supports. Yet, on the other hand, it requires additional costs to the technology provider and the principal, which may explain why in other BC cases (Table 1), principals use one BC system across the supply network.

Finally, the case study investigated did not involve small family-owned fruit stores or neighborhood markets in the downstream network, as it focuses on large-scale retail chains. Future research could investigate the use of BC in these other channels, including differences in terms of food quality and safety as well as ex-post opportunism.

Acknowledgments

Open access publishing facilitated by Universita degli Studi di Padova, as part of the Wiley - CRUI-CARE agreement.

Conflicts of Interest

The authors declare no conflicts of interest.

References

Autorità Garante della Concorrenza e del Mercato (AGCM). 2007. "Indagine Conoscitiva Sulla Distribuzione Agroalimentare (IC/28)." https://www.agcm.it/dotcmsCustom/getDominoAttach?urlStr=192.168.14.10:8080/C12564CE0049D161/0/8D9113CAEBAB738CC12572FB003CE5D3/$File/IC28.pdf.

Agenzia ICE. 2024. "Progetto TrackIT Blockchain." https://www.ice.it/it/blockchain.

Agnihotri, A., and S. Bhattacharya. 2025. *Combatting Counterfeit in Parmigiano Reggiano Cheese Through Blockchain*. In Sage Business Cases. SAGE Publications, Ltd.

Ahmed, W. A. H., B. L. MacCarthy, and H. Treiblmaier. 2022. "Why, Where and How Are Organizations Using Blockchain in Their Supply Chains? Motivations, Application Areas and Contingency Factors." *International Journal of Operations & Production Management* 42, no. 12: 1995–2028.

Antonucci, F., S. Figorilli, C. Costa, F. Pallottino, L. Raso, and P. Menesatti. 2019. "A Review on Blockchain Applications in the Agri-Food Sector." *Journal of the Science of Food and Agriculture* 99: 6129–6138.

Astill, J., R. A. Dara, M. Campbell, et al. 2019. "Transparency in Food Supply Chains: A Review of Enabling Technology Solutions." *Trends in Food Science & Technology* 91: 240–247.

Babich, V., and G. Hilary. 2020. "OM Forum—Distributed Ledgers and Operations: What Operations Management Researchers Should Know About Blockchain Technology." *Manufacturing & Service Operations Management* 22, no. 2: 223–240.

Bai, C., and J. Sarkis. 2022. "A Critical Review of Formal Analytical Modeling for Blockchain Technology in Production, Operations, and Supply Chains: Harnessing Progress for Future Potential." *International Journal of Production Economics* 250: 108636. https://doi.org/10.1016/j.ijpe.2022.108636.

Balci, G., and E. Surucu-Balci. 2021. "Blockchain Adoption in the Maritime Supply Chain: Examining Barriers and Salient Stakeholders in Containerized International Trade." *Transportation Research Part E: Logistics and Transportation Review* 156: 102539.

Behnke, K., and M. F. W. H. A. Janssen. 2020. "Boundary Conditions for Traceability in Food Supply Chains Using Blockchain Technology." *International Journal of Information Management* 52: 101969.

Biswas, B., and R. Gupta. 2019. "Analysis of Barriers to Implement Blockchain in Industry & Service Sectors." *Computers & Industrial Engineering* 136: 225–241.

Bradshaw, J. 2023. "Using Blockchain Technology to Increase Transparency in Agriculture." Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/01/20/using-blockchain-technology-to-increase-transparency-in-agriculture/?sh=76a53c8760b1.

Budler, M., B. F. Quiroga, and P. Trkman. 2024. "A Review of Supply Chain Transparency Research: Antecedents, Technologies, Types, and Outcomes." *Journal of Business Logistics* 45: e12368.

Bumblauskas, D., A. Mann, B. Dugan, and J. Rittmer. 2020. "A Blockchain Use Case in Food Distribution: Do You Know Where Your Food Has Been?" *International Journal of Information Management* 52: 102008.

Caldarelli, G., C. Rossignoli, and A. Zardini. 2020. "Overcoming the Blockchain Oracle Problem in the Traceability of Non-Fungible Products." *Sustainability (Switzerland)* 12, no. 6: 2391–2408.

Cao, Y., Y. Chaoqun, G. Wan, H. Hu, Q. Li, and S. Wang. 2022. "An Analysis on the Role of Blockchain-Based Platforms in Agricultural Supply Chains." *Transportation Research Part E: Logistics and Transportation Review* 163: 102731.

Chang, S. E., Y. C. Chen, and M. F. Lu. 2019. "Supply Chain Re-Engineering Using Blockchain Technology: A Case of Smart Contract Based Tracking Process." *Technological Forecasting and Social Change* 144: 1–11.

Chen, S., X. Liu, J. Yan, G. Hu, and Y. Shi. 2021. "Processes, Benefits, and Challenges for Adoption of Blockchain Technologies in Food Supply Chains: A Thematic Analysis." *Information Systems and e-Business Management* 19: 909–935.

Chod, J., N. Trichakis, G. Tsoukalas, H. Aspegren, and M. Weber. 2020. "On the Financing Benefits of Supply Chain Transparency and Blockchain Adoption." *Management Science* 66, no. 10: 4378–4396.

Clohessy, T., and T. Acton. 2019. "Investigating the Influence of Organizational Factors on Blockchain Adoption: An Innovation Theory Perspective." *Industrial Management & Data Systems* 119, no. 7: 1457–1491.

Clohessy, T., T. Acton, and N. Rogers. 2019. "Blockchain Adoption: Technological, Organisational and Environmental Considerations." In *Business Transformation Through Blockchain*, edited by H. Treiblmaier and R. Beck. Palgrave Macmillan.

Cole, R., M. Stevenson, and J. Aitken. 2019. "Blockchain Technology: Implications for Operations and Supply Chain Management." *Supply Chain Management: An International Journal* 24, no. 4: 469–483.

Creydt, M., and M. Fischer. 2019. "Blockchain and More—Algorithm Driven Food Traceability." *Food Control* 105: 45–51.

Crosby, M., P. Pattanayak, S. Verma, and V. Kalyanaraman. 2016. "Blockchain Technology: Beyond Bitcoin." *Applied Innovation Review* 2, no. 6–10: 7–19.

Danese, P., R. Mocellin, and P. Romano. 2021. "Designing Blockchain Systems to Prevent Counterfeiting in Wine Supply Chains: A Multiple-Case Study." *International Journal of Operations & Production Management* 41, no. 13: 1–33.

Duong, H. A. 2024. *Blockchain Applications in Agriculture: Revolutionizing the Food Supply Chain*. Vernon Presse.

Durach, C. F., T. Blesik, M. von Düring, and M. Bick. 2021. "Blockchain Applications in Supply Chain Transactions." *Journal of Business Logistics* 42, no. 1: 7–24.

Dutta, P., T. M. Choi, S. Somani, and R. Butala. 2020. "Blockchain Technology in Supply Chain Operations: Applications, Challenges and Research Opportunities." *Transportation Research Part E: Logistics and Transportation Review* 142: 102067.

Eisenhardt, K. M. 1989. "Agency Theory: An Assessment and Review." *Academy of Management Review* 14, no. 1: 57–74.

Ellram, L., and W. Tate. 2021. "Cost Avoidance: Not Everything That Counts Is Counted." *Journal of Business Logistics* 42, no. 4: 406–427.

Falcone, E. C., Z. R. Steelman, and J. A. Aloysius. 2021. "Understanding Managers' Reactions to Blockchain Technologies in the Supply Chain: The Reliable and Unbiased Software Agent." *Journal of Business Logistics* 42: 25–45.

Fayezi, S., A. O'Loughlin, and A. Zutshi. 2012. "Agency Theory and Supply Chain Management: A Structured Literature Review." *Supply Chain Management: An International Journal* 17, no. 5: 556–570.

Fosso Wamba, S., M. M. Queiroz, and L. Trinchera. 2020. "Dynamics Between Blockchain Adoption Determinants and Supply Chain Performance: An Empirical Investigation." *International Journal of Production Economics* 229: 107791.

Galvez, J. F., J. C. Mejuto, and J. Simal-Gandara. 2018. "Future Challenges on the Use of Blockchain for Food Traceability Analysis." *Trends in Analytical Chemistry* 107: 222–232.

Gligor, D. M., B. Davis-Sramek, A. Tan, et al. 2022. "Utilizing Blockchain Technology for Supply Chain Transparency: A Resource Orchestration Perspective." *Journal of Business Logistics* 43: 140–159.

Hastig, G. M., and M. S. Sodhi. 2020. "Blockchain for Supply Chain Traceability: Business Requirements and Critical Success Factors." *Production and Operations Management* 29, no. 4: 935–954.

ISMEA. 2023. "Italian Sounding: Quanto Vale e Come Trasformarlo in Export Made in Italy." https://www.reterurale.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/25106.

ISTAT. 2024. "Commercio al Dettaglio." https://www.istat.it/wp-content/uploads/2024/11/CS_Commercio_al_dettaglio_0924.pdf.

Kamble, S., A. Gunasekaran, and H. Arha. 2019. "Understanding the Blockchain Technology Adoption in Supply Chains-Indian Context." *International Journal of Production Research* 57, no. 7: 2009–2033.

Kamilaris, A., A. Fonts, and F. X. Prenafeta-Boldú. 2019. "The Rise of Blockchain Technology in Agriculture and Food Supply Chains." *Trends in Food Science & Technology* 91: 640–652.

Keskin, N. B., C. Li, and J. S. J. Song. 2023. "The Blockchain Newsvendor: Value of Freshness Transparency and Smart Contracts." https://doi.org/10.2139/ssrn.3915358.

Ketokivi, M., and T. Choi. 2014. "Renaissance of Case Research as a Scientific Method." *Journal of Operations Management* 32, no. 5: 232–240.

Kim, H. M., and M. Laskowski. 2018. "Toward an Ontology-Driven Blockchain Design for Supply-Chain Provenance." *Intelligent Systems in Accounting, Finance and Management* 25, no. 1: 18–27.

Köhler, S., and M. Pizzol. 2020. "Technology Assessment of Blockchain-Based Technologies in the Food Supply Chain." *Journal of Cleaner Production* 269: 122193.

Kouhizadeh, M., S. Saberi, and J. Sarkis. 2020. "Blockchain Technology and the Sustainable Supply Chain: Theoretically Exploring Adoption Barriers." *International Journal of Production Economics* 231: 107831.

Kshetri, N. 2018. "Blockchain's Roles in Meeting Key Supply Chain Management Objectives." *International Journal of Information Management* 39: 80–89.

Kurpjuweit, S., C. G. Schmidt, M. Klöckner, and S. M. Wagner. 2021. "Blockchain in Additive Manufacturing and Its Impact on Supply Chains." *Journal of Business Logistics* 42: 46–70.

Lansiti, M., and K. R. Lakhani. 2017. "The Truth About Blockchain." *Harvard Business Review* 95, no. 1: 118–127.

Leong, C., T. Viskin, and R. Stewart. 2019. "Blockchain in Food Supply Chain." https://www.accenture.com/us-en/insights/blockchain/food-traceability.

Li, K., J. Y. Lee, and A. Gharehgozli. 2023. "Blockchain in Food Supply Chains: A Literature Review and Synthesis Analysis of Platforms, Benefits and Challenges." *International Journal of Production Research* 61, no. 11: 3527–3546.

Liao, C., P. Palvia, and J. Chen. 2009. "Information Technology Adoption Behavior Life Cycle: Toward a Technology Continuance Theory (TCT)." *International Journal of Information Management* 29: 309–320.

Lumineau, F., and N. Oliveira. 2020. "Reinvigorating the Study of Opportunism in Supply Chain Management." *Journal of Supply Chain Management* 56: 73–87.

Lumineau, F., W. Wang, and O. Schilke. 2021. "Blockchain Governance—A New Way of Organizing Collaborations?" *Organization Science* 32, no. 2: 500–521.

Lumineau, F., W. Wang, and O. Schilke. 2025. "Reframing Blockchain's Promise: A Commentary on Gregory, Beck, Henfridsson, and Yaraghi's 'Cooperation Among Strangers'." *Academy of Management Review*, in-press (published online: 7 Jan 2025). https://doi.org/10.5465/amr.2024.0375.

Mangla, S. K., Y. Kazancoglu, E. Ekinci, M. Liu, M. Ozbiltekin, and M. D. Sezer. 2021. "Using System Dynamics to Analyze the Societal Impacts of Blockchain in Milk Supply Chains." *Transportation Research Part E: Logistics and Transportation Review* 149: 102289.

Miles, M. B., and A. M. Huberman. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. Sage Publications.

Momani, A. M., and M. Jamous. 2017. "The Evolution of Technology Acceptance Theories." *International Journal of Contemporary Computer Research* 1, no. 1: 51–58.

Morabito, V. 2017. *Business Innovation Through Blockchain: The B3 Perspective*. Springer.

Morgan, T. R., R. G. Richey Jr., and A. E. Ellinger. 2018. "Supplier Transparency: Scale Development and Validation." *International Journal of Logistics Management* 29, no. 3: 959–984.

Orji, I. J., S. Kusi-Sarpong, S. Huang, and D. Vazquez-Brust. 2020. "Evaluating the Factors That Influence Blockchain Adoption in the Freight Logistics Industry." *Transportation Research Part E: Logistics and Transportation Review* 141: 102025.

Pandey, V., M. Pant, and V. Snasel. 2022. "Blockchain Technology in Food Supply Chains: Review and Bibliometric Analysis." *Technology in Society* 69: 101954.

Pilkington, M. 2016. "Blockchain Technology: Principles and Applications." In *Research Handbook on Digital Transformations*, edited by F. X. Olleros and Z. Majlinda. Edward Elgar Publishing.

Pun, H., J. M. Swaminathan, and P. Hou. 2021. "Blockchain Adoption for Combating Deceptive Counterfeits." *Production and Operations Management* 30, no. 4: 864–882.

Rao, S., A. Gulley, M. Russell, and J. Patton. 2021. "On the Quest for Supply Chain Transparency Through Blockchain: Lessons Learned From Two Serialized Data Projects." *Journal of Business Logistics* 42: 88–100.

Richey, R. G., and B. Davis-Sramek. 2021. "Can We Connect? Benefits and Barriers to Adoption of Transformative Technology in Global Supply Chains." *Journal of Business Logistics* 42: 4–6.

Rogerson, M., and G. C. Parry. 2020. "Blockchain: Case Studies in Food Supply Chain Visibility." *Supply Chain Management* 25, no. 5: 601–614.

Saberi, S., M. Kouhizadeh, J. Sarkis, and L. Shen. 2019. "Blockchain Technology and Its Relationships to Sustainable Supply Chain Management." *International Journal of Production Research* 57, no. 7: 1–19.

Schmidt, C. G., and S. M. Wagner. 2019. "Blockchain and Supply Chain Relations: A Transaction Cost Theory Perspective." *Journal of Purchasing and Supply Management* 25, no. 4: 100552.

Sternberg, H. S., E. Hofmann, and D. Roeck. 2021. "The Struggle Is Real: Insights From a Supply Chain Blockchain Case." *Journal of Business Logistics* 42: 71–87.

Stranieri, S., F. Riccardi, M. P. Meuwissen, and C. Soregaroli. 2021. "Exploring the Impact of Blockchain on the Performance of Agri-Food Supply Chains." *Food Control* 119: 107495.

Tapscott, D., and A. Tapscott. 2016. "The Impact of the Blockchain Goes Beyond Financial Services." *Harvard Business Review* 10, no. 7: 2–5.

Thangamayan, S., K. Pradhan, G. B. Loganathan, S. Sitender, S. Sivamani, and M. Tesema. 2023. "Blockchain-Based Secure Traceable Scheme for Food Supply Chain." *Journal of Food Quality* 11: 4728840.

Tiwari, S., P. Sharma, T. Choi, and A. Lim. 2023. "Blockchain and Third-Party Logistics for Global Supply Chain Operations: Stakeholders' Perspectives and Decision Roadmap." *Transportation Research Part E: Logistics and Transportation Review* 170: 103012.

Torky, M., and A. E. Hassanein. 2020. "Integrating Blockchain and the Internet of Things in Precision Agriculture: Analysis, Opportunities, and Challenges." *Computers and Electronics in Agriculture* 178: 105476.

Tornatzky, L. G., and M. Fleischer. 1990. *The Processes of Technological Innovation*. Lexington Books.

Treiblmaier, H. 2018. "The Impact of the Blockchain on the Supply Chain: A Theory-Based Research Framework and a Call for Action." *Supply Chain Management* 23, no. 6: 545–559.

Treiblmaier, H., and A. Rejeb. 2023. "Exploring Blockchain for Disaster Prevention and Relief: A Comprehensive Framework Based on Industry Case Studies." *Journal of Business Logistics* 44: 550–582. https://doi.org/10.1111/jbl.12345.

van Hoek, R. 2019. "Exploring Blockchain Implementation in the Supply Chain: Learning From Pioneers and RFID Research." *International Journal of Operations & Production Management* 39, no. 6–8: 829–859. https://doi.org/10.1108/IJOPM-01-2019-0022.

Voss, C. A., N. Tsikriktsis, and M. Frohlich. 2002. "Case Research in Operations Management." *International Journal of Operations & Production Management* 22, no. 2: 195–219.

Vu, N., A. Ghadge, and M. Bourlakis. 2021. "Blockchain Adoption in Food Supply Chains: A Review and Implementation Framework." *Production Planning & Control* 34, no. 6: 506–523.

Wathne, K. H., and J. B. Heide. 2000. "Opportunism in Interfirm Relationships: Forms, Outcomes, and Solutions." *Journal of Marketing* 64, no. 4: 36–51.

Whipple, J. M., and J. Roh. 2010. "Agency Theory and Quality Fade in Buyer-Supplier Relationships." *International Journal of Logistics Management* 21, no. 3: 338–352.

Woodside, J. M., F. K. Augustine, W. Giberson, F. K. Augustine, and W. Giberson. 2017. "Blockchain Technology Adoption Status and Strategies." *Journal of International Technology and Information Management* 26, no. 2: 65–93. https://doi.org/10.58729/1941-6679.1300.

World Health Organization. 2024. "Food Safety." https://www.who.int/news-room/fact-sheets/detail/food-safety.

Xu, P., J. Lee, J. R. Barth, and R. G. Richey. 2021. "Blockchain as Supply Chain Technology: Considering Transparency and Security." *International Journal of Physical Distribution and Logistics Management* 51, no. 3: 305–324.

Yin, R. K. 2017. *Case Study Research and Applications: Design and Methods*. Sage Publications.

Zamani, E. D., and G. M. Giaglis. 2018. "With a Little Help From the Miners: Distributed Ledger Technology and Market Disintermediation." *Industrial Management and Data Systems* 118, no. 3: 637–652.

Zhao, X., P. Ai, F. Lai, X. Luo, and J. Benitez. 2022. "Task Management in Decentralized Autonomous Organization." *Journal of Operations Management* 68, no. 6–7: 649–674.

Zhu, Q., C. Bai, and J. Sarkis. 2022. "Blockchain Technology and Supply Chains: The Paradox of the Atheoretical Research Discourse." *Transportation Research Part E: Logistics and Transportation Review* 164: 102824.

Zsidisin, G. A., and L. M. Ellram. 2003. "An Agency Theory Investigation of Supply Risk Management." *Journal of Supply Chain Management* 39, no. 2: 15–27.

Zu, X., and H. Kaynak. 2012. "An Agency Theory Perspective on Supply Chain Quality Management." *International Journal of Operations & Production Management* 32, no. 4: 423–446.

Supporting Information

Additional supporting information can be found online in the Supporting Information section.

Appendix 1

Research Protocol

TABLE A1 | Protocol for the interviews.

Introduction	• Presentation of the research motivations and research team • Data confidentiality, research consent, and permission for recording
Interviewee general information	• Could you describe your current role and responsibilities within the company/consortium, and your years of experience?
Company/ consortium information	• Could you describe the history of the company/consortium and its mission? • What is the size of the company in terms of full-time employees and its annual revenue? • What is the size of the consortium in terms of associates? • How is the company/consortium positioned in the market? • What are the different activities/processes carried out? • What type of products or services does the company offer to the market? • Who are the main customers and suppliers of the company and where are they located? • What type of relationship does exist between the consortium and the SC actors? • Is there any contractual agreement between the consortium and the SC actors? What is the content of the contract?[a] • What type of opportunistic behaviors can occur that can compromise food quality and safety? Which phases in the SC can be viewed as the most critical in this regard? Why?[a] • Is any product quality control carried out within your company? In what SC phases is the products' quality currently controlled?[a] • Who is responsible in case of final product quality issues? Has the consortium any visibility on your internal processes today? Has the consortium visibility on SC actors today?[a]
BC system-related information	• How does the food industry perceive BC technology? • When did the project start? • What are the SC actors currently involved in the project and the ones that are not? What are the structure and characteristics of the supply network? • What are the reasons behind the consortium decision to promote the adoption of a BC system? What were the expected benefits? • What are the reasons behind the decision of the company to adopt the BC system? What were the expected benefits? • What benefits does the developed BC system promise to bring in terms of food safety, quality, and integrity? • To what degree does the top management understand the importance of BC for the company and support its adoption? • What are the reasons which led the SC actors to adopt the BC system? Which companies were the hardest to involve in the project? • Are there skilled employees within the SC actors with expertise on BC? Did the SC actors have an adequate network infrastructure for BC system implementation? • Has the company skilled employees with expertise on BC? An adequate network infrastructure for BC system implementation? • Could you describe the implementation process, the SC actors' processes involved, the required changes in the current activities, etc.? How long did the BC system implementation process take? • Have SC actors faced implementation hurdles or other types of difficulties? • Can you describe the BC system adopted? Is it public, hybrid or private? What are its main characteristics (e.g., degree of data visibility, immutability, veracity, data reading etc.)? Is the BC technology complemented by other technological tools, such as smart contracts, AI, or IoT? What are the characteristics of the latter? How are they used? What is the traceable unit? Is information detailed at the lot level? • Was the BC system proposed by the TP and the consortium adapted to SC actors' needs? What are the changes and the reasons behind them? Why the consortium originally designed a specific BC system? To what degree did SC actors find the proposed BC system complex? • What are the main costs related to BC system implementation and use? Who has covered costs? Has the project been financed by the government? • Are there some national norms or rules that regulate/restrict the adoption of BC systems by some SC actors? • What information is saved on BC by the SC actors and which data is made accessible to the consortium? • What type of information is publicly accessible to everyone? • How is the problem of data privacy managed? • Is the issue of interoperability taken into consideration? • Is the BC system compatible with the enterprise information systems and business processes currently in use within the SC companies? • How do the SC actors perform data entry? Who is responsible for this process? How can data veracity be assured? Is there any type of control over the gathered data? • What type of label is used to link the products to the related information saved on BC? • How do consumers access information that is saved on BC? • How is information presented to consumers?
Personal questions	• What do you think about the future development of the project? • What do you think are the main hurdles in adapting the BC system to a wider scale? • Do you have any other remarks or questions? • Could you provide us with additional documentation related to the project?

[a]Questions useful to derive information on the risk of ex-post opportunism.

TABLE B1 | Data reduction and operationalization (BC systems variables).

	BC System variables	
Variable	**Definition**	**Rating**
Permission model	Property of BC systems that determines the permission of accessing BC transactional information and the degree of information immutability.	*Private*: Access to information is restricted by a single validator to only a preselected number of authorized users. It offers low guarantees of data immutability by design. *Hybrid*: Access to information is managed by the network member who uploads the data, who can decide which transactions will be publicly accessible and which ones private, hence restricted to certain users. It offers high guarantees of data immutability by design.
Data entry	Process of data collection and transcription into BC using an electronic or mechanical device.	*Human*: Data is collected by human operators who periodically transcribes it on BC manually using an input device, such as a keyboard or a mobile phone. It is prone to data quality issues, such as time delays, input errors, and intentional manipulations. *Human + IoT*: Data is collected both by human operators and IoT sensors and the subsequent transcription on BC is performed both periodically through manual entry or automatically by using IoTs that directly upload data on BC. Human intervention is reduced but not eliminated; hence, the risk of data quality issues is only partially mitigated. *IoT*: Data is collected automatically by using IoT sensors that directly transcribe it on BC. Human intervention is eliminated; hence, the risk of data quality issues is severely mitigated.
Third-party certification bodies (TPCB)	Involvement of third-party certification bodies that carry out on-field audits to ensure the quality of the data collected and transcribed, both by humans and IoT sensors, into BC.	*No*: Trusted third-party certification authorities are not involved. *Yes*: Trusted third-party certification authorities are involved to perform regular audits and verify the correctness of human data entry as well as IoT sensors proper functioning and calibration.
Smart contracts	Computer programs based on BC data that automatically execute certain actions when pre-defined conditions are met.	*No*: Smart contracts are not implemented. *Yes*: Smart contracts are implemented to automate one or more activities of a certain process based on information that is saved on BC.

Appendix 2

Data Reduction and Operationalization

TABLE B2 | Data reduction and operationalization (contextual variables).

Contextual variables				
Dimension		**Variable**[b]	**Definition**	**Rating**
AGENCY THEORY		Risk of agent's ex-post opportunism	Risk that the agent acts in its own self-interest at the expenses of the principal. It is determined using a risk matrix (Figure 3) that considers both the likelihood that an event occurs and the resulting detrimental impact for the consortium, with a focus on product quality, safety, and authenticity (Zsidisin and Ellram 2003).	*Low*: The risk of opportunistic behaviors is low. *Medium*: The risk of opportunistic behaviors is medium. *High*: The risk of opportunistic behaviors is high.
TOE	TECHNOLOGICAL	Technology complexity[a]	Degree of difficulty perceived by the agents of implementing the BC system proposed by the consortium.	*Low*: The agent perceives a low difficulty in implementing and using the BC system. *Medium*: The agent perceives medium difficulty in implementing and using the BC system. *High*: The agent perceives high difficulty in implementing and using the BC system.
		Relative advantage[a]	Difference between tangible and non-tangible benefits perceived by the agent and the efforts/costs required to implement and use the BC system proposed by the consortium (Clohessy et al. 2019).	*Low*: The agent perceives the BC system as providing a low benefit considering the effort required for its adoption and use. *High*: The agent perceives the BC system as providing a great benefit considering the effort required to its adoption and use.
	ORGANIZATIONAL	Organizational size	Size of the agent in terms of total number of full-time employees (Clohessy et al. 2019).	*Small*: The agent has fewer than 50 employees. *Medium*: The agent has between 50 and 249 employees. *Large*: The agent has more than 250 employees.
		Top management support[a]	Degree of involvement, support and enthusiasm of the agent's top management towards the BC system proposed by the consortium (Clohessy et al. 2019).	*Low*: The agent's top management is reluctant to adopt the BC system, since it does not recognize the value for the company considering the effort/costs associated with its implementation and use. *High*: The agent's top management is willing to adopt the BC system, since it recognizes its value for the company compared with effort/costs associated to its implementation and use.
	ENVIRONMENTAL	Government or contractual incentives	Financial incentives granted by the government to the agent to support the implementation of the BC system or any incentive included in the agent-principal contract (Clohessy et al. 2019; Caldarelli et al. 2020; Kouhizadeh et al. 2020). For instance, some agents could benefit from resources granted by the Italian government to the consortium for BC implementation (government incentives). When needed, they could also use TPCB services by contract for free (contractual incentives).	*Yes*: The agent receives financial incentives from the government or incentives included in the agent-principal contract to adopt the BC system. *No*: The agent does not receive financial incentives by the government or incentives included in the agent-principal contract to adopt the BC system.
		Regulatory environment	Set of laws and regulations influencing BC use in the geographical area where the agent operates (Clohessy et al. 2019).	*Italy*: Laws and regulation do not condition BC systems *China*: Laws and regulation can influence BC systems and in particular favor the use of the Chinese national BC.

[a]This factor refers here to agents' perception of the BC system design proposed by the consortium.
[b]TOE factors that held constant across dyads were excluded from this analysis (see Supporting Information: "Sample controls and research boundaries").