Designing blockchain systems to prevent counterfeiting in wine supply chains: a multiple-case study

Pamela Danese and Riccardo Mocellin
Department of Management and Engineering, University of Padova, Padova, Italy, and
Pietro Romano
Polytechnic Department of Management and Architecture (DPIA), University of Udine, Udine, Italy

Received 7 December 2019
Revised 3 June 2020
14 October 2020
6 January 2021
Accepted 13 January 2021

Abstract

Purpose – The purpose of this paper is to contribute to the debate on blockchain (BC) adoption for preventing counterfeiting by investigating BC systems where different options for BC feeding and reading complement the use of BC technology. By grounding on the situational crime prevention, this study analyses how BC systems can be designed to effectively prevent counterfeiting.

Design/methodology/approach – This is a multiple-case study of five Italian wine companies using BC to prevent counterfeiting.

Findings – This study finds that the desired level of upstream/downstream counterfeiting protection that a brand owner intends to guarantee to customers through BC is the key driver to consider in the design of BC systems. The study identifies which variables are relevant to the design of feeding and reading processes and explains how such variables can be modulated in accordance with the desired level of counterfeiting protection.

Research limitations/implications – The cases investigated are Italian companies within the wine sector, and the BC projects analysed are in the pilot phase.

Practical implications – The study provides practical suggestions to address the design of BC systems by identifying a set of key variables and explaining how to properly modulate them to face upstream/downstream counterfeiting.

Originality/value – This research applies a new perspective based on the situational crime prevention approach in studying how companies can design BC systems to effectively prevent counterfeiting. It explains how feeding and reading process options can be configured in BC systems to assure different degrees of counterfeiting protection.

Keywords Blockchain, Case study, Counterfeiting, Supply chain

Paper type Research paper

1. Introduction

Some characteristics of blockchain (BC) technology – namely, immutability, transparency, traceability, data security and disintermediation – make it particularly appropriate for addressing the counterfeiting of physical products (Alzahrani and Bulusu, 2018; Galvez *et al.*, 2018). Policymakers and public agencies are seeking to assess and exploit these potential benefits. The EU Intellectual Property Office, as part

Funding: This research is funded by Fondazione Cassa di Risparmio di Padova e Rovigo.

International Journal of Operations & Production Management
Vol. 41 No. 13, 2021
pp. 1-33
Emerald Publishing Limited
0144-3577
DOI 10.1108/IJOPM-12-2019-0781

of a broad EU strategy to create a BC ecosystem, has recently launched a forum to encourage the development of BC implementations aimed at combatting counterfeiting (EUIPO, 2019). An additional aim is to determine whether BC could overcome the limits of existing anti-counterfeiting measures in ensuring compliance with food quality standards and EU directives, especially given that several recent food scandals (e.g. the UK's horsemeat incident and the USA's *salmonella* outbreak in peanut butter) indicate that mechanisms currently used are not sufficient to ensure food safety and integrity (Ali *et al.*, 2017). These scandals have shaken consumers' confidence in the guarantees traditionally offered by the food sector, as demonstrated by a recent survey of Italian wine consumers, which showed that almost one-third of those surveyed had recently reduced their willingness to pay for wines with protected designation of origin (PDO) marks (Villano *et al.*, 2017).

Several studies of BC pilot projects in different supply chain settings can be found in the literature (e.g. Martinez *et al.*, 2019; van Hoek, 2019), but the investigation of the use of BC to prevent product counterfeiting is still limited, and most publications generally remain at the sense-making/exploratory stage or are mainly anecdotally descriptive, conceptual, purely technical or based on secondary data from single cases (Cole *et al.*, 2019). Thus, as emerges from the systematic literature review by Queiroz *et al.* (2019), the assessment of the suitability of BC for addressing product counterfeiting represents an opportunity for SCM research. In particular, most existing research is based on the assumption that the technical characteristics of BC (such as data immutability, distributed consensus mechanisms and transparency) guarantee the accuracy and quality of the data saved and facilitate the ability to retrace the entire (true) transaction history for each product (e.g. Kumar *et al.*, 2020; Martinez *et al.*, 2019). This allows discovery of data manipulations and creates a transactional environment that is hostile to counterfeiting, where buyer-supplier information asymmetries that can favour counterfeiting are radically reduced (Schmidt and Wagner, 2019). Purchases are guaranteed by the BC itself (system trust), and trust in individuals and organisations is not required. Some authors warn about the validity of such assumption in real cases. Even though data are immutably saved on the BC, it is not designed to govern data acquisition, and BC feeding (the transferring of real-world data onto the BC) is a critical security challenge for this type of application (Babich and Hilary, 2019; Creydt and Fischer, 2019). In particular, BC technology provides no protection against data that are intentionally manipulated prior to their validation on the network (Schmidt and Wagner, 2019). Moreover, reading information from the BC is an issue because the information accessed by consumers on a certain product may be stored off-chain or may not actually refer to that specific product, given that commonly used smart labels can easily be cloned and then re-applied to counterfeited products (Lo *et al.*, 2019; Kumar *et al.*, 2020).

From the above, the core technical characteristics of BC technology do not necessarily assure effective counterfeiting protection if not complemented by a coherent set of measures for BC feeding and reading processes (i.e. a BC system). Although no study exists that offers an organic view of BC feeding/reading measures, scholars have described several options, ranging from artificial intelligence (AI) (Roeck *et al.*, 2020) and using third-party certification bodies to verify input data (Creydt and Fischer, 2019), to the use of the IoT to ensure high-quality and objective data collection (Kamble *et al.*, 2019) in BC feeding and from the commonly used tagging technologies (e.g. barcodes and QR codes) to the highly secure smart labels, such as NFC tags, which use data encryption (Alzahrani and Bulusu, 2018) in BC reading. However, the literature still lacks a clear operationalization of the BC system construct, as well as a complete overview of all the relevant variables that can be used to design a BC system. Moreover, by mentioning the potential implementation issues of some choices (e.g. QR codes vs NFC tags or manual vs automatic data entry), previous studies (e.g.

Galvez *et al.*, 2018; Alzahrani and Bulusu, 2019; Azzi *et al.*, 2019; Lo *et al.*, 2019) implicitly suggest that the different feeding/reading options used to complement the core BC technological properties can assure protection against counterfeiting to different extents, but again the view remains fragmented.

Therefore, the present research intends to contribute to the debate on BC as a counterfeiting prevention measure by investigating the following research question (RQ): "*How can BC systems be designed to effectively prevent counterfeiting?*". In particular, this paper applies the situational crime perspective to study this phenomenon, as it can help in the exploration of counterfeiting mechanisms and the design of anti-counterfeiting measures by focusing on the reduction of physical opportunities for crime and the increase of opportunities for offender identification (Spink *et al.*, 2013).

To answer the research question, we cross-analysed five case studies of BC adoption in the wine sector, which represents an ideal setting for various reasons. First, wine is one of the most counterfeited food products, as confirmed by several scandals, such as the Italian case of Brunello and Rosso di Montalcino (Villano *et al.*, 2017) and the Côtes-du-Rhône fraud case in France (Vinex, 2020). Threats of lost revenue, image and customer trust have driven winemakers to adopt anti-counterfeiting measures and, in some pioneering cases, to launch exploratory pilot BC projects. Second, BC feeding and reading are crucially important in the wine industry, as counterfeiting can pose serious health risks for customers who depend on assurances of the origin and authenticity of products they buy. Third, these guarantees of product origin and compliance to process specifications are also essential for intermediaries – such as wine importers, distributors, resellers, specialized wine shops and hotel and catering service providers – since counterfeited products detected by customers are among the major causes of legal disputes or damage to companies' reputations.

This research contributes to the BC research field in several ways, providing interesting implications for academics and practitioners. First, by starting from the BC literature and comparing real BC implementations, it identifies the critical variables characterizing a BC system and assesses the ability of the different feeding and reading options in protecting against counterfeiting. This is novel in the BC field, as most previous studies, although acknowledging that there are different options for BC feeding and reading (e.g. Alzahrani and Bulusu, 2018; Kamble *et al.*, 2019), focus on the features of BC technology (such as immutability, transparency and data security) and their value in guaranteeing system trust. This research instead helps to develop a clear operationalization of the BC system construct, which is lacking in the literature, and a more in-depth understanding of the level of counterfeiting protection provided by different BC system options. As recommended by several studies (Risius and Spohrer, 2017; Constantinides *et al.*, 2018; Pereira *et al.*, 2019), this research is not limited to the technical aspects of BC feeding/reading (e.g. smart labels or AI) but considers both technology- and process-related decisions in designing a BC system and their power in countering counterfeiting. Finally, this research contributes to the wider debate on the efficacy of different anti-counterfeiting measures (see, for example, Apte and Petrovsky, 2016; Biswas *et al.*, 2017; Alzahrani and Bulusu, 2018), laying the basis for a more rigorous and objective comparison between existing solutions and BC.

The remainder of this paper is organized as follows: Section 2 presents some theoretical underpinnings of the design of anti-counterfeiting measures, an overview of approaches to preventing product counterfeiting and a review of the relevant literature on BC systems. The research methodology is explained in Section 3; case analyses follow in Section 4. Section 5 discusses the results and provides theoretical and managerial implications. Finally, Section 6 summarizes the study findings and limitations and outlines further research opportunities.

2. Literature review

2.1 Designing anti-counterfeiting measures: theoretical underpinnings

In the literature, various definitions and nuances of product counterfeiting can be found, such as adulteration, tampering and simulation (Spink *et al.*, 2013). Counterfeiting also includes cases where fraudsters do not follow the regulatory definitions of good manufacturing practices (GMPs), good agricultural practices (GAPs) or good hygiene practices (GHPs). According to the World Trade Organization (WTO, 2020), counterfeiting is characterized as the misrepresentation of the identity or the source of products to deceive the purchaser into believing that he/she is buying the original goods. While the literature provides a wide variety of measures to mitigate counterfeiting (see Section 2.3), there is little theoretical development of the "chemistry" of the counterfeiting phenomenon, with the exception of the situational crime prevention approach (Spink *et al.*, 2013). According to this theory, it is by restricting the offender's opportunities for infringement (i.e. addressing the "fraud opportunity structure") that an effective prevention of counterfeiting can be fulfilled. Thus, anti-counterfeiting measures should be designed by considering to what extent the decision-maker intends to suppress the impulse to offend. The effectiveness of measures to prevent counterfeiting can be evaluated by considering that crime is the result of a choice: more effective measures are those that deter or detect intentional infringements because offending appears less feasible or attractive (for instance, because it is easier to intercept a counterfeited product or to identify the counterfeiter). Basically, the situational crime prevention approach suggests two partially overlapping ways of restricting the offender's opportunities: (1) physically reducing opportunities (e.g. steering wheel locks are a good visual deterrent for car thieves and home security systems discourage burglaries) and (2) increasing the chances of being identified (e.g. the obligation to wear crash helmets significantly reduced thefts of motor-cycles, as thieves could be easily spotted by the police).

Situational crime prevention also establishes that the understanding of the fraud opportunity structure requires a wide-ranging awareness of the vulnerabilities of the various supply network processes, ideally including sourcing, production, distribution, retail and, in extreme situations, final disposal or reuse of packaging material (Speier *et al.*, 2011; Spink *et al.*, 2013). Since the fraud opportunity structure is significantly different in the steps before vs those after the producer sells the product, in this paper, we distinguish between "upstream counterfeiting", which concerns sourcing and production activities, and "downstream counterfeiting", which concerns distribution and retail activities. Non-compliance with compulsory international or national production specifications and with product and production process characteristics declared by the company (e.g. use of vulnerable workers, failure to employ of bio, vegan, eco-friendly agricultural or production practices) are forms of upstream counterfeiting. Some practical cases are the production of drugs with no or few active ingredients or the use of substandard aftermarket parts for automobiles or aircrafts (Hopkins *et al.*, 2003). In downstream counterfeiting, the fraud opportunity structure is different. For instance, in the wine industry, counterfeiting can emerge after the wine company sells a bottle and takes the form of fake labels, bottle relabelling or refilling with cheaper wines. The recent large-scale wine scam uncovered by French anti-fraud bodies, in which a merchant tried to sell more than 48 million litres of wine falsely labelled as Côtes-du-Rhône, is an example of downstream counterfeiting (Vinex, 2020).

The situational crime prevention perspective was applied to our research setting where the decision-makers are brand owners who use BC as a measure that deters or detects intentional infringements and also as a traceability and communication tool that allows customers to autonomously verify that the products they buy are not affected by upstream and/or downstream counterfeiting. In this setting, the prevention of counterfeiting is pursued by deterring upstream supply network members from non-adherence to origin, production or

quality control specifications (both compulsory and declared) and deterring downstream members from manipulating original goods during distribution and retail. Thus, in this paper, we assume that the desired level of upstream or downstream counterfeiting protection the brand owner intends to guarantee to customers through BC, by setting precise requirements in terms of restriction of the offender's fraud opportunity structure, is the key driver in the design of their BC systems.

2.2 Measures to prevent product counterfeiting

We identify three broad categories of approaches that companies use to mitigate product counterfeiting: product/packaging-related, customer information/education-related and process-related measures. Table 1 offers a short description of each measure together with its weaknesses and classifies each of these on the basis of its suitability to address upstream and/or downstream counterfeiting.

Like track-and-trace systems, BC can be considered a measure to prevent both upstream and downstream counterfeiting (Schmidt and Wagner, 2019). Unlike the other measures and in common with traditional track-and-trace systems, it allows customers to autonomously verify the authenticity of each product without the need to involve specific equipment/competencies or perform destructive chemical/physical/organoleptic analyses. The literature emphasizes BC's capability to overcome the limits of traditional track-and-trace systems (e.g. risk of data manipulation or the poor quality of input data) thanks to its inherent features, such as transparency and decentralized and immutable data storage (Alzahrani and Bulusu, 2019; Saberi *et al.*, 2019). However, since companies adopt different BC feeding and reading options (Section 2.3), a precise and objective comparison between BC and existing counterfeiting approaches, in particular track-and-trace systems, would require a clearer understanding of the different BC system configurations and their advantages compared to traditional track-and-trace systems.

2.3 Blockchain systems

Although most studies recognise that BC's potential for preventing counterfeiting depends on its technical characteristics (immutability, transparency, etc.) (Wang *et al.*, 2019), a growing number of authors are discussing different BC feeding and reading options to complement BC technology and their implications for counterfeiting. A major issue concern is ensuring the quality of the input data. According to Creydt and Fischer (2019) and Bumblauskas *et al.* (2020), there is currently no universal solution for BC feeding. The potential of BC technology for preventing product counterfeiting can be improved by additional security measures and associated technologies that protect against the risk of human error and potentially dishonest behaviours, thus ensuring that the data that are entered into the BC are of a higher quality (van Hoek, 2019). Drawing on the assumption that information captured by humans can be subjective and unreliable, Roeck *et al.* (2020) suggest pairing BC with AI to identify patterns across manually entered data that may indicate anomalies or inconsistencies. The integration of BC and AI is recommended by several SCM scholars, although the empirical evidence for a combination of these technologies is still limited to a few early use cases (Kshetri, 2018; van Hoek, 2019; Wamba and Queiroz, 2020). Other studies consider the involvement of neutral third-party certification bodies to carry out field audits and verify data quality before they are manually saved (Creydt and Fischer, 2019). Commenting on this feeding measure, Kamilaris *et al.* (2019) argue that the need for such intermediaries may compromise the building of decentralized trust for BC technology. An increasing number of studies suggest the use of IoT sensors to automatically enter data to ensure that the feeding process remains objective by eliminating human interaction and the risk of input errors or fraudulent behaviours (Creydt and Fischer, 2019; Kamble *et al.*, 2019;

Table 1.
Traditional anti-counterfeiting approaches

Type of counterfeiting	Anti-counterfeiting measure	Description	Main weaknesses
Downstream counterfeiting	*Product/packaging-related measures*	Measures aimed at making the replication of original products or packaging more complex and expensive. They include overt technologies (e.g. holograms, watermarks and seals), covert technologies (e.g. machine-readable ink and hidden printed messages) and products/packaging upgrades (Li, 2013)	(1) Unsuitability for average users: product authentication can require specific equipment, training, or the involvement of trained inspectors, such as public or private certification bodies or law enforcement services (Li, 2013) (2) Packaging cloning: these measures can be subject to cloning and reuse on counterfeit products (Pustjens *et al.*, 2016) (3) No protection against upstream counterfeiting*: these measures do not prevent potential unfair practices, such as food adulteration and non-compliance with compulsory production specifications
	Customer information/ education-related measures	Measures aimed at informing final customers, intermediaries (e.g. distributors and resellers) and public agencies about how detrimental counterfeiting is and educate to autonomously distinguish between authentic and counterfeit products (Stevenson and Busby, 2015)	(1) Unsuitability for average users: these measures cannot be applied for those goods for which costumers cannot be educated to autonomously distinguish genuine from counterfeit products (e.g. drugs, wine) (Lybecker, 2007) (2) No protection against upstream counterfeiting: these measures do not educate customers to recognize if unfair practices occurred before the product is sold
Upstream counterfeiting	*Process-related measures: on-field audits*	Measures aimed at authenticating product consistency with production regulations by means of external auditors that collect on-field evidence. They include analysis of documentation processes as well as chemical/physical/organoleptic analyses (e.g. laser surface, DNA, isotopic, etc.) (Berman, 2008)	(1) Unsuitability for average users: the authentication of product consistency with production regulations is carried out by experienced external bodies and analyses may require laboratory testing or special equipment (Berman, 2008) (2) Analysis limited to samples: these measures can generally verify the authenticity of only a limited subset of items (Pustjens *et al.*, 2016) (3) No protection against downstream counterfeiting: these measures do not prevent counterfeiting after a product is introduced on the market.

(*continued*)

Type of counterfeiting	Anti-counterfeiting measure	Description	Main weaknesses
Upstream and downstream counterfeiting	*Process-related measures: track-and-trace systems*	Measures aimed at providing detailed information on product provenance and respect of safety/quality requirements, thus guaranteeing authenticity (Biswas *et al.*, 2017). They generally use common smart labels (e.g. QR codes and barcodes) as well as high-tech labelling (e.g. NFC and RFID tags) that allow users to easily access product-related information via their smartphones (Creydt and Fischer, 2019)	(1) Tags cloning: smart labels commonly used by these systems can be subject to cloning and reuse on counterfeit products (Lo *et al.*, 2019) (2) Manipulation of product-related information: these systems are vulnerable to information manipulation after data entry because data is stored on centralized servers that allow modifications (Biswas *et al.*, 2017) (3) Poor quality of the input data: track-and-trace systems can be fed with information that does not reflect reality if no specific activities and controls are carried out to verify data-entry quality

Note(s): *With the exception of those seals that need regulatory approval and can be issued only after on-field audits (e.g. "PDO" marks, "DOCG" wine labels), which provide assurances against upstream counterfeiting

Table 1.

Bumblauskas, 2020). Moreover, the IoT would eliminate the delay between data collection and data recording, which is an issue for manual entry (Zelbst *et al.*, 2019). In this last case, periodical data transmission after data collection is a common practice to avoid network congestion and higher transaction costs (Zhang *et al.*, 2020).

A further set of options and decisions is related to the security of smart labels that connect physical products to the related information saved on the BC (i.e. BC reading). Lo *et al.* (2019) point out that commonly used smart labels – such as barcodes, QR codes and serial numbers – are vulnerable to attacks, e.g. cloning. In their study, Azzi *et al.* (2019) argue that RFID tags can also be easily cloned, despite their more technologically advanced nature. This view is supported by Lo *et al.* (2019), who maintain that cloned tags contribute to the circulation of counterfeited products in supply chains. Conversely, as outlined by Alzahrani and Bulusu (2018), NFC labels provide greater guarantees of tag cloning and tampering. The security of NFC tags against tampering and replication can be improved using data encryption, although it is an expensive measure (Alzahrani and Bulusu, 2019).

A final critical point related to BC reading, although under-investigated, is that in real cases BC systems usually treat the BC as a backend database behind a centralized web server (Singhal *et al.*, 2018). Although an ideal application that prevents potential manipulations should make information visible to final customers directly from the BC hence ensuring complete decentralization, information displayed through user-friendly web pages or mobile applications is usually stored on external servers that should ideally reflect what is written on the BC. To let customers verify the alignment between the communicated information and that saved on the BC, companies associate this information with the related BC transaction link where the information was originally saved (Montecchi *et al.*, 2019). As clarified by Xu *et al.* (2019), large files (e.g. photos, videos or pdfs) are not stored on the BC due to the technology's limited capacity for handling a large quantity of data; therefore, it is usually preferred to store hash values, namely fixed-length alphanumerical strings unequivocally associated with each document by a secure encryption algorithm. The hash value allows verifying whether the information displayed on the web pages or mobile applications has been manipulated because any change in off-chain data would result in a different hash value from that saved on the BC.

Table 2 summarizes the different options that, according to the literature, could be chosen for BC feeding/reading and some open issues. Although use cases and BC studies contemplate the existence of different configuration choices for BC feeding/reading, they all lack a holistic and in-depth understanding of how a brand owner can design a BC system to assure a certain degree of security in preventing counterfeiting. In particular, there is uncertainty about which variables are relevant to the design of feeding and reading processes and how such variables can be modulated in accordance with the desired counterfeiting protection level. To address these gaps, the present research applies the concept of restriction of the fraud opportunity structure to the field of BC design to unveil the relationships between the degree of protection against counterfeiting a brand owner intends to guarantee to customers and the feeding/reading choices in the design of BC systems.

3. Research methodology

Considering the lack of empirical research on the use of BC to prevent counterfeiting, a qualitative and exploratory approach was chosen for the study. According to Yin (2017), when addressing "how" questions and examining recent or contemporary events, a multiple-case study is a particularly good methodology. Moreover, the purpose of this research is theory building, and research based on case studies facilitates the full understanding of a real-life complex phenomenon in its natural setting as well as the identification of its critical variables and the linkages between them (Yin, 2017).

Feeding/ Reading	Options and issues
Feeding	Data collected and uploaded manually, prone to unintentional human errors, intentional dishonest behaviours and delays (Galvez *et al.*, 2018; Azzi *et al.*, 2019; Creydt and Fischer, 2019; Kamble *et al.*, 2019; Kamilaris *et al.*, 2019; Montecchi *et al.*, 2019; Schmidt and Wagner, 2019; van Hoek, 2019; Zelbst *et al.*, 2019; Bumblauskas *et al.*, 2020). Complementary measures are (1) AI to cross-check data (Kshetri, 2018; Montecchi *et al.*, 2019; van Hoek, 2019; Bumblauskas *et al.*, 2020; Roeck *et al.*, 2020) (2) Neutral third-party bodies to verify data quality (Creydt and Fischer, 2019) Data automatically captured and uploaded on BC by IoT sensors, lowering the risk of input error, unethical behaviours and delays (Azzi *et al.*, 2019; Creydt and Fischer, 2019; Kamble *et al.*, 2019; Lo *et al.*, 2019; Zelbst *et al.*, 2019; Bumblauskas *et al.*, 2020)
Reading	Connection between physical products and related information on BC through: common tagging techniques (barcodes, serial numbers, QR codes, RFID) vulnerable to cloning (Azzi *et al.*, 2019; Lo *et al.*, 2019), or more sophisticated tagging techniques – such as NFC with data encryption – that prevent cloning (Alzahrani and Bulusu, 2018, 2019) Communication to customers: information can be read through websites or mobile applications (Creydt and Fischer, 2019; Montecchi *et al.*, 2019) Information presented to customers can be stored off-chain on a centralized server (Singhal *et al.*, 2018). Customers can access the associated BC transaction (Montecchi *et al.*, 2019)

Table 2.
BC system configuration

3.1 Case selection

We selected cases based on literal and theoretical replication (Yin, 2017). We deliberately searched for companies that showed differences and similarities in terms of the adopted BC systems (e.g. type of smart label, control measures over data, etc.). Furthermore, we attempted to include companies in our sample that adopted BC systems developed by different technological partners currently offering BC systems for the wine sector to present a broader picture of the phenomenon and facilitate the generalization of the results. To identify the cases, we first compiled a list of all the BC systems offered by the technology providers in the wine sector in Italy and of the winemakers involved in the implementation of these solutions. This was made possible by Internet searches and our attendance at several conferences and workshops related to BC technology. Second, we collected publicly available data and information on each BC system to decide whether it might represent an interesting case for the study.

We contacted all technology providers to present the area and purpose of the study, the research team and a brief outline of the interview protocol, and then ascertained their willingness to participate in the study. Subsequently, we identified some winemakers that were exemplar cases in the adoption of BC systems and contacted the CEOs of these winemakers via email, again presenting the team and research and ascertaining their willingness to collaborate. We also promised to give both the technology providers and winemakers the final study report and guaranteed data confidentiality. In the end, all technology providers and five Italian winemakers – pioneers in the adoption of BC technology in the wine sector – agreed to participate in our study. We will refer to the cases and related winemakers with labels from A to E.

Ideally, the unit of analysis for the study would be the supply network involved in the BC system. However, like the majority of BC-based projects at the time of this writing, those selected are in a pilot phase and therefore involve a limited number of actors, as shown in Table 3. In particular, companies C, D and E are fully integrated winemakers, as they are responsible for all production activities from grape harvesting to bottling. Companies A and B rely on external grape suppliers.

Table 3.
Overview of the cases

Case	Supply network members involved	Technology provider	Public BC	Interviewees
A	(1) One grapes supplier (southern Italy) (2) Company A (winemaking, bottling; northern Italy; 500,000 bottles per year)	Large professional service provider that operates globally offering different types of business advisory services for several industries. The group has developed systems based on both private and public BCs for several business applications such as SCM, food traceability, smart insurance, and public financial management	(1) Ethereum	(1) Winemaker's CEO (2) Winemaker's CFO (3) Winemaker's IT manager (4) Technology provider's project manager (5) Grapes supplier's CEO
B	(1) Three grapes suppliers (southern Italy) (2) Company B (winemaking, bottling; southern Italy; 300,000 bottles per year)	Leading global information and communication technology group that is strongly involved in digital innovation projects for public and private market sectors. It is well experienced in developing both private and public BC-based systems for different uses, such as goods traceability, notarization, and ticketing	(1) Ethereum	(1) Winemaker's CEO (2) Winemaker's sales manager (3) Technology provider's project manager (4) CEO of one of the grapes suppliers
C	(1) Company C (cultivation, winemaking, bottling; northern Italy; 200,000 bottles per year)	Global quality assurance and risk management company that provides services for a wide range of industries enabling clients to advance the sustainability and safety of their business. It delivers solutions based on private and public BCs mainly for SCM and secure document storage	(1) VeChain Thor	(1) Winemaker's CEO (2) Winemaker's sales manager (3) Technology provider's project manager

(*continued*)

Case	Supply network members involved	Technology provider	Public BC	Interviewees
D	(1) Company D (cultivation, winemaking, bottling; northern Italy; 150,000 bottles per year)	Italian start-up whose core business is the development of solutions based on the Ethereum BC to track and trace products from vine to dine, with a specific focus on the agri-food sector	(1) Ethereum	(1) Winemaker's CEO (2) Winemaker's sales manager (3) Winemaker's CFO (4) Technology provider's project manager
E	(1) Company E (cultivation, winemaking, bottling; northern Italy; 200,000 bottles per year)	Swiss software house focused on developing systems based on public BCs for the retail industry. It mainly operates in the food and luxury sectors	(1) Ethereum	(1) Winemaker's CEO (2) Winemaker's sales manager (3) Winemaker's CFO (4) Technology provider's project manager

Table 3.

3.1.1 Sample controls and research boundaries. The cases investigated belong to the wine sector and are Italian companies. Controlling for industry and country effects is important in this research, as they can limit choices in designing a secure BC system. In particular, the wine sector exhibits some peculiarities that are worth considering. Many processes are handcrafted, and the IoT, which in general helps to solve critical issues related to BC feeding (Table 2), is difficult to apply. More precisely, it is not suitable for determining whether viticulture and vinification processes are carried out under the requirements of production regulations as many parameters are hard to measure using sensors (e.g. the types of grapes used for vinification and their percentage as well as the type of oak used for ageing). Wine cellars are commonly underground where connectivity is poor and the environment not ideal for the functioning of electronic devices. For these reasons, the issue of BC feeding is particularly challenging in this sector, and finding possible solutions and alternatives is of paramount importance. Similar considerations apply in other industries, generally associated with agriculture, although some environmental parameters can be measured through sensors (Galvez *et al.*, 2018), or in the luxury clothing industry where products are handmade, which makes the investigation and results elaborated in this research of interest in different contexts from the wine sector. In more capital-intensive industries that use automated production lines, such as the pharmaceutical industry, where the IoT can be extensively and easily used, the investigation and results elaborated in the present study are less applicable.

A further research boundary is that the cases investigated are pilot projects that involve few actors. This limits the opportunity to test which BC system choices, among those identified here for designing a secure BC system, are more appropriate in complex supply networks (see Section 6.1).

Finally, as pointed out in Table 3, all cases adopt well-known public BCs, namely Ethereum (4 cases) and VeChain Thor (1 case). Public BCs, compared to private BCs, maintain some core advantages, such as data immutability, decentralized governance, open network access and transaction visibility. Private BCs generally offer enhanced data privacy and transaction writing speed compared to public BCs (Viriyasitavat and Hoonsopon, 2019). Given these differences, we argue that this research is only generalizable to networks using public BCs because the use of private BCs for anti-counterfeiting and how they can be complemented with BC feeding and reading could significantly change.

3.2 Data collection

Data collection took place between October 2018 and May 2019. Semi-structured interviews were chosen as the primary data source because they represent a highly efficient way to gather rich empirical data (Eisenhardt and Graebner, 2007).

We collected information from multiple respondents (Table 3) to capture data from different perspectives, reduce respondents' biases and reach data and theoretical saturation (Bowen, 2008). We decided to interview the winemakers' CEOs. Even if they were not BC experts, they were all directly involved in the pilot projects and were best informed about issues, such as the context, the reasons leading to BC adoption and the expected results. As often happens (even in the more structured wine companies), the winemakers' CEOs also played operational roles in the viticulture and vinification processes as agronomists or oenologists and were also involved in promotion and sales. Then, for each case, we interviewed the project manager of the technological partner to ask for more specific details and empirical evidence to clarify the technical aspects of the BC systems. With the same aim, we also interviewed the IT manager of company A; this role was not present in the other companies. It is worth noting that, in the cases investigated, the decision to adopt a BC system came from the winemaker who, with the support of the technology provider, promoted and guided the BC project. Although they were not directly involved in the decisions about the

design of the BC system, in cases A and B, where the winemakers were not vertically integrated upstream, we also interviewed the CEOs of two grapes suppliers involved in the BC project. As is typical in the wine sector, they were *vignerons*, owners of the vineyards and agronomists expert in grape cultivation. They, therefore, represent key figures in the wine production processes, working closely with winemakers and holding crucial information on cultivation that might be of interest to customers. In case B, given the uniformity in the production activities and in the BC use, we had sufficient information to limit our interviews to one supplier.

We mainly collected data through face-to-face, on-site interviews. For logistical reasons, as suggested by Creswell (2013), we used video conferences with actors located in southern Italy (four interviewees). In total, considering all the respondents of firms and technology providers, 20 interviews were conducted for all cases.

To improve accuracy, each interview was first recorded and then transcribed. Field notes were taken by two researchers to reduce observer's bias. To enhance reliability and validity, an interview protocol was developed based on the existing literature and our research question (Yin, 2017) (see Supplementary File 1). Semi-structured interviews allowed us to create a balance between an open discussion characterized by mutual reflection and knowledge sharing and a more specific questionnaire-based conversation with the aim of finding evidence for research purposes. While all respondents were asked all the questions in the protocol, the level of detail of the discussion on the different points and the focus varied depending on the respondent (Pandey and Patnaik, 2014). For example, when interviewing representatives of the technological providers, we focused on the characteristics of the BC systems, whereas with the winemakers' CEOs, we focused on the firms' internal processes, competitive strategy, etc.

Each interview lasted on average from 90 to 120 min. To validate the information or correct any misunderstandings, we decided to provide interviewees with a structured summary of the interviews' verbatim transcripts, including all relevant information for which feedback was necessary. Providing the respondent with this structured summary, instead of the entire transcript, maximized the probability of getting feedback from him/her, and thus minimized the risk of bias.

Whenever possible, triangulation of information from different sources was used to increase the reliability of the research and the validity of the analysis (Yin, 2017). In addition to interviews, the following secondary data sources were used: (1) official documents provided by the companies and technological partners (e.g. slides of internal presentations), (2) web resources (websites, public interviews) and (3) data gathered from the implemented BC systems. Follow-up phone calls were made to clarify any doubts about the data collected.

3.3 Data analysis

The analysis was carried out in two steps: analysis of within-case data and searching for cross-case patterns (Yin, 2017).

We started the within-case analysis by creating a detailed write-up of each case. Data reduction was then used to summarize the large amount of collected information: we broke down data and characterized each case based on a series of variables that described the different BC systems and the upstream and downstream counterfeiting protections (Tables 4 and 5). We applied the data coding procedure recommended by Yin (2017) to identify variables. As is typical in theory-building case-based research, this process was cyclic and iterative (Voss *et al.*, 2016). Starting from existing research on counterfeiting and BC (Section 2), we identified the relevant concepts in this study and, in particular, based on BC literature, we identified a number of variables potentially useful to distinguish BC systems. While some differences between BC systems clearly emerged from the use cases and BC

Table 4.
Data reduction and operationalization

Variable	Definition	Rating
BC systems		
Data veracity control measures	Actions and/or activities that are taken to prevent, reduce or eliminate the possibility that data saved on the BC does not accurately reflect reality	*No control:* manual data entry with no control carried out to check if the reality has been altered *Artificial intelligence (AI):* manual data entry that is checked through AI to identify any potential mismatches (e.g. between the quantity of harvested grapes and volume of wine produced; between geo-localization of mechanical grape harvesters and date of grape harvesting; between weather conditions and date of grape harvesting) *Third-party certification bodies (TPCBs):* on-site data collection and entry on the BC by trusted third-party authorities
Data-entry frequency	Frequency of information entering into BC.	*Low:* the time lag between the moment when an event occurs and the moment when the related information is written on the BC ranges between some weeks to several months *Medium:* the time lag between the moment when an event occurs and the moment when the related information is written on the BC ranges between some days to one week *High:* the time lag between the moment when an event occurs and the moment when the related information is written on the BC is less than 24 h
Smart labels + Customer communication channels	Physical identifiers used to link real-life objects (e.g. wine bottles) with the related information saved on the BC, that customers can access through different types of channel	*QR code + Web page:* two-dimensional code, composed of a series of black and white squares, that stores a link to a static stand-alone web page (URL). QR code can be read by mobile devices, using their built-in digital camera, that automatically redirect to the related web page *NFC tag + Mobile application:* sticker or wristband with embedded microchips that store a reference to data saved on the web. It is passive, i.e. does not require a battery. In addition to the encoded UID, it uses specific security mechanisms, such as data encryption, to prevent replicability. It can be read by NFC-enabled mobile devices through the use of a dedicated mobile application that performs data decryption

(*continued*)

Variable	Definition	Rating
Proportion of accessible data for which hashes are saved on the BC	Proportion of the total data accessible by consumers (through a web page or a mobile application) that is linked to BC transactions (for which the related hashes were originally and immutably saved)	*Low:* a small portion of the information provided to consumers is associated with the respective transactions saved permanently on the BC. Data stored off-chain in centralized servers rather than on the BC may be subject to manipulations *High:* most of the information provided to consumers is linked to the respective transactions permanently saved on the BC.
Counterfeiting protection		
Upstream counterfeiting protection	Desired protection level in preventing upstream counterfeiting	*Entry-level:* assurance that the wine has an acceptable quality level, rather than a true assurance of origin (e.g. grape origin) or adherence to special production and processing specifications, in order to ensure customers of wine safety *Medium-level:* assurance above all of the grape origin that has a major impact on wine quality, in order to make customer aware that quality is an important feature of the wine *High-level:* assurance that grapes come from the areas identified by PDO specifications (grape origin) and that production processes adhere to superior production practices, in order to make customers aware of the superior quality level of the wine and the extraordinary of grape origin
Downstream counterfeiting protection	Desired protection level in preventing downstream counterfeiting	*Null:* no protection against relabelling, fake labels and refilling *High-level:* high protection against relabelling, fake labels, and refilling

Table 4.

Table 5.
Within-case analysis

Case	Description	Variable	Rating
BC systems			
A	Data on key activities of cultivation and production processes (e.g. days and kinds of insecticide treatments, harvest calendar, etc.) are collected and stored on the Ethereum BC. Data-entry is merely manual: administrative staff enters information onto the BC using a front-end graphical software interface installed on the devices (e.g. tablets, personal computers) already in use. No investment in new hardware and no changes in operational processes were required	Data veracity control measures	No control
	There is a time lag between the BC transactions timestamp and the time when the concerned events occurred. In many cases, the delay can exceed one month	Data-entry frequency	Low
	A QR code applied to each bottle allows customers to access data. Scanning the QR code with a smartphone camera, customers are directed to a web page where stored information is presented. They can read the specific production batch of each bottle and be acknowledged about the historical background of the wine, details on processes (e.g. where the grapes were grown, the nature of the carried out treatments, etc.) and grapes/wine ownership transfers (detailed at the lot level), as well as additional information about the company	Smart labels + Customer communication channels	QR code + Web page
	Most of the information presented on the website related to cultivation (e.g. kinds of fertilizers, form of breeding, quantity of grapes harvested, water consumption) and winemaking processes (grape variety used, fermentation temperature, quantity of bottles produced, type of tartaric stabilization) is not provided with the link that redirects to the relative BC transactions where the data hashes were initially saved. Moreover, all the photos of the vineyard, cellar, and cultivation activities displayed on the website as well as the product organoleptic characteristics and the information on the geographical context (e.g. vineyard surface area, locations of the vineyard and cellar) are only stored on centralized servers	Proportion of accessible data for which hashes are saved on BC	Low

(*continued*)

Table 5.

Case	Description	Variable	Rating
B	The Ethereum BC is used to store process-related information synchronized with data previously collected and saved on the Italian agricultural information system for reasons of compliance with national wine norms. These data are certified by preliminary checks conducted by third-party certification bodies and prescribed by the Italian legislation	Data veracity control measures	Third-party certification bodies
	Data synchronization between the Italian agricultural information system and BC is almost immediate. Information is generally entered on the BC within 24 h of data collection	Data-entry frequency	High
	Each bottle comes with an NFC tag, applied under the front label, that the buyers can scan with a mobile device. These tags work with additional security functionalities, specifically data encryption and unique, permanent, and read-only serial identifiers (UID). The use of a dedicated application for mobile devices that support NFC technology is required to read the encrypted data saved on the tag. The application is designed to run on iOS and Android and provide the consumer with several types of information (e.g. textual description, photos, videos) about the product, the company, and the wine-making processes	Smart labels + Customer communication channels	NFC Tag + Mobile application
	Most of the presented information, which is specific for every single production batch, has their counterparts saved on BC. In particular, while all the information related to cultivation (e.g. date of harvesting, quantity of grapes harvested) and winemaking processes (e.g. days of soft pressing, quantity of bottles produced) is associated with the relative BC transactions links, the access to videos and photos of vineyards and cellar redirect to external websites not related to BC. As to the product organoleptic characteristics, they are only stored on centralized servers. Instead, information related to geographical context is provided in combination with the links to the associated BC transactions	Proportion of accessible data for which hashes are saved on BC	High
C	The VeChain Thor BC is used to record product-related information concerning the phases from agronomic activities to the bottling of every production batch. Data come from on-site inspections made by the same third-party certification body mandated by the national central control authority that operates to guarantee compliance with Italian wine norms	Data veracity control measures	Third-party certification bodies
	Information is firstly stored in the certification body's servers and then synchronized with BC. The process from data collection to data synchronization on BC usually requires less than a day	Data-entry frequency	High
	An NFC tag is applied to each bottle. A UID is encoded into each tag and data encryption is used. Customers use a dedicated mobile application to scan the NFC tag and access detailed information on products and production processes that is recorded on BC.	Smart labels + Customer communication channels	NFC Tag + Mobile application
	Most of the data accessible to consumers related to cultivation (e.g. date of pruning and harvesting, quantity of grapes harvested), vinification (days of cold maceration, type of barrel used for fermentation, number of bottles produced) as well as the geographical context are described in detail and linked to the associated BC transactions for which the data hashes were originally saved. Only a few of the displayed information – namely certifications and awards of the company, documents related to company commitment to sustainability, wine organoleptic characteristics, bunch thinning percentage – does not have its counterpart stored on BC.	Proportion of accessible data for which hashes are saved on BC	High

(*continued*)

Table 5.

Case	Description	Variable	Rating
BC systems			
D	For each production batch, during the different phases from grapes harvesting to bottling, a large amount of data are manually entered by administrative staff in the platform provided by the technology provider using a dedicated front-end interface. No purchase of new hardware was required. AI checks the correctness of some quantitative data-entered by comparing with data previously uploaded on the platform (e.g. data related to wine production volume is compared with the quantity of harvested grapes; misalignment warns about the grape origin or the bunch thinning percentage, and in turn on wine quality) Moreover, some automatic controls are carried out to prevent data-entering mistakes	Data veracity control measures	Artificial intelligence
	Each new data, before being immutably saved on the Ethereum BC, is stored in the central servers of the technology provider. Then, a notification message is sent to the company asking for confirmation about the data sent. Only when data content is confirmed, data are stored on the BC. If the company finds some inaccuracies in the data, this is deleted, and the transaction not executed. The time period between data collection and the moment when data are entered on BC usually ranges from a few days to one week	Data-entry frequency	Medium
	Each bottle is labeled with a QR code that is connected to its batch. Scanning the QR code with the camera of their mobile device, customers have access to a web page where information is presented	Smart labels + Customer communication channels	QR code + Web page
	Information related to cultivation (e.g. type of insecticide and fungicide treatments, date of winter pruning, date of harvesting) and wine-making processes (days of cold pressing, fermentation mode, quantity of bottle produced) is linked to BC transactions. Only few data related to the company (e.g. received awards) and product characteristics (e.g. alcoholic strength, organoleptic characteristics) are not linked to any BC transaction	Proportion of accessible data for which hashes are saved on BC	High
E	Using a web-based platform, the administrative staff manually uploads information related to each wine, such as digital copies of the certification of geographical origin or documents to demonstrate compliance with production specifications. Information/documents uploaded by the company are not subject to any type of control	Data veracity control measures	No control
	As to process-related information that is saved on the Ethereum BC, there's a significant time lag between transactions timestamp and the moment when the described events occurred, which generally range from some weeks to several months	Data-entry frequency	Low
	The platform generates a specific QR code for each production batch. Each bottle belonging to the batch is then labeled. Customers scan the QR code to access a web page containing all the information provided by the company	Smart labels + Customer communication channels	QR code + Web page
	Only a small portion of the accessible information is linked to the respective BC transactions. In fact, data on awards received by the company, certifications and geographical context are provided with links to BC, whereas most of the information on wine characteristics, cultivation (e.g. type of plants protection treatments, quantity of grapes harvested) and production processes (e.g. quantity of bottles produced, grape variety used) are only presented on the website and saved on centralized servers as well as	Proportion of accessible data for which hashes are saved on BC	Low

(*continued*)

Table 5.

Case	Description	Variable	Rating
Counterfeiting protection			
A	Given the product/price positioning (everyday wines sold at a low price (Wine Folly, 2016)), the company intends to reassure customers about the wine quality to avoid the perception that low price is due to a poor quality and safety. Quality is only a qualifying competitive factor (i.e. one that does not create extra business if the firm improves its performance, but can certainly cause lose business if performance falls below a certain point), thus the company aims to share with customers some information about product origin, cultivation/vinification processes, and quality measures so as to prevent them to assume that low prices mean a not-safe wine that can cause health problems, rather than to provide true empirical evidence of grape origin or adherence to production and processing specifications, since the company does not own special production skills or resources to differentiate from competitors	Upstream counterfeiting protection	Entry-level
	Given to its focused target segment (a relatively small number of national large-supermarkets), the company can exert a rather close control on distribution channels and has never experienced problems due to downstream counterfeiting. In addition, the low price and margins make the diffusion of counterfeit products a not-attractive option for a potential offender	Downstream counterfeiting protection	Null
B	Company B produces weekend wines of high international rating, produced in a famous wine area in compliance with stringent PDO specifications, targeted at customers who enjoy fine wines and are willing to pay a high price (Wine Folly, 2016). Competitive advantage roots on both special resources (i.e. grape suppliers located in an important wine area) and skills (i.e. superior viticulture, winemaking, and quality assurance know-how are needed to produce top-quality crus, create wine blends and be compliant with PDO specifications). The guarantee of genuineness, honesty, and transparency is a prerequisite to be competitive, especially abroad, where the company makes most of the business and the brand is less known. Thus, the company aims to provide consumers with true guarantees that grapes come from the areas identified by PDO specifications and that production processes are effectively conducted as promised. The management is aware of the consequences that false statements could have on customer trust, as shown by the several scandals in the wine sector	Upstream counterfeiting protection	High-level
	Given the target market segment -i.e. international market (more than 50% export), wine Ho.Re.Ca. channels (i.e. restaurants, hotels, bars and catering service providers) including wine specialized shops- and the high-price positioning, the management considers re-labelling, re-filling and, in general, the diffusion of false bottles a serious threat to the company reputation and its business, especially because these fraudulent practices primarily concern foreign markets and more expensive wines. The company aims to make customers confident that the high price they paid is for bottles whose authenticity can be verified	Downstream counterfeiting protection	High-level

(*continued*)

Table 5.

Case	Description	Variable	Rating
C	Company C produces special occasion wines of high international rating, in one of the most important wine areas in compliance with stringent PDO specifications and sold at a premium price (Wine Folly, 2016). Given these product characteristics and the premium-price positioning, the management believes that it's vital to satisfy the customer's desire to know the true story behind each bottle, as only if the company is able to provide genuine information that demonstrates the high value for price ratio the customer will re-buy. Thus, the company aims to provide consumers with true guarantees that grapes come from the areas identified by PDO specification and that production processes truly meet the high-quality standard of quasi-handcraft production on large-scale	Upstream counterfeiting protection	High-level
	Given the target market segment (international wine Ho.Re.Ca. including specialized shops, 60% export) and the premium-price positioning, the management is strongly concerned about illegal reproduction of the company fine wines and considers essential to guarantee the authenticity of each bottle the customer buys. Any failure in assuring the genuineness of wines has a negative impact on the company image and reputation. Thus, the company aims to assure that the very high price they paid is for bottles whose authenticity can be verified	Downstream counterfeiting protection	High-level
D	Business strategy aims at differentiating the product from the traditional everyday wines, by rooting on distinctive resources: owned vineyards located in a special terroir (narrow wine area, morainic hills, unique microclimate) that guarantee a better quality of grapes. The resulting product is a "niche" everyday wine whose slightly higher price than everyday wines is justified by higher quality. This business strategy assumes that even for everyday wines, whose purchase significantly depends on the price, some customers can search for products whose quality level is more than simply "acceptable" and are willing to pay a small extra-price for this additional quality. Obviously, customers/consumers do not pretend that quality levels (and associated guarantees) be comparable to those of more expensive wines. Therefore, for management it is important to make customers aware that attention to quality is higher than that of a typical everyday wine producer and provide assurance (data, pictures, videos on vineyards, and cultivation processes) about the grape origin on which quality differentiation is based	Upstream counterfeiting protection	Medium-level
	Being a recent startup, whose brand awareness is still limited also within the focused target segment it serves (a relatively small number of national large-supermarkets), the company has never experienced problems due to downstream counterfeiting. According to management, the medium-price positioning prevents downstream counterfeiting being fraudulent replica not profitable	Downstream counterfeiting protection	Null
E	Given the product characteristics (everyday wines) and the budget-price positioning (Wine Folly, 2016), the management intends to avoid customers perceive that very low price has been achieved by reducing costs of both raw materials and production quality controls with a negative impact on the wine safety. Although for the company quality is only a qualifying competitive factor (everyday wines purchase depends on the price), the management intends to reassure customers about the wine quality and safety by sharing some information about product origin, cultivation/vinification processes, and quality measures. The key message is "do not worry, we have nothing to hide" rather than "we intend to provide true empirical evidence of grape origin or adherence to production and processing specifications."	Upstream counterfeiting protection	Entry-level
	Given to its focused target segment (a relatively small number of national large-supermarkets), the company can exert a rather close control on distribution channels and has never experienced problems due to downstream counterfeiting. Moreover, the very low price makes illegal reproduction a not significant problem	Downstream counterfeiting protection	Null

studies (Table 2), a clear operationalization of the BC system construct was lacking in the literature. Thus, looking at evidence emerging from the data was fundamental to abductively identifying relevant variables. Identified variables were rated according to precise rules, and again, the comparison of data across cases was central to defining these rules (Section 4.1, Tables 4 and 5).

The result of this coding led to the selection of four variables to characterize BC systems: data veracity control measures, data-entry frequency, smart labels and related customer communication channels and the proportion of accessible data for which hashes are saved on the BC. Two of these variables had already been addressed by previous BC-related studies (i.e. data veracity control measures, smart labels and communication channels), whereas the other two (i.e. data-entry frequency and the proportion of accessible data for which hashes are saved on the BC) had only been briefly mentioned as potential issues in BC implementations (Table 2). Furthermore, by analysing and comparing cases, we distinguished between different desired levels of upstream and downstream counterfeiting protection (Section 4.2, Tables 4 and 5). This was strictly linked to their exposure to the risk of downstream counterfeiting by potential offenders and the extent to which they intended to insure consumers against upstream counterfeiting, guaranteeing that viticulture and vinification activities followed production and quality standards and were as declared.

As suggested by Miles and Huberman (1994), the data were organized in tabular displays (see Section 4), which was useful for both within-case analyses and cross-case comparisons. They comprised two columns: a description of the case broken down into the relevant variables and the corresponding rating of each variable according to the rules of Table 4.

Cross-case analyses were performed by structuring the data as two-variable matrices (Figure 1) to detect commonalities and differences between cases. The results derived from case analyses were then summarized in the form of propositions.

4. Case analysis

4.1 Blockchain systems

Case comparison showed the existence of commonalities as well as differences in the implemented BC systems (see Tables 4 and 5).

In all cases, the data were manually uploaded to the BC, but different measures were adopted to control data veracity: from no control measure in cases A and E, to AI in case D and third-party certification bodies in cases B and C. While these BC feeding options are well-known in the BC literature (Table 2), an important distinction emerged from the cases concerning data-entry frequency, which had received little attention in previous studies. This varied from some weeks/months (low frequency) in cases A and E, to some days/one week (medium frequency) in case D and less than 24 h (high frequency) in cases B and C. This variable appears to be relevant in the characterization of a BC system because it can influence fraud opportunity. In fact, a higher risk of manipulation occurs when data remain unrecorded and vulnerable to modification for a long period.

As to BC reading, cases differ in the use of smart labels and customer communication channels, as expected from the BC literature. In all the examined systems, product-related information displayed to customers through web pages or mobile applications is not taken directly from data saved on the BC. All data are stored on external centralized servers, but customers can verify information provided through the hashes linked to the BC transactions. This is a common practice, especially when uploading large files. However, a significant difference emerged between cases A and E and cases B, C and D, regarding the proportion of data for which hashes are saved in the BC. This has important implications for the level of protection assured by BC technology since a consumer should be able to verify at any time

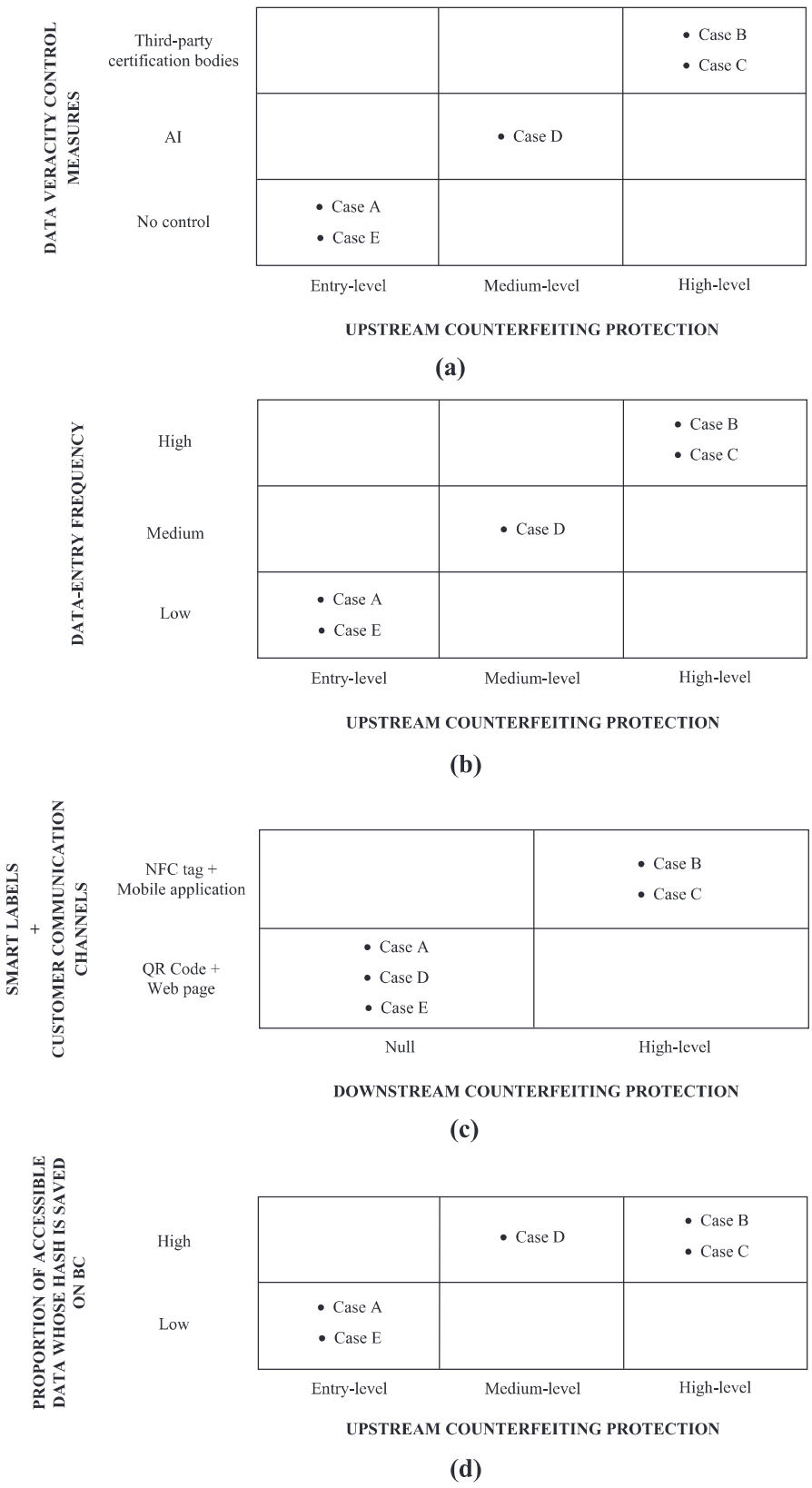

Figure 1.
Cross-case analysis

what information is aligned with data originally stored on the BC to avoid the risk of potential manipulation.

4.2 Upstream and downstream counterfeiting

As emerges from Table 5, cases significantly differ in the desired upstream and downstream counterfeiting protection level. This is strictly linked to their business strategy, namely how they intend to create and maintain their competitive advantage through distinctive skills and/or resources (Mintzberg *et al.*, 1995) and to the risk of downstream counterfeiting depending on their price positioning and target market.

For companies B and C, guaranteeing grape origin, as well as growing and production processes, and product authenticity are of paramount importance. In fact, they own a special know-how related to grape growing and winemaking as well as superior quality assurance skills. They also produce in famous wine areas in compliance with stringent PDO specifications. This results in top-quality wines sold at a very high price, also in international markets. These companies are exposed to the risk of counterfeit copies and thus intend to protect customers against downstream counterfeiting (high level of downstream counterfeiting protection). Moreover, given the special product characteristics, they aim to assure them that wines are produced as declared (high level of upstream counterfeiting protection).

For companies A and E, given the wines they sell (i.e. everyday wines) and consumers they target (i.e. national large supermarkets), there is no real risk of downstream counterfeiting for their products, and thus they are not interested in reducing this risk. They also have no special skills or resources, and thus it is not important for them to provide true empirical evidence of grape origin or adherence to particular production and processing specifications. Instead, they want to reassure customers about the quality and safety of the wine (entry-level of upstream counterfeiting protection).

Finally, for case D, the level of upstream counterfeiting protection the wine producer intends to provide to customers is classified as medium, given its interest in guaranteeing the grape origin on which wine quality differentiation is based. In fact, it produces "niche" everyday wines in a narrow area with morainic hills, and its strategy is based on this distinctive resource, rather than on distinctive production skills. Given the medium-price positioning and target markets (i.e. national large supermarkets), there is no particular risk of downstream counterfeiting (null downstream counterfeiting protection).

4.3 Formulation of propositions

In this study, the data were cross-compared to derive propositions for how BC systems are designed to achieve a desired level of upstream and downstream counterfeiting protection. To this aim, we first investigated the existence of a link between the desired upstream and downstream counterfeiting protection and the BC system variables (Figure 1). Then, based on the situational crime perspective, which identifies the reduction of the fraud opportunity structure as the key driver in the design of anti-counterfeiting measures, we proposed how the desired degree of counterfeiting protection affects the design of BC systems given the varying ability of the system variables to reduce fraud opportunity.

The cross-comparison revealed different clusters of cases with similar patterns. Cases A and E, which aimed for an entry-level protection against upstream counterfeiting and no protection against downstream counterfeiting, took similar decisions in terms of BC systems, namely no control measure for data veracity, a low data-entry frequency, the use of QR codes and web pages as customer communication channel, as well as a low proportion of accessible data for which hashes were saved on the BC. Cases B and C exhibit an opposite pattern. They both desired a high level of upstream and downstream counterfeiting protection and adopted

similar BC systems, with third-party certification bodies as data veracity control measure, a high data-entry frequency, NFC tags and mobile applications as customer communication channel, as well as a high proportion of accessible data for which hashes were saved on the BC.

Finally, case D is similar to cases A and E with their use of QR codes and web pages as customer communication channel, while it differs in its use of AI, a medium data-entry frequency and a high proportion of accessible data for which hashes were saved on the BC. Only this latter characteristic is common to cases B and C. Since case D has commonalities with cases A and E (no desired downstream counterfeiting protection) and differs from all the cases aiming at a medium level of protection against upstream counterfeiting, it appears evident that the precise relationships between the BC system options must be considered through a disaggregated analysis to distinguish between upstream and downstream counterfeiting.

The following proposition summarizes the results of the cross-case analysis at an aggregate level:

P1. Different levels of desired upstream and downstream counterfeiting protection determine different BC systems in terms of (1) data veracity control measures, (2) data-entry frequency, (3) smart label and customer communication channel and (4) proportion of accessible data for which hashes are saved on the BC.

As for data veracity control measures, Figure 1a suggests that the desired upstream counterfeiting protection level is linked to the use of these measures: from no control when an entry-level of protection is required, to the use of AI when it is at a medium level and the use of third-party certification bodies when it is at a high level.

In cases B and C, the relevance of making customers aware of the superior quality level of the wine, grape origin and specific production processes led to the use of third-party certification bodies for data collection and data entry. Interviewed managers agreed that this choice entails higher costs, but judged this the best way to dissuade fraudulent behaviour in their context, as it can be employed to control the veracity of a large set of data ranging from process yields to cleaning, cellar temperature and so on. Both cases B and C share a significant amount of information through BC, from cultivation and winemaking processes to information related to the geographical context. The use of third-party certification bodies can insure customers against the risk of deliberate and intentional manipulation of all declared data. In contrast, company D is mainly interested in providing assurance about the grape origin on which its differentiation is based and thus aims at a medium level of protection to prevent upstream counterfeiting. It adopts AI to detect inconsistencies between some quantitative data (e.g. between hectares cultivated, tonnes of grapes harvested and bottles produced). The existence of inconsistencies means that the wine origin or even quality (e.g. a low percentage of bunch thinning) is not guaranteed; however, their absence offers a certain level of assurance of the use of grapes from declared vineyards. At the same time, AI is ineffective in verifying how some activities have been accomplished (e.g. cleaning of equipment and facilities and proper bottle storage), which is in fact not crucial for a company that aims to differentiate for grape origin rather than production processes. Thus, we can conclude that AI reduces fraud opportunity only to a certain extent and offers a counterfeiting protection level that is lower than the use of third-party certification bodies. Finally, in cases A and E, the desired upstream counterfeiting protection is at an entry-level, as they simply aim to reassure customers that the product quality is acceptable although the price is low, without any interest in providing guarantees for the grape origin or adherence to wine production specifications given that they do not possess distinctive skills and resources. Thus, they do not rely on particular data veracity control measures and can potentially save information on the BC that does not reflect reality. However, the fact that such information is

shared through an immutable traceability technology represents an entry-level discouragement of fraudulent conduct.

Based on this evidence, the following proposition is advanced:

P2. The level of desired upstream counterfeiting protection determines the choice of data veracity control measures in the design of BC systems. To achieve a high level of protection, companies use third-party certification bodies; to achieve a medium level, they use AI; when an entry-level protection is desired no control measures are used.

The pattern in Figure 1b is similar. It relates the desired upstream counterfeiting protection to the frequency of entering process-related information on the BC. Cross-case analysis suggests that companies B and C, aiming for high-level protection, enter data on the BC with a high frequency. In particular, after a first short period where collected information is stored on the certification body's servers or in the Italian national agricultural information system, data are synchronised with the BC. The whole process takes up to 24 h. This minimizes the time between data collection and data entry during which manipulations may occur, thus reducing the fraud opportunities. For company D, which pursues a medium level of protection, process-related data are stored and grouped on the technology provider's servers and undergo a further manual correctness check before being immutably saved on the BC. Then, the set of data is registered in a BC transaction between 24 h and a week after data collection. When the desired protection is at an entry-level – as in cases A and E – companies first use paper registers or electronic files to group information related to production processes. The timestamps of BC transactions show significant time lags for events, which range from one week to several months. In general, a higher data-entry frequency implies higher costs, as the number of transactions increases, as in cases B and C. For these latter cases, given the exclusivity of their products, it is important designing a BC system that offers higher guarantees that no manipulation can occur in the upstream network before on-chain registration, so as to provide customers with strong evidence of their distinctive skills and resources. In summary, we can conclude that the higher the data-entry frequency, the lower the fraud opportunities, as data remain vulnerable to modification for less time. Based on assumptions derived from the situational crime perspective, it follows that a higher data-entry frequency guarantees a higher protection against upstream counterfeiting.

The following proposition encapsulates this evidence:

P3. The level of desired upstream counterfeiting protection determines the choice of data-entry frequency in the design of BC systems. The higher the level of upstream counterfeiting protection desired, the higher the data-entry frequency.

A further relationship represented in Figure 1c links the desired downstream counterfeiting protection to the different types of smart labels and communication channels. Companies A, D and E all use QR codes printed on the wine label, which redirect to web pages. This solution is cheap, but the interviewed managers are aware that it does not significantly reduce downstream counterfeiting opportunities, as QR codes are also easily cloneable (e.g. by scanning the label, printing it and applying it to a fake bottle). However, in all these cases, downstream counterfeiting is not an issue. The target segment and the price positioning (everyday wines) in cases A and E make the risk of products being counterfeited close to zero. Similarly, managers in company D think that this risk is extremely low given the low brand recognition, the medium-price positioning and the targeted market segment. In contrast, in cases B and C, the companies decided to use NFC tags with mobile applications. This solution entailed higher costs because it required the redesign of the labelling process. However, the managers agreed that, unlike the QR codes, NFC tags significantly deter downstream counterfeiting, which was a priority for them. In fact, the NFC tags adopted by companies B and C are difficult to physically remove and provide additional guarantees of non-

replicability, such as the encoded unique identifier (UID), as well as data encryption combined with the associated mobile application that decrypts the hidden data stored in the tag. These measures reduce the opportunities for fraudulent conduct, as they discourage counterfeiters from extracting the reference that redirects customers to the web content related to the genuine product from the original NFC tag and then using this link to replicate the tag. Given the exclusivity of their wines due to their distinctive skills and resources, and the consequent need for high-level protection against downstream counterfeiting, companies B and C designed a BC reading solution that is able to provide customers with a stronger guarantee of non-replicability.

The following proposition encapsulates these findings:

P4. The level of desired downstream counterfeiting protection determines the choice of smart label and customer communication channel in the design of BC systems. To achieve a high level of protection, companies use NFC tags with mobile applications; when no protection is desired, companies use QR codes associated with web pages.

A final important BC system option regards the proportion of accessible data for which hashes are saved on the BC. For companies B, C and D, which aim for a medium or high level of protection against upstream counterfeiting, most of the data shared with customers is related to the hashes saved on the BC (Figure 1d). Companies B and C sell high-priced and exclusive wines with a certified grape origin, and their production is complex and meet high-quality standards. Company D's differentiation relies on grape cultivation in an exclusive *terroir*. They are very committed to assuring customers that the shared information is stored on the BC, which offers a higher guarantee that accessible information has not been manipulated. The aim of these companies is to reduce data manipulation and fraud opportunities by giving customers the opportunity to verify the alignment between the information related to their distinctive resources and/or skills and that saved on the BC. Conversely, companies A and E aim to guarantee an entry-level protection against upstream counterfeiting, as they sell lower priced wines in large-scale supermarket chains and do not rely on distinctive skills and resources. They only share and store information on the BC that is necessary to guarantee that their wines meet the acceptable quality standards, and then share further information without providing the related hash, assuming that customers are not concerned about adherence to declared production processes or grape origin, which is not distinctive. Thus, compared to the other cases, the restriction of fraud opportunity, and thus the protection level against counterfeiting is lower.

The following proposition summarizes this evidence:

P5. The level of desired upstream counterfeiting protection determines the proportion of accessible data for which hashes are saved on-chain in the design of BC systems. To achieve a high or medium level of protection, the proportion is high; when an entry-level protection is desired, the proportion is low.

5. Discussion

The major theoretical contributions of this study are positioned in the research stream on the design and use of BC technology in supply chains (Treiblmaier, 2018; Queiroz *et al.*, 2019; Wang *et al.*, 2019). This research applies the situational crime perspective to investigate how the degree of protection against counterfeiting a brand owner intends to guarantee to customers affects the design of BC systems. The use of widely recognized theories to explore the implications of BC has been advocated by several scholars (Cole *et al.*, 2019; Hald and Kinra, 2019). The interpretation lens of the situational crime perspective, which identifies the restriction of fraud opportunities as the key driver for effective counterfeiting prevention,

made it possible in the present research to advance knowledge on what is necessary for a more secure BC system to prevent counterfeiting.

This research contributes to the operationalization of the BC system concept, including BC reading and feeding options. The previous literature agrees on the general common key features of a BC technology, such as immutability, traceability, disintermediation and consensus mechanisms (Schmidt and Wagner, 2019; Kumar *et al.*, 2020). Past studies and BC use cases also mention and discuss the possibility that BC technology could be complemented by different BC feeding and reading options (Table 2). However, a clear operationalization of the BC system construct is lacking, and in this regard, the value of the present research is twofold. First, the literature review and comparison with real BC implementation cases enabled the identification and codification of four relevant variables that can be used to describe a BC system, namely data veracity control measures, data-entry frequency, smart label and customer communication channel and the proportion of accessible data for which hashes are saved on the BC. Second, the assessment of each BC design option in terms of its protection against upstream and downstream counterfeiting provides researchers and managers with a clearer understanding of the implications of each choice. The situational crime prevention approach (Spink *et al.*, 2013) provided the foundation for the reasoning on the power of each option to prevent counterfeiting by restricting the fraud opportunity structure. Some variables proposed for characterizing a BC system have already received significant attention in the previous literature; for example, data veracity control measures, which can include the use of AI (Kshetri, 2018; Montecchi *et al.*, 2019; van Hoek, 2019; Bumblauskas *et al.*, 2020; Roeck *et al.*, 2020), or neutral third-party bodies for the verification of data quality (Creydt and Fischer, 2019) or smart labels and customer communication channels differentiated by the use of common tags like QR codes associated with a web page (Azzi *et al.*, 2019; Lo *et al.*, 2019) and more sophisticated methods like NFC tags associated with a mobile application (Alzahrani and Bulusu, 2018, 2019). As expected, the present research confirms that decisions on smart labels and customer communication channels are determined by the desired downstream counterfeiting protection level, as they use different security measures (e.g. UID and data encryption) characterized by varying dissuading power against fraudulent actions such as cloning or re-labelling (Alzahrani and Bulusu, 2018). As to data veracity control measures, instead, based on case studies, this research elaborates interesting arguments and novel evidence on the level of protection against upstream counterfeiting that AI can guarantee compared to neutral third-party bodies, which were considered more effective as they allow verifying more information beyond quantitative data. Although this evidence requires further research (see Section 6.1), it may contribute to stimulating a more in-depth investigation of the use of AI to understand under what conditions their potential is fully exploited. This research also identifies two variables characterizing a BC system that received less attention in previous studies: data-entry frequency and the proportion of accessible data for which hashes are saved on the BC. Although the issues of data-entry frequency (Zhang *et al.*, 2020) and the common practice of not making information visible to final customers directly from the BC are mentioned in the BC literature (Singhal *et al.*, 2018), this research is more precise in identifying the differences that can exist between cases, which is important as the ability to reduce fraud opportunities (and thus the upstream counterfeiting protection level) can be significantly affected. Data-entry frequency can vary from data written on the BC from less than 24 h to months, greatly changing the risk of data manipulation. Similarly, when most of the information provided to consumers is linked to the respective transactions saved permanently on the BC, companies are providing customers the opportunity to verify the data, significantly reducing fraud opportunities and providing greater protection against upstream counterfeiting.

Overall, these results further contribute to the research on the design and use of BC technology by emphasizing the importance of the organizational dimension in designing BC

systems. Some authors (Risius and Spohrer, 2017; Constantinides *et al.*, 2018; Pereira *et al.*, 2019) warn about the prevalent focus on the technical aspects of BC (e.g. type of permission model, consensus mechanisms, block structure, etc.) and their interaction with technological tools (e.g. RFID, NFC tags, IoT, etc.), while an investigation from an organizational and managerial perspective is less explored. The present research indicates that some decisions on the processes related to BC feeding and reading, such as the choice of involving third-party certification bodies, the proportion of accessible data for which hashes are saved on the BC and data-entry frequency, are crucial in determining the power of a BC system for preventing counterfeiting.

This study contributes to the debate on the potential of BC technology to guarantee product authenticity in comparison to traditional approaches, both in general and in particular in the wine industry (see, for example, Apte and Petrovsky, 2016; Biswas *et al.*, 2017; Alzahrani and Bulusu, 2018). Previous scholars (e.g. Galvez *et al.*, 2018; Lu *et al.*, 2019) agree that BC might be considered a promising solution for effectively preventing product counterfeiting because of its characteristics, but did not investigate the validity of such an assumption in real cases. The conclusion that different BC system configurations are related to different protection levels against upstream and downstream counterfeiting, the classification of the different BC system options accounting for BC feeding and reading processes and the detailed explanation of how the desired degree of counterfeiting protection affects the design of BC systems pave the way for a clearer and more objective comparison with existing measures for counterfeiting. In particular, our work suggests that BC systems have a wider scope than other measures (except for track-and-trace systems) since each of them is focused on preventing a single type of counterfeiting, whereas BC systems can be used to prevent both upstream and downstream counterfeiting (see Tables 1 and 4). Moreover, this study claims that any comparison between the characteristics of BC systems and other counterfeiting measures should be made at a micro rather than macro level, namely considering the characteristics of each specific BC system. In theory, a measure that only focuses on upstream counterfeiting (e.g. a measure aimed at authenticating product consistency with production regulations using external auditors that collect on-field evidence) could provide higher guarantees than a BC characterized by an entry-level protection against upstream counterfeiting, while only a BC system designed to fully exploit its potential in reducing fraud opportunities both upstream and downstream actually offers a high degree of confidence in the prevention of both types of counterfeiting. Previous studies (Apte and Petrovsky, 2016; Biswas *et al.*, 2017; Alzahrani and Bulusu, 2018) discuss how BC implementation is expected to contrast counterfeiting and overcome some weaknesses of traditional counterfeiting measures (Table 1), by reducing the risk of post-data-entry manipulations and allowing an "average" user to autonomously verify the authenticity of each product without the need to involve specific equipment/competences or perform destructive chemical/physical/organoleptic analyses. This research instead suggests that assessing BC protection levels against upstream and downstream counterfeiting requires careful consideration of BC feeding and reading options since they can influence BC performance in terms of fraud opportunity restriction.

5.1 Managerial implications

This study provides some practical suggestions to properly address the design and use of BC systems.

First, it warns managers against using the BC as a stand-alone technology and instead suggests viewing it as a part of a wider BC system where decisions on technical aspects (e.g. type of smart labels and communication channels, use of AI, etc.) must be complemented with organisational choices regarding BC feeding and reading processes (e.g. third-party

involvement and data-entry frequency). A coherent set of these decisions is crucial to ensuring that data written in and read from the BC accurately reflects reality.

Second, the study suggests that BC systems are not one-size-fits-all solutions and therefore should be adapted to the required upstream and/or downstream counterfeiting protection level. Specifically, the study presents a set of variables that managers should consider when designing BC systems and shows how they can be modulated in accordance with the desired guarantees of product authenticity. Several key learnings for managers can be derived. This research indicates how to design BC systems characterized by a high level of protection against upstream and/or downstream counterfeiting. It also argues that in certain contexts (as in cases A and E), the use of BC systems without particular attention to strict data input and reading measures is a good solution, as they offer some deterrent power against intentional infringements and also operate as traceability and communication tools that allow customers to autonomously verify the safety of products they buy. For instance, in the case of upstream counterfeiting, an entry-level protection is better than no protection since the core technical features of BC technology (e.g. transparency, immutability and traceability) allow the discovery of post-entry manipulation and the detection of the counterfeiter, thus making offending less feasible or attractive. In the case of downstream counterfeiting, no protection can be a viable choice where there is no real risk of downstream counterfeiting (e.g. low price and no brand products).

The third practical contribution is directed towards policymakers who are evaluating the potential of BC vs existing measures to protect consumers, honest producers and national brands from risks due to fraudulent copies or imitations. This study corroborates the advisability of the prudential decisions of many governments to fund BC-based pilot projects to explore the real potential of this technology to defend product authenticity before extending its use on a large scale. However, it also suggests caution in considering BC a *panacea* that overcomes all the weaknesses of existing measures. This study demonstrates that BC systems are versatile, their real potential in reducing fraud opportunities (and defending product authenticity) in comparison with existing measures can vary and that choices on BC feeding and reading determine this variation. Thus, the configuration and management of such processes is crucial to ensure that BC technology is better able to guarantee product authenticity than existing measures.

6. Conclusions

This research represents a first attempt to apply the situational crime perspective to the study of BC systems, with a focus on the different options of BC feeding and reading that complement the use of BC technology. Based on the analysis of five case studies in the wine sector, this paper concludes that the desired upstream and downstream counterfeiting protection level guides decisions on BC system configurations, as their ability to reduce fraud opportunities is variable. In particular, this research advances that the desired upstream counterfeiting protection level determines choices of data veracity control measures, data-entry frequency and the proportion of accessible data for which hashes are saved on the BC; whereas the desired downstream counterfeiting protection level determines decisions on smart labels and customer communication channels. The higher the desired protection level, the more the companies choose those BC options that can reduce fraud opportunities to a greater extent.

6.1 Limitations and future research directions

A first limitation of this study is linked to the characteristics of the cases investigated (Section 3.1.1), which restricts the generalizability of this research and sets precise research boundaries. First, as in most existing BC initiatives, all the examined BC projects are in the

pilot phase and thus involve a limited number of companies and products. Further studies may consider BC system implementations in more complex supply networks. For instance, a possible issue may concern the scalability of the use of third-party physical inspections, as in cases B and C. Whereas cost is not significant in simple supply chains such as those analysed in this study, third-party inspections could become economically unsustainable in more complex supply networks. Second, all the analysed cases apply public BC technologies that differ significantly from private BCs in terms of data immutability and decentralized governance, and thus conceptually in their counterfeiting protection. Further studies of private BCs are needed to understand the effectiveness of their adoption for anti-counterfeiting and whether and how BC systems may differ in terms of BC feeding and reading. Third, as argued in Section 3.1.1, the implementation of the IoT in the wine sector is still a challenge. Future research could investigate the issue of BC feeding in more automated sectors, such as the pharmaceutical sector, to understand the implications of IoT use and its efficacy in solving BC feeding issues. Although several scholars (e.g. Kamble *et al.*, 2019; Bumblauskas, 2020) consider the IoT an effective means of guaranteeing objective data collection and recording, which reduces the risk of human manipulation; others argue that IoT sensors can also be subject to intentional manipulation (Rejeb *et al.*, 2019; Schmidt and Wagner, 2019). In the future, more specific IoT sensors could be developed and spread to appropriately detect important production data, e.g. in the wine cellars. Further research, in the wine or luxury clothing contexts, could investigate the use of the IoT in combination with AI algorithms to support BC feeding. These solutions could eliminate the need for third-party certification bodies for data that are currently not measurable by sensors.

A further limitation of this study is that it assumes the perspective of a brand owner who configures the BC system in line with a desired counterfeiting protection level. Once BC systems become more mature and widely used, it will become essential to consider the buyers' perspective, in particular the final customers' perspective, to understand to what extent and for which clusters of customers the perceived risk of counterfeiting results is reduced through BC technology.

References

Ali, M.H., Zhan, Y., Alam, S.S., Tse, Y.K. and Tan, K.H. (2017), "Food supply chain integrity: the need to go beyond certification", *Industrial Management and Data Systems*, Vol. 117 No. 8, pp. 1589-1611.

Alzahrani, N. and Bulusu, N. (2018), "Block-supply chain: a new anti-counterfeiting supply chain using NFC and blockchain", *1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pp. 30-35.

Alzahrani, N. and Bulusu, N. (2019), "A new product anti-counterfeiting blockchain using a truly decentralized dynamic consensus protocol", *Concurrency and Computation: Practice and Experience*, Vol. 32 No. 12, pp. 1-27.

Apte, S. and Petrovsky, N. (2016), "Will blockchain technology revolutionize excipient supply chain management?", *The Journal of Excipients and Food Chemicals*, Vol. 7 No. 3, pp. 76-78.

Azzi, R., Chamoun, R.K. and Sokhn, M. (2019), "The power of a blockchain-based supply chain", *Computers and Industrial Engineering*, Vol. 135, pp. 582-592.

Babich, V. and Hilary, G. (2019), "Distributed ledgers and operations: what operations management researchers should know about blockchain technology", *Manufacturing and Service Operations Management*, Vol. 22 No. 2, pp. 223-240.

Berman, B. (2008), "Strategies to detect and reduce counterfeiting activity", *Business Horizons*, Vol. 51 No. 3, pp. 191-199.

Biswas, K., Muthukkumarasamy, V. and Tan, W.L. (2017), "Blockchain based wine supply chain traceability system", *Paper Presented at Future Technologies Conference (FTC) 2017*, 29-30 Nov, Vancouver, Canada, available at: https://saiconference.com/Conferences/FTC2017Proceedings (accessed 10 February 2021).

Bowen, G.A. (2008), "Naturalistic inquiry and the saturation concept: a research note", *Qualitative Research*, Vol. 8 No. 1, pp. 137-152.

Bumblauskas, D., Mann, A., Dugan, B. and Rittmer, J. (2020), "A blockchain use case in food distribution: do you know where your food has been?", *International Journal of Information Management*, Vol. 52, 102008.

Cole, R., Stevenson, M. and Aitken, J. (2019), "Blockchain technology: implications for operations and supply chain management", *Supply Chain Management: An International Journal*, Vol. 24 No. 4, pp. 469-483.

Constantinides, P., Henfridsson, O. and Parker, G.G. (2018), "Introduction – platforms and infrastructures in the digital age", *Information Systems Research*, Vol. 29 No. 2, pp. 381-400.

Creswell, J.W. (2013), *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, Sage Publications, Thousand Oaks, California.

Creydt, M. and Fischer, M. (2019), "Blockchain and more – algorithm driven food traceability", *Food Control*, Vol. 105, pp. 45-51.

Eisenhardt, K.M. and Graebner, M.E. (2007), "Theory building from cases: opportunities and challenges", *Academy of Management Journal*, Vol. 50 No. 1, pp. 25-32.

EUIPO (2019), "Anti-counterfeiting blockathon forum", available at: https://euipo.europa.eu/ohimportal/en/web/observatory/blockathon (accessed June 2020).

Galvez, J.F., Mejuto, J.C. and Simal-Gandara, J. (2018), "Future challenges on the use of blockchain for food traceability analysis", *Trends in Analytical Chemistry*, Vol. 107, pp. 222-232.

Hald, K.S. and Kinra, A. (2019), "How the blockchain enables and constrains supply chain performance", *International Journal of Physical Distribution and Logistics Management*, Vol. 49 No. 4, pp. 376-397.

Hopkins, D.M., Kontnik, L.T. and Turnage, M.T. (2003), *Counterfeiting Exposed: How to Protect Your Brand and Market Share Hoboken*, John Wiley and Sons, New Jersey.

Kamble, S., Gunasekaran, A. and Arha, H. (2019), "Understanding the blockchain technology adoption in supply chains-Indian context", *International Journal of Production Research*, Vol. 57 No. 7, pp. 2009-2033.

Kamilaris, A., Fonts, A. and Prenafeta-Boldú, F.X. (2019), "The rise of blockchain technology in agriculture and food supply chains", *Trends in Food Science and Technology*, Vol. 91, pp. 640-652.

Kshetri, N. (2018), "Blockchain's roles in meeting key supply chain management objectives", *International Journal of Information Management*, Vol. 39, pp. 80-89.

Kumar, A., Liu, R. and Shan, Z. (2020), "Is blockchain a silver bullet for supply chain management? Technical challenges and research opportunities", *Decision Sciences*, Vol. 51 No. 1, pp. 8-37.

Li, L. (2013), "Technology designed to combat fakes in the global supply chain", *Business Horizons*, Vol. 56 No. 2, pp. 167-177.

Lo, S.K., Xu, X., Wang, C., Weber, I., Rimba, P., Lu, Q. and Staples, M. (2019), "Digital-physical parity for food fraud detection", in Joshi, J., Nepal, S., Zhang, Q. and Zhang, L.J. (Eds), *Blockchain - ICBC 2019, Lecture Notes in Computer Science*, Vol. 11521, Springer, Cham, pp. 65-79.

Lu, D., Moreno-Sanchez, P., Zeryihun, A., Bajpayi, S., Yin, S., Feldman, K., Kosofsky, J., Mitra, P. and Kate, A. (2019), "Reducing automotive counterfeiting using blockchain: benefits and challenges", *IEEE International Conference on Decentralized Applications and Infrastructures*, pp. 39-48.

Lybecker, K.M. (2007), "Rx roulette: combatting counterfeit pharmaceuticals in developing nations", *Managerial and Decision Economics*, Vol. 28 Nos 4/5, pp. 509-520.

Martinez, V., Zhao, M., Blujdea, C., Han, X., Neely, A. and Albores, P. (2019), "Blockchain-driven customer order management", *International Journal of Operations and Production Management*, Vol. 39 Nos 6/7/8, pp. 993-1022.

Miles, M.B. and Huberman, A.M. (1994), *Qualitative Data Analysis: An Expanded Sourcebook*, Sage Publications, Thousand Oaks, California.

Mintzberg, H., Quinn, J.B. and Ghoshal, S. (1995), *The Strategy Process*, Prentice Hall International, Hemel Hampstead.

Montecchi, M., Plangger, K. and Etter, M. (2019), "It's real, trust me! Establishing supply chain provenance using blockchain", *Business Horizons*, Vol. 62 No. 3, pp. 283-293.

Pandey, S.C. and Patnaik, S. (2014), "Establishing reliability and validity in qualitative inquiry: a critical examination", *Journal of Development and Management Studies*, Vol. 12 No. 1, pp. 5743-5753.

Pereira, J., Tavalaei, M.M. and Ozalp, H. (2019), "Blockchain-based platforms: decentralized infrastructures and its boundary conditions", *Technological Forecasting and Social Change*, Vol. 146, pp. 94-102.

Pustjens, A.M., Weesepoel, Y. and van Ruth, S.M. (2016), "Food fraud and authenticity: emerging issues and future trends", in Leadley, C. (Ed.), *Innovation and Future Trends in Food Manufacturing and Supply Chain Technologies*, Woodhead Publishing, Cambridge, pp. 3-20.

Queiroz, M.M., Telles, R. and Bonilla, S.H. (2019), "Blockchain and supply chain management integration: a systematic review of the literature", *Supply Chain Management: An International Journal*, Vol. 25 No. 5, pp. 241-254.

Rejeb, A., Keogh, J.G. and Treiblmaier, H. (2019), "Leveraging the internet of things and blockchain technology in supply chain management", *Future Internet*, Vol. 11 No. 7, pp. 1-22.

Risius, M. and Spohrer, K. (2017), "A blockchain research framework", *Business and Information Systems Engineering*, Vol. 59 No. 6, pp. 385-409.

Roeck, D., Sternberg, H. and Hofmann, E. (2020), "Distributed ledger technology in supply chains: a transaction cost perspective", *International Journal of Production Research*, Vol. 58 No. 7, pp. 2124-2141.

Saberi, S., Kouhizadeh, M., Sarkis, J. and Shen, L. (2019), "Blockchain technology and its relationships to sustainable supply chain management", *International Journal of Production Research*, Vol. 57 No. 7, pp. 2117-2135.

Schmidt, C.G. and Wagner, S.M. (2019), "Blockchain and supply chain relations: a transaction cost theory perspective", *Journal of Purchasing and Supply Management*, Vol. 25 No. 4, 100552.

Singhal, B., Dhameja, G. and Panda, P.S. (2018), *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*, Apress, New York, New York.

Speier, C., Whipple, J.M., Closs, D.J. and Voss, M.D. (2011), "Global supply chain design considerations: mitigating product safety and security risks", *Journal of Operations Management*, Vol. 29 Nos 7-8, pp. 721-736.

Spink, J., Moyer, D.C., Park, H. and Heinonen, J.A. (2013), "Defining the types of counterfeiters, counterfeiting and offender organizations", *Crime Science*, Vol. 2 No. 8, pp. 1-10.

Stevenson, M. and Busby, J. (2015), "An exploratory analysis of counterfeiting strategies", *International Journal of Operations and Production Management*, Vol. 35 No. 1, pp. 110-144.

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: An International Journal*, Vol. 23 No. 6, pp. 545-559.

van Hoek, R. (2019), "Exploring blockchain implementation in the supply chain", *International Journal of Operations and Production Management*, Vol. 39 Nos 6/7/8, pp. 829-859.

Villano, C., Lisanti, M.T., Gambuti, A., Vecchio, R., Moio, L., Frusciante, L., Aversano, R. and Carputo, D. (2017), "Wine varietal authentication based on phenolics, volatiles and DNA markers: state of the art, perspectives and drawbacks", *Food Control*, Vol. 80, pp. 1-10.

Vinex (2020), "Massive wine fraud uncovered by French trading standards", available at: https://en.vinex.market/articles/2018/03/19/massive_wine_fraud_uncovered_by_french_trading_standard (accessed September 2020).

Viriyasitavat, W. and Hoonsopon, D. (2019), "Blockchain characteristics and consensus in modern business processes", *Journal of Industrial Information Integration*, Vol. 13, pp. 32-39.

Voss, C., Johnson, M. and Godsell, J. (2016), "Case research", in Karlsson, C. (Ed.), *Research Methods for Operations Management*, Routledge, London, pp. 165-197.

Wamba, S.F. and Queiroz, M.M. (2020), "Blockchain in the operations and supply chain management: benefits, challenges and future research opportunities", *International Journal of Information Management*, Vol. 52, 102064.

Wang, Y., Han, J.H. and Beynon-Davies, P. (2019), "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda", *Supply Chain Management: An International Journal*, Vol. 24 No. 1, pp. 62-84.

Wine Folly (2016), "Reality of wine prices (what you get for what you spend)", available at: https://winefolly.com/update/reality-of-wine-prices-what-you-get-for-what-you-spend/ (accessed June 2020).

World Trade Organization (2020), "Glossary: counterfeit definition", available at: https://www.wto.org/english/thewto_e/glossary_e/glossary_e.htm (accessed September 2020).

Xu, X., Lu, Q., Liu, Y., Zhu, L., Yao, H. and Vasilakos, A.V. (2019), "Designing blockchain-based applications a case study for imported product traceability", *Future Generation Computer Systems*, Vol. 92, pp. 399-406.

Yin, R.K. (2017), *Case Study Research and Applications: Design and Methods*, Sage Publications, Thousand Oaks, California.

Zelbst, P.J., Green, K.W., Sower, V.E. and Bond, P.L. (2019), "The impact of RFID, IIoT, and blockchain technologies on supply chain transparency", *Journal of Manufacturing Technology Management*, Vol. 31 No. 3, pp. 441-457.

Zhang, A., Zhong, R.Y., Farooque, M., Kang, K. and Venkatesh, V.G. (2020), "Blockchain-based life cycle assessment: an implementation framework and system architecture", *Resources, Conservation and Recycling*, Vol. 152, 104512.

Appendix

Supplementary file 1 on available online

Corresponding author

Pamela Danese can be contacted at: pamela.danese@unipd.it