JOURNAL OF MANAGEMENT INFORMATION SYSTEMS
2021, VOL. 38, NO. 2, 338–373
https://doi.org/10.1080/07421222.2021.1912919

Routledge
Taylor & Francis Group

Use Of Blockchain As A Resource For Combating Corruption In Global Shipping: An Interpretive Case Study

Suprateek Sarker[a], Stefan Henningsson[b], Thomas Jensen[b], and Jonas Hedman[b]

[a]McIntire School of Commerce, University of Virginia, Charlottesville, VA, USA; [b]Department of Digitalization, Copenhagen Business School, Frederiksberg, Denmark

ABSTRACT

Corruption is one of the most troubling societal challenges facing businesses today. Businesses have been combating corruption in fragmented ways, sometimes by creating anti-corruption policies applicable to certain stakeholders and, at other times, by harnessing digital technologies. Recently, the power of blockchain, with its capacity to provide full transactional disclosure and thereby reduce uncertainty, insecurity, and ambiguity in transactions, has been touted as being a game changer in the fight against corruption. Based on a study of the global shipping industry, we find that blockchain mitigates both process and document-related corruption. Based on these findings, we develop an understanding of how corruption may be combated using both social and digital/informational resources, including blockchain technology. Our model, drawing on past work on corruption, shows the complex interplay between identity, institutional actors, technical and other resources, and practices, and we develop conditions that could be effective in fighting corruption by using technologies such as blockchain.

KEYWORDS

Blockchain; corruption; fraud prevention; global shipping; anti-corruption methods; interpretive case study

Introduction

Corruption is one of the most troubling societal challenges facing organizational managers today and often involves individuals or organizations misusing their positions to benefit themselves [45, 8182]. The consequence of corruption can be uncertainty, inefficiency, and/or unfairness across all human and business activities [26]. According to the United Nations (UN), "*corruption is a serious impediment to the rule of law and sustainable development*" [29], and it is estimated that corruption adds approximately 10 percent to the cost of doing business globally [20]. A number of measures have been taken worldwide to combat corruption and related fraud [27]. Examples of international initiatives include the formation of the UN Convention against Corruption, which is the only legally binding universal anti-corruption instrument. Within the maritime sector, the context of our investigation, more than 100 organizations have formed a nongovernmental organization—the Maritime Anti-Corruption Network—to work toward "*the vision of a maritime industry free of corruption that enables fair trade to the benefit of society at large.*" The problematic aspect of these types of initiatives is that "*anticorruption campaigns have always begun with*

CONTACT Jonas Hedman jhe.digi@cbs.dk Department of Digitalization, Copenhagen Business School, Howitzvej 60, Frederiksberg 2000, Denmark.

Supplemental data for this article can be accessed on the publisher's website.

enthusiasm and ended with cynicism" [47, p. 24] and have had a limited impact on corruption [68]. Whether in academic or trade literature, proposed remedies to corruption and related fraud generally point to somewhat generic issues such as leadership, policies, institutional change, extensive training, rigorous vetting of local consultants/agents, and so on.

There is, however, increasing recognition that the power of information technology (IT), particularly that of the Internet and its applications such as e-government, can be harnessed to address corruption and fraud [58, 84]. Interestingly, multiple studies reviewed have suggested mixed or contradictory effects of IT on corrupt and fraudulent activities [see, for instance, 84]. Recently, blockchain has been promoted as a revolutionary technology with the capacity to lower uncertainty, insecurity, and ambiguity in business transactions by providing single truth for all network participants [13, 16, 48, 66, 97]. This has led thought leaders such as Santiso [77] to wonder "*Can it [blockchain] be a game changer in the global fight against corruption?*" He concludes that *it can possibly be* (a game changer) and offers the following rationale (emphasis added):

technology readiness

> Blockchain has two distinctive features that make it a potent tool against corruption. First, it provides an **unprecedented level of security** of the information and the **integrity of records** it manages, **guaranteeing their authenticity**. It **eliminates opportunities for falsification** and the risks associated with having a single point of failure in the management of data. It also helps **overcome the data silos in traditional bureaucracies in which public entities are reluctant to share information** among themselves.

While the first point (in the aforementioned quote) refers to *data integrity*, the second refers to *transparency* through data sharing ability [28]. Despite the obvious promise of blockchain and the hype surrounding it, there is little evidence beyond the facilitation of cryptocurrency, where disinterested researchers have intensively studied the role of blockchain to reveal *how and under what conditions* this technology can help combat the evils of corruption and related fraud. Thus, our research question for the study is:

> *Can blockchain help combat corruption and related fraud, and if so, how and under what circumstances?*

Based on our findings with respect to the question, we will also offer practical implications.

Our study was undertaken in the global shipping context, where a strategic decision was taken by a major shipping company to adopt blockchain with the intention of streamlining document handling and eliminating corrupt practices that had become part and parcel of doing business. Through our study, we aspire to make several empirical and theoretical contributions. First, while previous studies have focused primarily on blockchain as a facilitator of cryptocurrency transactions, our study addresses an important societal challenge of today—that of corruption and fraud in global shipping—and seeks to offer a sociotechnical understanding of how corruption and fraud may be combated, in line with recent calls for research to be aligned with the discipline's "axis of cohesion" [79]. Second, through the revelatory case narrative, we present a "consultable record" [89] of how corruption and related fraud can occur, and when/how blockchain may (or may not) be able to help.

Overview of Two Key Areas: Corruption and Blockchain

Corruption

According to Transparency International, the fundamental issue with corruption is that it corrodes the fabric of society. It is the "unwanted virus" [89] or a "cancer" [93] that must be eradicated [88], since it undermines people's trust in political and economic systems, institutions, and leaders [87]. This view on corruption illustrates a broad take on the phenomena, which historically has focused on "the misuse of public office for private gain" [94]. Today, corruption is seen as "the abuse of entrusted power for private gain" [40, 84] or "organizational gain" [8, 22] and includes activities such as bribes, kickbacks, embezzlement, illicit gifts, favors, nepotism, and informal promises [11, 21, 22, 51, 69].

The recognition of corruption and anti-corruption activities in the world has spurred research in many fields, including economics, political science, sociology, organization studies, management, strategy, supply chain, international business, business ethics, psychology, philosophy, and IS. In organization studies and management, research has focused on the organizational context in which corruption occurs, for instance, with the number of actors involved [49]. An important contribution from organizational research is the widening of corruption from a state of misuse to also a process [4, 8]. Drawing on organizational research, which is generally silent about the role of IS in creating conditions for or against corruption, we find a number of concepts and theoretical models related to combating corruption that are potentially relevant to our work, and we discuss a small but important subset. Adopting an open systems perspective, Lange [49, p. 715] offers a corruption control circumplex with 8 types of control mechanisms that are categorized as "autonomy reduction," "intrinsically oriented controls," "environmental sanctioning," and "consequence systems." The circumplex—consisting of many simultaneously active control mechanisms—provides an opportunity for looking at IT and blockchain as having multiple roles in preventing corruption. Bernstein [18], conversely, discusses the various kinds of transparency, not all of which are needed to control corruption, that could function as a basis for theorizing on what blockchain actually does. More relevant is a theoretical framework based on the interplay between "institutional logics, resources, and institutional entrepreneurs" [62], which allows the inclusion of IT in general and blockchain in particular. Indeed, our theoretical model will build on and adapt Misangyi et al. [62] work by introducing the role of technology that interact with the social processes [79] related to dealing with corruption.

Review of IS-Related Corruption Literature

Corruption is of great concern to the IS community [1, 34, 84], but in most IS studies, corruption is an explanatory variable or empirical context [see, for instance 9, 34, 60, 82], not the focal phenomenon. There are a few exceptions though [1, 84]. Thus, there exists limited conceptual understanding of how IT relates to corruption in IS. However, in public administration [5, 2425, 43, 45, 63, 83], and especially in e-government research [19, 44, 55, 91], there is a body of research focused on how IT can mitigate corruption. In the Online Supplemental Appendix A1, we summarize our review of IS-related research on the role of IT in corruption.

Starting with the positive and encouraging results, there are multiple studies that offer empirical evidence that IT can curb corruption [6, 7, 43, 55, 73, 83, 84]. IT introduces transparency into the decision-making processes of governmental officials, and it demands accountability [31, 45]. For example, a study notes that "*e-government reduces contact between corrupt officials and citizens and increases transparency and accountability*" [6]. However, in many cases, it is hard to know how IT actually affects corruption since "*IT aiming at ambitious institutional changes [encounters] obstacles from the wider context of government and society that [erodes its] anti-corruption effects*" [1]. Furthermore, most research is based on secondary data from the Organisation for Economic Co-operation and Development (OCED) and similar sources. For instance, Andersen [6] used panel data and standard indices of IT usage to infer conclusions about corruption. More detailed descriptions are found in a small number of published cases studies [e.g., 25, 44]. As previously mentioned, much of the existing research is based on secondary data. In addition, the unit of analysis is that of countries, and corruption is assessed using some form of an aggregated measure, such as the Control of Corruption Indicator [42]. However, this measure does not specify or help differentiate between the different types of corruption, such as grand, systemic, and petty corruption. Furthermore, most existing research is from developing countries, such as China, Ghana, and India where e-government is seen as the silver bullet for preventing corruption.

Blockchain in Global Supply Chain

Similar to how Nakamoto envisioned blockchain would transform money and payments, Santiso [77] articulated his hope that blockchain would be the silver bullet in fighting global corruption. In reviewing the emerging literature on the topic, we found either technically oriented abstract work, for example, about a consensus algorithm [50] and cryptocurrencies [37, 67, 86], or domain-specific work covering the Internet of Things [23], e-identification [85], shipping [41], maritime sector [72], health care [2], the food supply chain [4647], governance issues [97], and the choice of blockchain technology [121314]. However, this existing research deals with limited aspects of blockchain, featuring few applications that demonstrate the fact that the real transformative power of blockchain lies in "its openness and technologically driven capability to pervade multiple vertical layers of [the] digital ecosystem infrastructure" [33]. This applies particularly for the supply chain and shipping context, where blockchain use cases are found along the entire supply chain [61, 92, 95] and where there are strong requirements for validation and immutable transactions [33] with key documents [56, 61].

Blockchain, being a distributed technology, is touted to provide transparency, traceability, and secure transactions to distributed nodes (supply chain members) via a peer-to-peer communication network [16, 48, 66]. It is a strategic tool [30], which ensures that supply chain stakeholder requirements for various goals are fulfilled [76] by increasing product provenance information—for example, origin, production, modifications, and custody [64]. This may reduce logistics costs and optimize operations, for instance, with fresh food delivery [70]. This is also helpful when integrating blockchain with legacy backbone systems because information can be shared with partners while ensuring different levels of visibility along the supply chain [57]. This property can help detect counterfeit products [3]. Blockchain can establish trust and create traceability by ensuring secure and authenticated

trust

information in logistics and supply networks [35, 46]. Overall, blockchain may be thought of as an information infrastructure [39]. Furthermore, it provides data integrity and transparency, similar to what many centralized, secured e-government systems do in public decision-making processes [84] which can curb illegal practices.

Methodology

Data collection, undertaken by the second, third, and fourth-listed (equal) authors, has been an ongoing process from 2012 to 2020, with the addition of new interviewees as our insights and understanding evolved and new questions emerged. Furthermore, our focus has also shifted as we analyzed, reflected on, and enriched our insights and gained new knowledge about the global shipping context and the role of digital technologies. For example, the theme of corruption was not a focus of ours early on but emerged as an important theme through the many conversations with our interviewees and the first-listed author. Similarly, our interest in blockchain emerged in around 2017 as a major shipping line (pseudonym SHIPCo) started experimenting with blockchain in a strategic cooperation with a major tech partner (pseudonym TECHCo).

Several of the interviewees saw IT as a means to improve international trade, especially the supply chain with regard to both efficiency and security. We interviewed a range of key stakeholders in SHIPCo and TECHCo including the CEO, the strategy officer, the chief financial officer, the chief information officer, the digital information officer, and innovation team members. We also spoke to governmental authorities, personnel in anti-corruption bodies, and several IT-related people with deep insights into both IT and the complexity of international shipping. Furthermore, the research team became a partner in a large sponsored research project on international trade with more than 70 partners. This opened the doors to set up focus groups with traders and authorities plus a range of IT providers trying to set up solutions in so-called living labs [15]. To investigate the problems in international trade, fresh products were physically followed from farms in an African nation (pseudonym AFCT) to their point of retail distribution in Europe. Regarding corruption, several of the interviewees mentioned *facilitation fees* and how the use of such fees through service providers facilitated the flow of paperwork and goods and prevented unnecessary delays. The main aim of the collaboration between SHIPCo and TECHCo was to propose IT solutions to address the main issues of international trade through shipping. This included blockchain technology prototypes that were being piloted and later adopted, to varying degrees. The results of this work by SHIPCo and TECHCo laid the foundation for a commercial solution that is being increasingly adopted by traders, shipping lines, and authorities in the world. This solution based on blockchain became the focus of our research from 2017 to 2020. In 2019 and 2020, we revisited the previous interviews and deliberately selected relevant individuals for new interviews focused primarily on corruption. The number of interviews conducted, along with the profiles/positions of the interviewees by year, are listed in Table 1. We note that many of the individuals were interviewed on multiple occasions.

Case Study Genre: Interpretive Case Study

Consistent with the tenets of the chosen case study genre and the constructivist nature of the work, we have followed Walsham's [89, 90] guidelines broadly. A summary of the

Table 1. Interviews conducted by role and year.

Role	2012	2013	2014	2015	2016	2017	2018	2019	2020
Influencers	3 nonprofit organization	1 director of association	1 director of association	1 nonprofit organization and 2 governmental officers	3 governmental officers	2 governmental officers	3 governmental officers	4 nonprofit organization	1 nonprofit organization
Shipping line	2 CIOs and 4 innovation team members	8 top managers including the CEO, CFO, SO, CIO, and 4 innovation leaders	2 top managers and 5 local managers	3 top managers and 5 local managers	11 top managers	2 top managers	1 top manager	2 top managers and 2 managers	5 managers
Traders/ Shippers		4 traders	26 traders	45 traders	19 traders	5 traders	2 traders	1 trader	
Authorities		6 customs officers	9 customs officers	16 customs officers and 15 port of authority officers	12 customs officers and port of authority officers	7 customs officers and port of authority officers	6 customs officers		3 customs officers
Service providers		16 terminal operators and service providers	6 service providers	19 service providers	16 service providers	8 service providers	2 service providers	2 service providers	
Total	9	29	49	108	58	22	11	9	9

methodological considerations for the study are provided in the Online Supplemental Appendix A2, adapted from Sarker and Sarker [78].

Case Narrative: Global Shipping and Nature of Corruption

Our investigation started with the flow of agricultural goods between ports of an African country (pseudonym AFCT) and of a country in Europe (pseudonym EUCT). When goods are exported from AFCT to EUCT, it passes through a chain of up to 40 actors who each enact a specific role in the supply chain. Some steps are common regardless of different factors, while others are specific to the trade route (means of transport, traversed borders, etc.), the kind of goods exported, and the specific actors involved. For the goods, we mapped points of corruption along the journey. In our case, the focal good is an agricultural product (pseudonym AGRI_PROD) that must be suitable for human consumption when it arrives, and thus has to be transported in refrigerated containers. Since AGRI_PRODs are perishable, transportation is subject to time pressure. Longer lead times affect both the shelf life and the selling price. These aspects raise additional possibilities for corruption compared to some less time-sensitive products, given that export requires several kinds of processing and issuance/checking of multiple certificates.

The shipping of AGRI_PROD consists of three combined processes—export, shipping, and import—that are connected through containerized ocean shipping. First, farmers grow, harvest, and package the AGRI_PRODs before they are picked up by local freight forwarders and brought to the port of departure. When cleared for export, the AGRI_PRODs are loaded on and transported by a designated ship to Europe, typically through the Suez Canal and the Mediterranean Sea. On the import side, the AGRI_PRODs arrive through a major port in EUCT and need to be cleared for unloading by the EUCT authorities before entering the country, and, subsequently, must be approved for import by another office of the EUCT authorities. The cleared goods can then leave the port area and are transported to other locations and, in some cases, reexported to other countries in Europe and beyond.

Points of Corruption

The potential for corruption in the international shipping of AGRI_PRODs is related to the many steps in the supply chain, where specific actors (organizations and individuals) have delegated authority. Over 40 organizations are involved in the chain, and any one of them can hold back the container in the export of AGRI_PRODs from AFCT to EUCT. At every single point in the chain, there is a potential for corrupt behavior. Table 2 provides a sample of the corruption possibilities we identified by tracking shipments of AGRI_PRODs. In Figure 1, these points of corruption are visualized with respect to the flow of products through export and import.

Corruption primarily happens either in relation to speeding up/delaying the flow of goods or in relation to the certificates and declarations that are necessary to process export and import declarations. As can be seen in Figure 1, the complete journey (i.e., a typical journey without extraordinary events) from the farmer to the warehouse for distributions was, according to our investigation, 34 days. About half of this time is idle time related to, for example, waiting to be allowed into the port area of AFCT (which is often jammed with traffic) to unload goods. This is then a possible point of corruption

Table 2. Corruption possibilities

Code	Corruption Event	Description
		Process-related corruption
Pa1	Gating in to port, prioritization	To avoid extensive waiting time for trucks and containers at the port gates, paying a surcharge allows one to be prioritized and to bypass the queue of waiting container vessels.
Pa2	Port opening hours	Getting in to the port outside normal operating hours is possible by paying a fee.
Pa3	Certificate of origin, processing	The certificate of origin establishing the provenance of goods needs to be physically stamped before loading on a ship for export. Fees may need to be paid to enable and speed up processing.
Pa4	Veterinary certificate, processing	The veterinary certificate establishes that the producers of the goods have been subject to the relevant veterinary inspection. Fees may need to be paid to enable or speed up processing.
Pa5	Phytosanitary certificate, processing	The phytosanitary certificate establishes that the goods meet relevant health considerations (i.e., concerning the use of pesticides). Fees may need to be paid to enable or speed up processing.
Pa6	Export declaration, processing	The export declaration establishes that the goods are being exported and are not subject to export taxation rules. Fees may need to be paid to enable or speed up processing.
Pa7	Ship departure slots	Ship departure slots from ports are allocated manually. Fees may need to be paid to obtain a slot and/or reduce waiting time when the ship is ready for departure.
Pa8	Passage through Suez Canal	Gifts or direct payment of fees may be needed to grant passage through the controlled channel.
Pa9	Use of import service	Using consultants with extensive process knowledge and personal networks may resolve the issue and speed up processing, e.g., of imported goods at the destination country.
Pa10	Overlooked control task	Customs agents overlook inspection duties, allowing for smuggling of illegal goods.
		Documentation-related corruption
Pb1	Certificate of origin, issuing	The incorrect issuing or approval of this certificate containing fraudulent information.
Pb2	Veterinary certificate, issuing	The incorrect issuing of this certificate containing fraudulent information.
Pb3	Phytosanitary certificate, issuing	The incorrect issuing or approval of this certificate containing fraudulent information.
Pb4	Export declaration, approval	The incorrect approval of an export declaration stating incorrect information.
Pb5	Import declaration	The incorrect lodging and approval of an import declaration specifying product details that determine import duties.
Pb6	Tax declaration	The incorrect lodging and approval of a product's categorization or of the country of origin to reduce or avoid taxation.
Pb7	Pro forma invoices	Falsified invoices not matching real shipments or the actual contained goods to reduce taxes.
Pb8	Fake organizations	Use of nonexistent or storefront organizations for tax evasion.

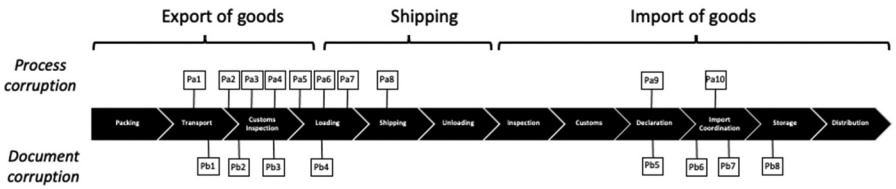

Figure 1. Points of corruption during the shipping of AGRI_PRODs from AFCT to EUCT.

(Pa1 in Table 2), where one needs to pay a facilitation fee to get into the queue earlier or extend the port's opening hours (Pa2) so that the AGRI_PRODs can be loaded before a given vessel sails off, instead of waiting up to a week for the next departing vessel. In

fact, we learned that some authorities systematically cause delays and then organize facilitation activities around possibilities to work around formal opening hours, planning or delaying ship departures to formally closed hours (Pa3) or counting on getting document issued on Sundays to be able to meet a weekly departure slot (Pa4–Pa6). Some of these activities are, by our definition, corrupt behaviors. While not formally illegal, they extort or at least encourage the payment of facilitation fees (e.g., an express handling and after-hours surcharge). Less openly and commonly not including obvious monetary payments or demands for such payments, service providers offer to assist and facilitate this process; this happens in the African as well as European ports. For example, specialized service providers facilitate the clearance of fresh produce that involves phytosanitary authorities and also customs offices for duties. These service providers can assist in direct product flows in ports of entry whereby the import process would be far smoother than without their assistance. On the EUCT import side, the most relevant points of process corruption were related to the influence of organized crime to impact control of processes. This might include the setup of illegitimate companies to deal with import taxes and duties (Pa9) and to enable smuggling of illegal products, such as drugs or weapons (Pa10). Corrupt officials are engaged in these activities by overlooking their responsibilities of ensuring adequate controls.

A second category of corruption pertains to the falsification of documents needed for export and import or issuing them on incorrect grounds. For example, because AFCT and the European Union have a free trade agreement covering agricultural products, AGRI_PRODs from AFCT are not subject to import duties. But AGRI_PRODs from other countries may be subject to duties. Therefore, AGRI_PRODs that are shipped through AFCT and incorrectly certified (Pb1) as produced in AFCT will not be subject to import duties. Similarly, there might be economic advantages from fraudulent certificates regarding health inspections, the use of pesticides in products, the product category, and other important certificates (Pb2–Pb4) that make shipping possible or economically more attractive. For example, if AGRI_PRODs are categorized, for example, as *fresh-cut* roses or *grafted* roses, they are subject to different rules and tariffs (Pb6). Also stated quantities, weight, and volumes impact duties and fees and are therefore frequently stated incorrectly and approved at various places in the process (Pb5). Incorrect issuing or approval of original documents has traditionally been an important source of fraud/corruption since the import authorities only accept original documents with stamps and signatures that are difficult to forge. Import authorities require these documents to be presented in their original form, with a reference number that is also logged on the AFCT side. Prior to blockchain, importing authorities in EUCT would call, mail, or fax their AFCT counterparts to validate the existence and accuracy of key certificates. Sometimes, inconsistencies arising from the tampering of logged records in AFCT would be identified through a labor-intensive process. However, irrespective of the technology implemented, there was no easy way to prevent scenarios where a certificate should not have been issued in the first place.

Another possibility to exploit weaknesses in document handling is related to the acceptance of pro forma invoices in the import process (Pb7). These invoices are the grounds for calculating duties but can differ substantially from the actual invoices used in commercial transactions. Of course, there are other behaviors of customs officers and authorities (e.g., punctuality, discipline in documentation that can aid corruption) and infrastructure issues

that can only be partially managed with non-governmental policies and latest technologies. We consider them to be outside the scope of our study.

Role of Digitization

In this context, digital technologies that help manage the possibilities for corruption have been implemented in three phases. The first was part of a broad adoption of enterprise applications such as supply chain management systems and accounting systems in various organizations (including the SHIPCo) participating in the shipping process. Some companies were earlier adopters than others; for example, SHIPCo already had elaborate IT enablement in place in the 1980s. Others, such a minor AFCT growers, are in the early stages of introducing digital technologies. Fundamentally, these technologies digitize processes internal to companies. Their widespread adoption means that most data elements related to shipping are digitized at some point and are being processed by some digital means.

The second era has seen the introduction of e-customs systems that digitize specific information exchanges. In the European Union, e-customs is regulated centrally and is moving toward a harmonized set of applications. While the customs and trade systems are numerous, the most important systems for the shipping of AGRI_PRODs from AFCT are the import declaration system, customs risk assessment systems, and the database for the European Operators Registration and Identification system. Recently, the import declaration system has been integrated as a sub-component of a new automated import system. In AFCT, e-customs was introduced as part of the Revenue Administration Reform and Modernization Program, which, among other things, established a national revenue system. Previously, revenue control was enabled by a multitude of subsystems, each managed independently with individual digital identities used. In 2018, it was replaced by the Integrated Customs System. Because of the growing complexity of e-government solutions, both the AFCT and European authorities have also introduced central connection points, referred to as single windows, that serve as portal systems that give access to a large set of governmental systems.

Finally, in the third era, the shipping industry has, over the last few years, seen an explosion in initiatives embracing blockchain. AFCT pioneered the use of blockchain in trade when an application was trialed in 2016-2017 as a proof-of-concept to enable and track information exchanges in a few shipments of flowers. The experiences were positive, and there was a subsequent move toward implementation. To do so, the decision was made together with other African countries to develop a shared blockchain-based solution, following the Tangle architecture by IOTA. This project was due for completion in 2020 but has been delayed.

Instead, other initiatives involving customs authorities have moved faster to address supply chain traceability and/or document exchange with blockchain. The Israeli shipper ZIM, in 2017, and the G2 Ocean consortium, in 2018, presented their respective solutions to digitize the bill of lading using blockchain. Soon after, Maqta Gateway piloted a blockchain-based solution for the Abu Dhabi port community, and in 2019, a multimodal blockchain solution to trace products combining road and sea transport from Chongqing in China to Singapore. The blockchain application that has gained widespread adoption is TradeLens, a partnership between Mærsk and IBM that was commercially released in 2018. As of 2020,

TradeLens has gained a growing user base comprising more than 100 international ports, 10 national customs authorities, and 10 international shipping lines. Taken together, the shipping lines in the TradeLens ecosystem account for approximately 65 percent of global container shipments. In the Online Supplemental Appendix A3, we summarize the key blockchain related shipping initiatives.

A point worth noting is that while pilots of these systems have been tested around the world, commercialization of blockchain in shipping is still in its infancy, especially in AFCT, which prompted us to adopt three approaches in assessing the impact of blockchain and related technologies on corruption in shipping: *a retrospective approach, a focus on current state-of-affairs*, and a *prospective approach*. Through a retrospective approach, we constructed how goods flow through the system, what kinds of corruption and fraud have been known to occur, and how gradually digital technologies have been introduced over the years. The current state of affairs is based on concrete examples from experimental use of blockchain technologies, in EUCT as well as other countries around the world. The status of Blockchain implementation in AFCT is also reported. Finally, our prospective account was based on: a) the emergent use cases across the globe of the Blockchain application started by the two partners (SHIPCo and TECHCo), and b) expert opinions on the impacts of the Blockchain technology in the future, since this state-of-the art technology has not been fully implemented and routinized. We have discussed the *reported effects* and *anticipated effects* separately later in the paper.

Theoretical Lens

Following the interpretive case research tradition, we use a theoretical framework adapted from [62] as a *lens* to make sense of the complex, multidimensional, and messy world represented in the empirical material. We note that while the lens does not explicitly highlight the role of digital technologies, it does allow us to focus on the interplay between institutional logics, institutional entrepreneurs, and resources (including digital resources such as blockchain) that are all indicated in our empirical material. Through the data-theory interaction, a sociotechnical understanding of how corruption is being tackled in the global shipping arena emerged.

Let us briefly review the different concepts [73] and thereafter understand how they work together. First, we consider the social actors. *Social actors* operate in the institutional field and carry meaning that both reflects and is reflective of practices. *Institutions* tend to influence the practices of the actors through the regulative, normative, and cognitive pillars [32]. *The actors' practices* also draw on the resources they have available: economic, social, symbolic, and even cultural. Given the *different rules and schemas* of the actors initially, they have *fragmented identities* as a collective. That is, they enact competing institutional logics in their practices, while simultaneously trying to coopt or coerce other social actors to act in accordance with their preferred logic or to adopt compromised positions as necessary [4]. While there can be a variety of social actors, the ones who are most pertinent for our context (of combating corruption) are those who are keen to retain the existing state of affairs (i.e., the "*defenders of the status quo*" – those defending and reproducing the corrupt order), *those who are indifferent* and are willing to go with the flow to achieve their own goals, and those who seek to actively promote changes to the existing state of affairs (i.e., the "*institutional entrepreneurs*" – those championing and working toward a corruption-free order) by

creating a different *system of meaning* and coopting/coercing disparate set of actors to behave consistently [32]. Being effective in institutional entrepreneurship is far from trivial for a number of reasons. Indeed, the literature acknowledges "that the emergence of novelty [the new institutional reality] is not [an] easy or predictable process and is rife with politics and ongoing negotiation" [32].

Furthermore, the institutional entrepreneurs must have access to resources, including digital technologies, whose properties must be *framed* in a way that is meaningful to the other groups of social actors. Only through this access may a shared "system of meaning" and a *shared identity* with accompanying schema and rules result.

Case Interpretation

We now present the evolution of the entire institutional field of the shipping of agricultural products such as AGRI_PRODs from a major port in AFCT to a major port in EUCT. We present four different eras with respect to the coordination of efforts: era 1 (1985-2000), era 2 (2000-2015), era 3 (2015-2020), and era 4 (ongoing since 2021). Table 3 presents an overview of the four eras and subsequently interprets the process by which the corrupt institutional field in global shipping has gradually moved toward becoming an anti-corrupt field.

Era 1 (approx. 1985-2000): Fragmented Identity

The five social actors we consider are the shipping company, the shipper, customs/authorities in the AFCT port, customs/authorities in the EUCT port, and service providers.

With respect to identity, social actors do not have a shared initially at this stage. We may say actors have a fragmented identity due to the very different and independent schemas and routines as well as resources being drawn upon by different stakeholder groups. For example, the shipper is interested in getting the goods though within a given time from the warehouse to the African port, then through customs, onto the ship, through European customs, and then to the European distributor (since AGRI_PRODs have a limited shelf life). To avoid delays, in light of the efficiency-at-all-costs mindset, the shipper is willing to pay facilitation fees (sometimes through service providers) at various points, first to port authorities, who can potentially delay steps in letting the shipper's truck through the gate of the port, in loading the cargo, and in authorizing the departure of the cargo, and second to customs officers, who could cause major delays in the customs inspection process and in moving the products toward shipping (unless facilitation fees are paid). They could also, for the right fee, overlook erroneous entries in documents or sign off on false declarations (regarding the origin of the products and product expiry dates). For example, a manager of SHIPCo noted that "a box of cash" was often needed to deal with delays. He added:

> For [SHIPCo], it is a matter of clearing the manifests and other vessel related documentation. And that has to be expedited promptly of course to allow entry or departure from the ports. Any delay of course cost a lot of money . . . Every importer uses service providers for logistics, custom clearance, and declaration, else their fresh produce in the containers would get both reduced shelf life and prices.

Another manager added:

Table 3. The Institutional field of corruption in the global shipping case and the four eras.

Key Concepts	**Era 1** (approx. 1985-2000)	**Era 2** (approx. 2000-2015)	**Era 3** (approx. 2015-2020)	**Era 4** (approx. 2020-2030)
Identity	*Fragmented identity related to corruption* Fragmented between *efficiency-at-all-costs mindset, service-provider-for-a-price* (status quo), and emergence of *anti-corruption identities* of social actors	*Disjointed identity related to corruption* *Anti-corruption identity starts to strengthen*, though competing logics among social actors and lack of widespread buy-in of the "corruption-as-a-societal-ill" framing exists	*Emergent Identity against corruption* Anti-corruption identity becoming dominant	*Unified and normalized identity against corruption* Anti-corruption identity is expected to be seen taken-for-granted, with the identities condoning or supporting corruption being the rare exception.
Social actors	*Defenders of status quo* are in large proportion, if not dominant. Majority of actors indifferent to the issue of corruption, seeking to run business with efficiency and expediency. New realization among a key actor (SHIPCo) that it has a responsibility to prevent corruption that is harmful to society. No serious *institutional entrepreneurship*.	*Institutional entrepreneurs gaining in momentum*, forming alliances through anti-corruption interest organizations. With the laws catching up, passive actors or defenders of status quo are challenged in their use of corruption as a natural part of business. In some cases (though rare), corruption can lead to heavy fines and prosecution of individuals.	*Anti-corruption institutional entrepreneurial actors are becoming dominant* as defenders of the anti-corruption institutional order. Passive actors are being coopted or coerced into accepting this order as business rationale favors enactment of anti-corrupt schemas and routines.	*Anti-corruption is the norm and anti-corruption actors are engaged in defending the new institutional order*. Actors not conforming to the order is systematically excluded from participation in trade processes.
Schemas and routines	Corruption is *a natural part of doing business* Corruption not having any stigma, and seen as "*gifts for services*" or "*lubrication*" Special accounts for corruption—deductible operating costs Using paper-based and cash-based transactions—*easy to hide corrupt payments*	Corruption as *sometimes a necessary evil* *Coexistence* of paper and cash-based process with digital processes Slush-funds and pocket money to be used to *grease palms for the sake of efficiency*. Use of local service providers to make payments, thereby circumventing internal policies (*outsourcing of corruption*). Physical papers are mirrored in IT, allowing for *some degree of authenticity checking of documents*	*Moral commitment to eradicating corruption* Digitalization of trade and use of *blockchain-enabled process for transparency and secure trade document exchange* in select locations *Removal of cash* from trade process making bribery very difficult. Management action to minimize their legal exposure, from being seen as aiding/abetting corruption.	Digitalization of trade and use of *blockchain-enabled process for transparency and secure trade document exchange* *Automation through smart contracts*

(*Continued*)

Table 3. (Continued).

Key Concepts	**Era 1** (approx. 1985-2000)	**Era 2** (approx. 2000-2015)	**Era 3** (approx. 2015-2020)	**Era 4** (approx. 2020-2030)
Resources (including digital)	Very limited initially but introduction of an *official anti-corruption policy* by one actor and an *intraorganizational transaction systems* that made bribes and payments visible *within* organizations	*Policy of limited number of companies and strong judicial systems* with anti-corruption laws *Interorganizational transaction systems* seen as resolving some documentation validation issues	*Blockchain* for complete transparency of process to hold actors accountable *Strengthened coalition* of anti-corruption supporting actors	Access to *blockchain* becomes key resource for business operations, enabling voluntary compliance
Framing	No effective framing	Competing frames with respect to policies and technologies for interorganizational systems but traders express longing to go back to "good old paper-days"	*Moral imperative to remove corruption from the shipping process* *Blockchain* touted as "neutral ground" for business to digitize shipping, *framed as trade-enabling for all actors* Blockchain seen by senior managers as *a tool to avoid personal prosecution* due to staff actions found to be related to corruption	Blockchain seen as an *integral part* of *conducting efficient and corruption-free trade*
Practices	*Presentation of false documents to authorities/customs at destination* *Payment of facilitation fees*, directly or indirectly, in response to new accounting practices and internal controls *Articulation of anti-corruption policy* by one actor but only partial cooptation of other actors *Rationalization by corrupt actors*	Possible manipulation/*falsification of documents electronically* Institutional entrepreneurs *draw on company policy and strong judicial systems* with anti-corruption laws *Limited rationalization by corrupt actors*	*Cooptation and coercion of defenders* of corrupt order by institutional entrepreneurs Dealing with *implementation complexities* of blockchain in particular integration to existing legacy systems	Dealing with *interoperability* between blockchain solutions *Encouraging participation in the blockchain application* for access to business network and for greater efficiency; de-risking based on data available in blockchain

(*Continued*)

Table 3. (Continued).

Key Concepts	**Era 1** (approx. 1985-2000)	**Era 2** (approx. 2000-2015)	**Era 3** (approx. 2015-2020)	**Era 4** (approx. 2020-2030)
Nature of corruption addressed	Limited impact. Decreasing level of direct corruption by some actors due to: a) articulation of an uncorrupt policy by a key actor; and b) implementation of accounting practices and internal transaction control	Some level of validation of certificates and documents, though no guarantees Removes (or separates spatially) human-to-human transactions. Institutional entrepreneurs framing corruption as a societal ill; this is to resist direct corruption based on their collective economic and political powers.	Immutability of events on the blockchain makes falsification of certificates and declarations largely disappear Move to remove human involvement, thus fewer possibilities to deliberately stall or delay processes Transparency provided by the blockchain's distributed ledger technology prevents, for instance stalling	*Prevention* rather than detection (and subsequent prosecution) of corruption as risk of exposure and accountability is getting known
Resolved corruption	Please see Table 4		Improved retrospective accountability about any sort of bribery or facilitation payments or receipt	

> That [i.e., paying facilitation fees] is the everyday challenge for anyone doing business in particularly in those parts of the world.

Speaking about the issue of falsified documents, a senior manager within TECHCo added:

> Talking about materials provenance, you know that's a—yeah, that is, that is a big area. So, for example, you say you know this cotton is organic. Is it really organic? Is your coffee really fair trade?

The shipping company would also typically equip its captains or captains of subcontractors with the cash needed to pay local fees. Beyond paying legitimate fees, ship captains would also use these funds to buy "*gifts*" or to "*compensate*" local authorities and operators for expedient processing, for example, to speed up the slow verification of documentation before departure. Scheduling ship departures on days when ports were officially closed or counting on gates being open during after-hours remained a standard practice to encourage special facilitation fees to be paid to authorities.

Finally, some fees (e.g., a consultancy charge) were offered to agents interfacing with the European customs authorities to utilize their knowledge on ways to convince authorities that the documents were credible and to release shipments without delay. Interestingly, many of the facilitation agents in the African and European ports happened to be former customs officers or port authorities. During this time period, the focal shipping company went from an official position that corruption was a local, culturally accepted business practice to starting to see it as a problematic activity that was to be avoided. In operational terms, corruption-related expenses were removed from the corporate accounting schema. The fact that SHIPCo, a global shipping company with significant economic power and legitimacy, encouraged such a mindset to develop and frame internal policies also influenced other social actors in the institutional field. Corrupt activities where shipping company personnel were directly involved gradually started to diminish (Pa3-Pa6). For example, to cross the Suez Canal, it was customary to offer "gifts" to the pilots and officials who helped navigate the ship through the canal itself. The shipping company tried to resist this practice. Yet, in the absence of a shared resource (e.g., a policy forbidding such facilitation, buy-in by some of the other shipping companies) and a common anti-corruption identity and related rules and resources, the practice of offering "gifts" was not fully discontinued. As the CEO of SHIPCo recollected,

> For many, many years . . . sailing through the Suez Canal meant paying hundreds of thousands of dollars [in addition] to the new [...] state-owned flat rate, plus some cigarettes carton [*sic*] and a bottle of whiskey to those who were allowed to drink . . . [This] was needed to get [keep] things running.

In practice, the availability of flexible/uncontrolled funds and the use of cash (off the books) continued to enable corrupt local practices, including the use of service providers who officially acted as agents to grease the palms of authorities. Similar issues were experienced with regard to facilitation fees offered to customs and other port authorities. As suggested by the literature, an implicit negotiation among the actors ensued, with a number of rationalization mechanisms being invoked, including the "denial of responsibility" ("What can I do? My arm is being twisted"), the "denial of injury" ("No one was really harmed"), and empathy with the poverty of the authorities [4].

Table 4. Corruption possibilities and impact of digital and other resources.

		Impact of Policies, Laws, and Digital Technologies (Including Blockchain)			
Type of Corruption	Corruption Event	Era 1	Era 2	Era 3	Era 4*
Process-related corruption	Gating in to port, prioritization (Pa1)				
	Port opening hours (Pa2)				
	Certificate of origin, processing (Pa3)	Partially resolved		Resolved	
	Veterinary certificate, processing (Pa4)	Partially resolved			Expectation
	Physio sanitary certificate, processing (Pa5)	Partially resolved			Expectation
	Export declaration, processing (Pa6)	Partially resolved	Resolved		
	Ship departure slots (Pa7)		Resolved		
	Passage through Suez channel (Pa8)		Resolved		
	Use of import service (Pa9)				Expectation
	Overlooked control task (Pa10)			Partially resolved	
Documentation-related corruption	Certificate of origin, issuing (Pb1)				
	Veterinary certificate, issuing (Pb2)				
	Physio sanitary certificate, issuing (Pb3)				
	Export declaration, approval (Pb4)			Partially resolved	
	Import declaration (Pb5)			Resolved	
	Tax declaration (Pb6)			Resolved	
	Proforma invoices (Pb7)				Expectation
	Fake organizations (Pb8)				Expectation

Note: * Expectation: Expert assessment that the behavior can be detected or largely prevented.

Nevertheless, with the official position of the major shipping company with respect to eradicating corruption-related practices changing, gradually the other shipping companies and some shippers were beginning to officially oppose paying facilitation fees. Yet other issues such as the falsification of certificates and other documents as a shipment made its way from the shipper's warehouse to the distributor's warehouse could not be controlled even if the practice of direct corruption was being discontinued. In addition, given that all transactions between parties in the trade flow involved physical interchanges using humans, most other points of corruption remained.

Era 2 (Approx. 2000-2015): Disjointed Identity

During the second era, with SHIPCo taking a lead in framing corrupt practices as being harmful for society, there was some level of cooptation of other shipping companies, and in 2011, the Maritime Anti-Corruption Network (MACN) was established. Furthermore, with the introduction and increased awareness of corruption laws, the other shipping companies were increasingly buying into the anti-corruption identity *officially*; however, the enacted identity can be seen as disjointed given that authorities and service providers were still indirectly being used by the shipping companies for "facilitation."

SHIPCo was increasingly being pressured by public opinion and home country legislation to establish and implement a strict internal policy on anti-corruption. In 2009, SHIPCo formulated an anti-corruption policy as part of its sustainable business practice, and in 2011, it sent 19,000 staff on an anti-corruption training course. A senior manager said that there was a clear edict by top management that SHIPCo "*is not going to be involved in any sort of facilitation*." Also, being one of the signatory members of an anti-corruption body among companies involved in international shipping, and engaging with other networks led by the UN, Oxfam, and African-based interest organizations, SHIPCo sought to clarify what was or was not considered corrupt behavior and to build a network agreeing to this interpretation. In the end, the distinction was rooted in what was illegal versus what was not. For example, the senior manager from SHIPCo expressed the view that the company had a zero-tolerance policy toward corruption but admitted to the occasional use of service providers who facilitated product flows as part of an efficient business practice:

> Well, your first priority is to get the container vessel alongside [the quay] and as soon as possible to maintain your schedule. Facilitating that . . . More stuff. Everybody at the receiving end knows it's more money.

The new strategic anti-corruption alliances formed a key resource to address corruption in certain critical instances through coordinated action. For example, unlike behaviors in the previous phase, the actors who were anti-corruption group members, in coordination, refused to pay cash fees or provide gifts for passage through the Suez channel. The CEO of SHIPCo saw the success at the Suez Canal as an important landmark winning:

> Over the last many years, we have actually managed to eliminate facility [facilitation] fees and pay virtually no.. [fees].

Similarly, through joint actions, the anti-corruption coalition was starting to target certain ports or steps in the export process, although "in [some] cases, these actions have hurt business." A manager acting on the ground at a port recalled:

> In the beginning when [SHIPCo] took the stance of not paying, ships got delayed. It took a while—I think up to a year—before it was accepted and understood.

Overall, the coordinated strategy to target such corruption was successful, and the coalition of social actors was able to establish anti-corruption schemas for their specific organizations, but managers from SHIPCo recognized that, to some extent, "we only moved the problem from one place to another as the corrupt officers would go after someone who wouldn't resist [trading efficiency for] corruption."

With respect to the authorities, the September 11 attacks in the US and a series of food-related diseases (e.g., mad cow, and bird flu) increased emphasis on the need to monitor international shipping without compromising trade efficiency and harming national competitiveness. The response was to develop interorganizational systems that allowed for electronic submission of trade information to authorities. Within customs, these new systems were placed on both the African and European sides and were initially seen as a panacea to resolving the needs for control and security.

The farmers or traders, however, were getting increasingly unhappy about the rapid growth in the number of systems they needed to deal with and the explosion in the amount of data they were expected to provide to authorities in any transaction. Seeing the new systems as a means to implement additional controls on them, they resisted compliance. As explained by one shipper:

> For each country, we need to develop interfaces to each governmental agency. And we are a pan-European business so we have to do that in almost every European country.

Therefore, much of the shipping trade continued on paper-based processes since the cost of electronic submission appeared to be overshadowing the benefits of moving to electronic submission. In addition, electronic submission practices were not considered secure enough for documents of importance, and paper-based documents with stamps remained the sole option. Unfortunately, adopting this paper-based option meant that these crucial documents remained open to forgery and falsification. Even where it was possible to move to digitized documents, authorities reportedly refused to implement such changes because, as per some of our interviewees, this would eliminate the possibilities of collecting facilitation fees. In some governmental agencies, collecting these fees was the only way to supplement the agents' very meager salaries, which led to the rationalization of such payments by some of the remaining defenders of the corrupt order.

Two parallel schemas and routines for shipping therefore were in existence. One was increasingly digitized, relying on transactions enabled by a growing set of interorganizational systems. This schema was associated with the increasing use of digital payments. In parallel, the option of completely manual paper-based processes and cash payments was retained. Not surprisingly, even in 2015, a captain of a ship travelling between Africa and Europe would carry up to 400 different paper documents associated with the cargo (and a "box of cash") on board.

The transition to electronic submission processes proved effective toward eradicating some corrupt behaviors. First, paper-based documents such as the certificate of origin would be logged at both issuing and accepting authorities, which meant that when authenticity was found questionable, accepting authorities could validate a document by checking the system. Second, in contrast to paper-based processes, the electronic submission systems removed

some human intervention (Pa6) and in other instances separated the sender and receiver from each other (Pa7), making it more challenging to demand that fees be paid in cash. Third, the systems also logged all activities, contributing to greater transparency and traceability – making it possible to retrospectively investigate which individuals had been involved in which transaction(s), and to identify incriminating behaviors. Such traceability resulted in the detection of transactions such as paying larger sums to pass through the Suez Canal (Pa8).

Yet, despite these successes, some corrupt practices continued for three important reasons. The first is that the electronic submission systems were claimed by some authorities to not be secure enough to digitize critical paper documents. Notwithstanding the possibility that this assessment was offered by the defenders of the corrupt order and by traders who did not have the IT capability to integrate with electronic submission systems, the practice of using paper documents remained the only option in some important instances. And as asserted by one operator in AFCT:

> The more documentation you need to facilitate downloading, the more openings you have for facilitation and corruption.

Second, the existence of parallel practices (digital and paper based) made it possible to switch between the two as convenient. This meant that data collected through the electronic submission systems had blind spots, and this partially prompted a fall back on corrupt behavior to resolve practical needs at hand. This also allowed for continued use of service providers who could cater to particular cases when shipments were not cleared for some reason, making the facilitation payments invisible.

Third, even though data was recorded, it was still trapped in data silos. This meant that judicial systems were faced with the tedious job of piecing together information, much like in a puzzle, from a range of sources to trace a process flow, thereby becoming ineffective. As expressed by a senior customs officer, easy access to data was an impediment to accountability:

> I think it is immensely important to have global governing standards in place that the exchange of these standards standard forms are done electronically and that these data are as much as possible from and to the source.

In practice, judicial systems could only act on a few major cases and were always reactive to suspicious corruption-related behaviors. Eventually, this meant that although the anti-corrupt identity of corruption was gaining in acceptance given the broader acknowledgement that corruption was damaging to society, there were enough resources among defenders of corruption (e.g., limitations of technologies) to preserve corrupt practices, resulting in a disjointed identity with respect to corruption.

Era 3 (approx. 2015-2020): Emergent and gradually spreading anti-corrupt identity

In the words of the CEO of SHIPCo, who had decided to invest in blockchain to streamline the process and root out corruption:

> [Anti-corruption] is the whole purpose of the [blockchain application]. The [blockchain application] must do two things: it must create visibility, physically.. for the papers . . . But it must also digitize the documents so that we get away from . . . physical document with signature on, etc.

Similarly, a representative from an organization involved in testing the blockchain application in AFCT stated that, along with the enablement of efficient export, reducing corruption was a driver for the test:

> Enabling trade was the bigger picture. What are the main barriers to trade and how can we tackle them. . . . But improving control was also a reason. The view of customs was then, and is still, that any piece of technology that can help in the job is welcome. This can do a lot of good for us, it can improve our targeting, improve in terms of revenue collection, improve port operations and decrease forgeries in documents like the Phytosanitary certificate and certificates for agricultural products. That is not in contention to enabling trade.

During the emerging era of blockchain for shipping, there have been clear signs of the anti-corrupt institutional order becoming dominant, and an anti-corruption identity emerging in the institutional field and gradually solidifying. A senior director from EUCT customs explained how society was increasingly seeing corruption as a major societal threat:

> The attention put to it [corruption] is much, much, much higher. Criminal organizations are seen as a major threat to society . . . smuggling is one of their activities.

The framing in companies has also been shifting from corruption being a necessary evil to their existing a moral imperative to combat corruption. In recent company reports of progress on anti-corruption, it was asserted that:

> Corruption undermines social and economic development and adds to the cost of participating in global trade . . . We maintain near elimination of facilitation payments on our own ships while continuing to develop our compliance programme [*sic*] on corruption . . . We aim to eliminate corruption in the maritime industry through both multi-stakeholder [*sic*] collaboration and our own operations . . . a maritime industry free of corruption that enables fair trade to the benefit of society at large.

Several concrete examples from trials of blockchain applications document the possibilities to improve transparency and accountability when blockchain becomes a means to: a) log the flow of products; b) exchange digital documents; and c) execute smart contracts without human interventions when conditions are met (e.g., the granting of export permission). The use of blockchain addresses issues arising from the lack of trust amongst systems as well as among actors, that were previously exploited to enable corruption. A senior director in EUCT explained:

> Blockchain makes it possible for actors that do not trust each other to share data. There was an actual case when not even the authorities in a single country trusted each other. One agency did not trust another to access their data, they thought that for example a customs officers couldn't be trusted to release a specific certificate or something because he might be corrupt. The problem was about the traceability of information from the initial moment it was created and here it turned out that blockchain was a very good solution.

The bridging of data silos was showcased when the blockchain-based solution initially tested in AFCT was trialed by a customs organization in the Middle East. Among other advantages, the blockchain solution appeared to eliminate the possibility of a corrupt officer deliberately stalling the issuance of certificates, such as a certificate of origin (Pa3) as part of the shipping process, and going unnoticed. As a manager at SHIPCo recounted:

> If someone at the port says that you need to pay extra fees because goods needed to [be stored] while waiting for a missing certificate, you can actually check that against [blockchain application] and see if it's true.

Furthermore, a trial by customs in an Eastern European country demonstrated how blockchain helped to detect fabricated or otherwise incorrect documentation in the shipping process (Pb5 and Pb6). A manager of SHIPCo explained:

> Customs officers compared the data provided in the import declaration with the reliable data from the blockchain-based bill of lading. The found that the weight had been incorrectly stated in the import declaration. . . . In another test, the product category stated to tax authorities was different from what was found on the blockchain. I'm not sure what happened to that in the end, but the authorities asked us to provide data from the blockchain to use in a legal case.

In several customs authorities, blockchain has been proven to detect goods seeing with false (or sometimes, not quite accurate) declarations to avoid or lower taxes and tariffs. For example, it was discovered that garlic was declared as vegetables, e-bikes as bikes, and shoes as sandals. Additionally, by cross-checking declarations against other documents mediated by the blockchain, it was discovered that the values of goods were incorrectly declared as being just below the threshold value for tariffs and duty to assessed.

Positive effects were also confirmed by EUCT customs officers, who explained how they used blockchain to verify that data provided through other channels had not been tampered with:

> We have already several use cases based on [blockchain application]. In one, we were the exiting harbor. We then traced the goods from its origin to wherever it finally went. And this we did as part of putting sanctions on the trader. We also used [blockchain application] for goods from the US, where based on the information we got from the shipping line we couldn't fully trace the real flow, we couldn't determine what was the real export and import . . . then we used it [blockchain application] to look for additional information and based on this we could determine that this was indeed a valid process and in this case we used the data to de-risk the shipment.

For EUCT, automating this task using reliable data from the blockchain partially addressed situations where customs officers were influenced to overlook control tasks (Pa10) or approve export declarations (Pb4). However, blockchain would not take out the human element of manual inspections when needed. A customs officer could still pretend to inspect a container and inappropriately approve it.

Contributing to the institutional field's move toward anti-corrupt practices is the growth in the numbers of the institutional entrepreneurs pushing for anti-corruption. An EUCT customs manager also mentioned that this drive to combat corruption benefitted from national governments' support:

> The national government provides extra money for the fight against what they call the undermining of society. We get extra people, extra stuff, extra money to fight against undermining.

As expressed by several government officials, corruption is being regarded as a barrier to economic growth by the public, and extensive petty corruption is upsetting them. The growing number of anti-corruption bodies, such as the MACN, the World Economic Forum, and the UN have been successful in their strategies to shape public opinion and are becoming a major resource being drawn upon by institutional entrepreneurs. The use of

blockchain to counter corruption is a strategy encouraged by authorities in Canada, Russia, Saudi Arabia, Netherlands, and the United States.

Because of this changing identity, along with schemas and rules, and the strengthened legal system against corruption acting as a dependable resource, local officials are gradually becoming aligned to anti-corruption, some enthusiastically. For example, a group of customs officials proudly showcased how they had closed off possibilities for corruption, though there were others who regretted seeing an important part of their income being diminished. In the latter group, some have remained passive, and a few have been more active in defending the corrupt order. Some officials involved in, or aiding corruption, had informal lists of companies who were still paying facilitation fees and those who were not. One of the managers at SHIPCo recollected:

> One time there was a local officer that wanted us to pay, even though we just had made an agreement with some senior people in the government that we wouldn't do that. So we called our contact, and he called someone who then called the local officers saying something like "I told you not [to] ask [SHIPCo] to pay. Anyone else is fine, but not [SHIPCo]!"

Shipping companies are also getting aligned on the issue of fighting corruption. Importantly, senior executives in large international companies are very keen to embrace blockchain as it reduces the risk of company employees acting illegally, behavior for which the executives would be held personally responsible in the strengthened anti-corruption legal system. A senior manager at SHIPCo confirmed that it was a consideration that "*US authorities were acting as the world's police*." Within SHIPCo, this has generally been seen as good for business as it has leveled the playing field between actors, but the senior manager added that:

> It would have been even better if some of the collected fines went back to the states where corruption happened, to ease the poverty that was one of the root causes for corruption.

While being opposed to corruption, many of the shipping companies are continuing to engage in or support behaviors that are, in our definition, instances of corruption; however, in strict terms, such behaviors are not illegal, an example being the reliance on extended opening hours of ports or expedient issuing of certificates. Such behaviors have thus not been targeted in the blockchain implementation.

SHIPCo's edict of anti-corruption and strong legal systems, on the social side, and blockchain, on the technical side, are the key resources against corruption that shippers are drawing on. Through digitalization, including the strategic use of digital payments and the immutable logging of transactions and documents, a strong legal system can overcome the monitoring challenges that arise from the spatial and temporal distance in shipping. The use of blockchain in shipping forms an immutable record of shipping behavior that is a basis for accountability. Specifically, it automates critical steps in the process flow ("*avoiding human intervention is always good*") through smart contracts, and for the rest of the steps, it records all deviations in the process flow in way that allows for investigation of abnormalities.

Era 4 (Approx. 2020-2030): Unified and Normalized Anticorrupt Identity

We are just entering Era 4, and as mentioned earlier, this section is prospective in nature, highlighting anticipated effects of blockchain implementation. These anticipated effects are

based on interviews with shipping industry experts and other participants who have been closely involved with blockchain in shipping. Extrapolating from past experiences, some of our interviewees indicated that key actors in the shipping industry are expecting that the anti-corrupt order will continue to evolve, and eventually become normalized. The processes being put in place, enabled by digitization and specifically by blockchain, are more than likely to result in commercial practices with higher efficiency than in the case of manual processes. In addition, as key actors and countries move to require digitized documentation flows and processes *without exception*, participation in these practices will increasingly become *a prerequisite for being part of the trade community*. Therefore, the anti-corrupt order that we saw as starting to dominate during Era 3 is expected to become the norm in Era 4. The anti-corruption actors will become the new defenders of the institution, and to be part of the business network, all parties will be expected to comply with the systems (including blockchain applications) with the capability to detect corrupt practices.

Anticipating the future use of Blockchain, experts and representatives of the involved actors envisioned two distinct effects. First, along the same lines as already seen in test cases, extended possibilities of corruption detection in both corruption-related process manipulation and document forgery are expected. An AFCT customs representative acknowledged that they had chosen to implement a blockchain application to digitize trade flow because it "curbs documentary fraud" (Pa4-Pa5). Similarly, an AFCT customs official acknowledged that similar to how EUCT customs uses trade data from the blockchain to conduct risk analysis, they expect that the solution will offer "to get data from the primary source" and thus "offers improved information traceability" of pro forma invoices (Pb7) and can be used to detect "fake organizations" set up to carry tax and other duties (Pb8). Ultimately as blockchain allows for digitizing more steps of the trade process, EUCT customs expects it will reduce the need for agents involved in the manual facilitation of import (Pa9).

Second, despite the evidence that blockchain can be used to detect incidents of corruption, a TECHCo manager explained the *prevention rather than detection* would be the key effect of blockchain:

> I think that you know most of our thinking on this has been that it will indirectly reduce corruption . . . We're not, for example, building products to directly attack the problem. We're building products to increase transparency . . . create audit trails. Although I do think that the, you know . . . the interesting thing about blockchain is it's an immutable distributed audit trail. And . . . you have to have it. You have to have a registered identity on the blockchain network in order to interact with it. So it becomes very hard to change records after the fact . . . So I think I think it makes corruptions [*sic*] more difficult.

In both AFCT and EUCT, customs authorities assert that the main use of blockchain is corruption prevention. Detection was seen as an interim state before involved actors realized that there are new possibilities that authorities have to control corrupt practices. Instead of combating corruption through detection alone, blockchain encourages good behavior of avoiding corrupt practices, that is, makes it attractive for the parties to do the right thing, from the customs point of view. In AFCT, the initial blockchain trial in 2015 was associated with the implementation of the World Customs Organization's Authorized Economic Operator (AEO) schema, where trusted traders who submitted all relevant documents in advance and voluntarily complemented them with additional requested

data received benefits such as rapid customs clearance. A local manager involved in the test explained that based on experiences in other parts of the government, the ambition was to make possible and incentivize anti-corrupt practices. The manager said, "*The aim was to double the AEO companies*."

Similarly, in EUCT, customs authorities appear to see the use of blockchain as way to reduce the risks in different trade flows. EUCT customs categorize trade flows as green, yellow, or blue depending on the availability of reliable data. A senior customs manager explained:

> With [blockchain application], we are what I call splitting haystacks. From one big haystack to three different ones. We have green trade flows that involve only actors that are seen as reliable and that are open. Here we have traders and trade routes that are categorized as 'trusted'. The green flow is a haystack with low risk. The blue flow is where we have no additional data, here we know very little. This [blockchain application] de-risk trade flows from blue to yellow. Yellow flows are where we have a lot of additional data that we can trust and cross-validate, like the one from [blockchain application]. We are trying to create a haystack where we know there is nothing wrong. So, [blockchain application] does not help us to find risk, but to create a haystack where we know there is nothing wrong. It's more focused on de-risking. And then we can focus inspections on the blue stack. Of course, the green and yellow flows can be hijacked, but the blue flow is where we need to focus. Here we have trade flows with a non-compliance rate of 90-95 perecent.

Therefore, while initial use of blockchain has been used to detect and prosecute corrupt behaviour, the future strategic use of blockchain in global shipping rests in its potential to encourage transparent behaviors and appropriate declarations that prevent corruption. As asserted by a customs expert from TECHCo:

> You can, however, make it easy to identify them [corrupt parties] and prosecute them. And then that maybe prevents them from taking bad actions.

In summary, Table 4 presents an overview of how the identified points of corruption have been, and are expected to be, impacted by digitalization. It is noteworthy that current use of digital technologies including blockchain applications has not demonstrated significant impact on some of the corruption points identified earlier. Regarding this matter, two contributing explanations are put forward. The first is that some human actions fall outside the domain addressed. This includes many elements of port operations, for example, managing the gating in to the port (Pa1) and port operating hours (Pa2). A manager from AFCT explained the impact of the "human element":

> There are these who want to comply. But then there are these who want to circumvent the system. Technology won't determine the number of invoices you upload or the value you write on those invoices. People will still declare that they bring in X number of tires in a container, but then you find that they have smaller tires hidden within the big ones. And then a customs officers need to look carefully and report what he sees [they see]. This human element is not taken care of by [blockchain application], but the intention is that you can track [actions] and that you can also reward those who are complying with special green-light processing. Technology is a way to support those who want to comply . . .

Similarly, a manager from SHIPCo noted the futility of isolated technical solutions to deep-rooted social issues such as corruption and fraud, saying:

> You can just as well push a button when you shouldn't as you can stamp a document when you shouldn't.

A manager from EUCT customs echoed this sentiment regarding the limits of blockchain:

> The problem with blockchain and trade is the physical dimension. Yes, this is secure from the point when the information exists. But how do you ensure that the initial data is correct? That what you put on the blockchain is actually the real phytosanitary certificate? That's the main issue, that point of converting the physical to digital.

This reasoning applies to the issuing of certificates (Pb1-Pb3). *If what gets stored on the blockchain is incorrect in the first place, it does not matter that it is an immutable record*. In the end, the context of blockchain use is critical to its impact. And while there is initial evidence as well as extensive agreement on the potential of blockchain to combat corruption, a local manager in AFCT offered an opinion representative of many actors:

> There is always a lot of enthusiasm in the prospect, but when it comes to actual implementation things are typically slower. . . . It's going to be a gradual process.

Discussion

While the overall nature of the model, presented in Figure 2, is similar to that of Misangyi et al. [62] and other high-level frameworks based on institutional theory, a number of issues specific to addressing corruption with blockchain have been revealed. These issues are highlighted and specified via the alphabetical numbering of arrows in Figure 2.

The first is a clear realization that *blockchain is only a resource—it is not a solution, certainly not a silver bullet*. The material properties of data integrity and data sharing do not automatically offer desirable affordances to the actors or get actualized without a supportive set of conditions. This assertion is consistent with discussion on "*the increasingly symbiotic relationship between IT and organization*" [96] where blockchain, on the one hand (see *arrow a*, Figure 2), enables transparency across data silos and high level of data security in

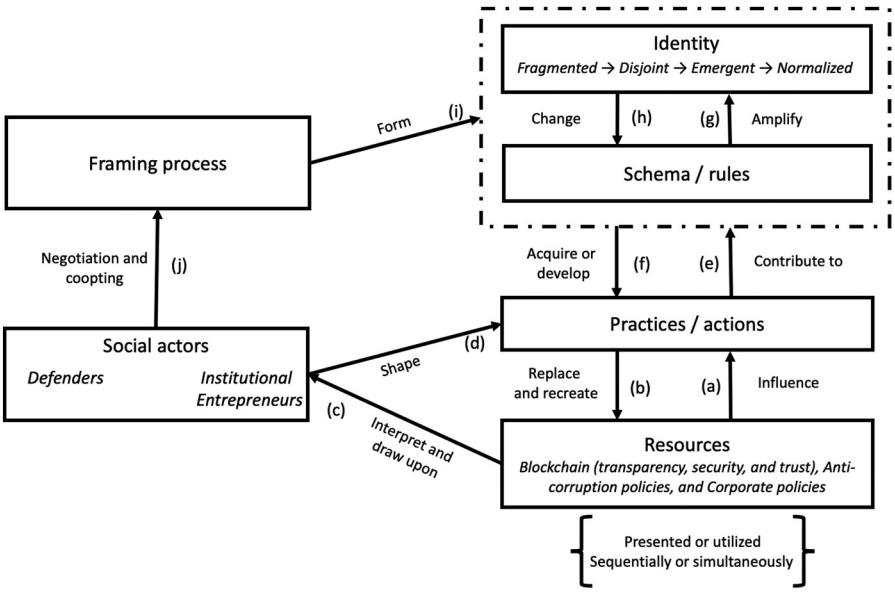

Figure 2. A framework depicting how corruption is reproduced, resisted, and eradicated, based on [62].

the supply chain, and, on the other hand, new practices emerge that replace social interaction, for instance while handing over paper documents, with digital documents, leading to the need for additional technologies and policies (*arrow b*).

These digital documents together with blockchain affordances and anti-corruption and corporate policies become new resources for the institutional entrepreneurs to draw upon *(arrow c)*. In this context, the ability of institutional entrepreneurs, in particular, the relevant corporate actors to shape current practices is critical (*arrow d*). It is also important to recognize the fact that as a resource, blockchain is leveraged to combat corruption in two distinct ways. One is that it provides *transparency to processes and immutable information flows*. The other, generally seen as more relevant by operational staff, is its potential to enhance *efficiency in the supply chain* by speeding up the flow of goods through better monitoring [53]. In our investigated case, the blockchain was, among other things, an entry point to an important commercial business network requiring its use. This means that actors were inclined to use the blockchain for the purpose of *shipping efficiency* and *commercial development*, thereby minimizing adoption resistance, but by doing so, they also indirectly contributed to implementing anti-corrupt schemas and routines (*arrow e*). This dual use of the blockchain made it particularly powerful as a basis for an anti-corruption strategy.

Second, given that a blockchain had been *strategically positioned as having a key role in combating corruption within a global shipping institutional field* (an interorganizational setting with multiple social actors), a significant social change process supported by existing resources had to ensue for given social actor(s) to form an identity against corruption (*arrow i*), to contribute to the changing of the existing schema (*arrow h*), and to develop routines consistent with this new self-conception (*arrow f*) [10]. This understandably required several rounds of negotiation, cooptation, or even coercion amongst relevant social actors *(arrow j)* before a world-view could emerge, one that would support a specific identity with respect to corruption [cf. 14]. This formation of a normalized identity (such as *one related to a moral imperative to fight a societal malady*) required a framing that resonated with all/most actors and would become difficult to oppose. It also required the actors coalescing around this identity to develop the capacities to implement associated schemas and routines. In our case, relevant authorities needed to acquire or develop the expertise *(arrow f)* consistent with the schema/rules to assess blockchain-based documents with the same precision as experienced officers would have previously inspected the stamps of potentially falsified paper documents. They also needed to develop analytical capacities to benefit from the sudden availability of product-tracking data from the blockchain application *(arrows a and e)*.

Third, social resources such as policies or technological resources such as blockchain will seldom lead to institutional change. Our study suggests that there has to be *a simultaneous, sequential, or recursive harnessing of social and technological resources* to create the right foundation for change over time. Changing identity takes time, and the anti-corruption schema/rules (*arrow g*) that are expected to guide the future need to be amplified in support of such identity transformation [36].

The sociotechnical nature of the process is clear. For example, blockchain without a supportive social system (laws, schema, and routines undermining corruption, etc.) would be rendered ineffective through workarounds and other avoidance mechanisms to the digitization of critical documents in the process. It is also clear that institutional

entrepreneurs play a crucial role because they have to help destroy institutional barriers [54] in the adoption of anti-corruption programs [65]. They do this based on their interpretation of the role of blockchain (*arrow c*) and how they change practices and invest in the technology (*arrow d*) [22]. It is interesting to note that it was in part the individual motivation of top managers at SHIPCo to not get into legal trouble (given the emergence of resources in the form of new corruption laws, i.e., the new understanding of corruption laws) that triggered their interest in implementing blockchain; in other words, the initial motivation was not really to eradicate corruption but arguably self-preservation (*arrows a and b*). Thus, the *social interpretations* of digital technologies and other resources such as laws by different social actors need to be understood and harnessed.

Finally, we note that blockchain is an advanced digital technology enhancing our ability to observe and monitor in and around organizations to get desirable information [80]. Observations depend on the *transparency* of key participants' actions [38]. Together with backbone technologies such as enterprise resource planning systems, customer relationship management systems, and data analytics packages, blockchain is known to contribute to transparency by providing data integrity and traceability [71] to participants in the ecosystem, including shippers, third-party logistics providers, freight forwarders, intermodal operators (e.g., train operators), government authorities, ocean carriers, and financial service providers. Our analysis shows a critical distinction between blockchain and preexisting digital technologies in the form of traditional IS. While IS acted to digitize islands of work, blockchain is acting to connect the islands in a way that has been acceptable to the actors; this is needed given the amount of coordination required to combat corruption. Past attempts, for example, the European Union–funded Information Technology for Adoption and Intelligent Design for E-Government and Common Assessment and Analysis of Risk in Global Supply Chains projects, have failed to develop a common global supply chain infrastructure. One explanation has been that the proposed centralized infrastructure was not adopted because it was not able to protect sensitive corporate data. However, in the case of blockchain, there is the perception that it offers a secure solution. Blockchain works at the intersection of actors, expanding upon and unleashing the capacities of existing digital components. Without these preexisting digital technologies, the blockchain implementation would not have been possible, but without the blockchain, these isolated IS could not have been integrated. Once integrated, the black boxes in the product flow change in nature, and do not readily support the possible use of service providers as corruption agents, by shipping companies and shippers/traders. In this sense, blockchain reduces opportunities for corruption.

This discovery puts further emphasis on the need to better understand blockchain relative to the concept of transparency. It is widely recognized that transparency is a key feature of blockchain technology; however, the ways in which blockchain contributes to transparency has yet to be conceptualized. Inspired by and adapting the discussions on transparency in the management and organizational literature [18] and the findings in our study, we can conceptualize four closely related roles of blockchain transparency:

- In the first role, blockchain can be seen as a *reconnaissance technology* that collects data, for example, documents, from a process or activity and makes it available to the

network. This can increase the awareness of process performance by sharing data across networks.

- In the second role, it can be seen as a *visualization technology* that provides data and information about a process or set of activities. This can reduce uncertainty about the arrival of goods.
- In the third role, it can be seen as *a regulation technology* which offers close, constant, and comprehensive control of processes. This can affect any participant in the network by enforcing a Big Brother effect, which increases compliance.
- In the fourth role, it can be seen as *a disclosure technology* that makes new or previously unknown data and information known. This can improve market efficiency by reducing information asymmetry but can also be a cause of serious opposition from actors seeking to keep some information hidden.

Rossi2018 This conceptualization addresses the call to theorize blockchain at the protocol, interaction, and application levels [74]. Previously, governance and trust issues could be found at protocol level [17], while at the interaction level, we found framing related to generativity [5], and at the application level, we found privacy framing [19, 23]. The aforementioned blockchain transparency conceptualization brings interorganizational relationships and ecosystems into the transparency literature and thereby goes beyond the traditional boundaries of transparency research that have generally been confined to organizations and individuals. This conceptualization is not only an answer to some calls for research but also a call for new research.

Practical Implications: Blockchain as a Strategy to Combat Corruption

Our study brings at least three important implications for anti-corruption actors with an interest in employing blockchain as a strategy to combat corruption. First, the basis for such use of blockchain is *an understanding of how closely corrupt and fraudulent practices are tied to the overall institutional identity of corruption*. Succeeding with a blockchain strategy to combat corruption is *as at least as much a network-building process as it is a technology development and implementation initiative.*

Second, among the resources leveraged to this end, a unique aspect of blockchain is that its functionality is twofold. *It is both a tool for efficiency and for transparency*. While for corruption combating, the transparency feature is directly applicable, the efficiency feature makes compliance more attractive. In our study, we showed that actors were migrating toward the anti-corruption practice *initially* not because of their shared non-corruption identity but because of the efficiency gains in marketing as well as operations activities that the technology promised. The role of promised operational efficiency gains, along with providing access to new partners that could potentially make the process more commercially viable, was particularly useful in getting buy-in from different stakeholders. In other words, *successful implementations of blockchain should seek to harness these dual features of the technology* to build critical mass.

Third, blockchain is not a stand-alone technology. Instead, it works by catalyzing and extending already existing digital technologies. In our case, it made existing data in silos accessible and added security to existing document processing so that the eventual handling of the most sensitive documents became acceptable. However, without this pre-installed

base of digital components, the implemented blockchain would not have been effective. Therefore, practice should recognize that *blockchain needs a foundation of an elaborate installed digital base* when used as part of a strategy to combat corruption.

It is also important to acknowledge some limitations or boundary conditions of our work on using blockchain in combating corruption. They include the following:

- When key social actors in the field do not deem a given behavior as illegal or something wrong, it does not seem to matter when such a behavior is highlighted as undesirable by actors considered outsiders—it does not seem to trigger any change. For example, given that restricting opening hours for the purpose of being able to charge exorbitant out-of-hours fees was not illegal, the practice continued to be seen as normal for one of the ports be studied.
- Some corruption, for example, the issuing of certificates, happens outside the field of blockchain. Officers can push a button and issue a false certificate when they should not. With the false certificate in the system, blockchain cannot help in preventing or detecting corruption or fraud.
- Finally, of the different kinds of corruption, *grand corruption is very different in nature* than the corrupt practices we discuss, and consequently, would need a radically different approach to combat relevant behaviors.

Conclusion

Corruption, whether systemic or petty, and related fraud still remains in the global shipping industry, but the mechanisms to effectively fight it are emerging. Historically, anti-corruption bodies and organizations have relied upon policies and legal framework to battle corruption. However, with digital technologies in general and blockchain in particular, anti-corruption actors have new resource at their disposal. We see how blockchain can fight both process and document-related corruption on a global scale across continents and economies, bringing to attention the misuse of funds for improper gift giving, kick-backs, or inappropriate social activities [59,60], in the same way that an enterprise resource planning (ERP) system provided transparency for internal business processes and activities. In particular, institutional entrepreneurs, whether individuals or organizations, have drawn upon these new emerging resources such as blockchain and social enablers such as policies and laws in their quest to change the world. They have sought to transform practices and to shape the identity of the industry—toward corruption-free operations. While this was happening, a progressively shrinking number of defenders of the old legacy of corruption were hard at work; however, resources such as technologies and policies/laws, and the framing of the corruption cause continued to resonate with the key stakeholders, and resulted in the development of a shared purpose and identity, making it increasingly difficult to defend the old legacy. While we celebrate the positive developments, drawing on Rousseau [75], we hasten to add a note of caution that transparency alone cannot accomplish the anti-corruption goals; in fact, it "*may instead of exposing frauds, only conceal them; for prudence is never so ready to conceive new precautions as knavery is to elude them*." In other words, there is a chance that regardless of the sophistication of blockchain, fraudsters and dishonest individuals will find new ways to corrupt the system or use the system to their advantage [52].

The framework (Figure 2), adapted from [62], presents a theoretical understanding of how corruption can be resisted, and eradicated in the long run. Clearly, digital technologies have an important role, and blockchain, with its unique material properties, is becoming part of the technological strategy of many firms. Blockchain is sometimes changing ingrained, undesirable behaviors, and can be part of a sociotechnical solution to corruption in global shipping and elsewhere.

Acknowledgement

The authors are thankful for the helpful guidance from editors and the anonymous reviewers throughout the process.

References

1. Addo, A.A.; and Avgerou, C. Information technology and government corruption in developing countries: Evidence from Ghana customs. *MIS Quarterly* (forthcoming).
2. Agbo, C.C.; Mahmoud, Q.H.; and Eklund, J.M. Blockchain technology in healthcare: A systematic review. *Healthcare*, *7*, 56 (2019), 1–30.
3. Alzahrani, N.; and Bulusu, N. Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain. In, Ferretti, S., and D'Angelo, G., (eds.), *CryBlock'18: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, Munich, Germany: Association for Computing Machinery, 2018, pp. 30–35.
4. Anand, V.; Ashforth, B.E.; and Joshi, M. Business as usual: The acceptance and perpetuation of corruption in organizations. *Academy of Management Perspectives*, *18*, 2 (2004), 39–53.
5. Andersen, J.V.; and Bogusz, C.I. Self-organizing in blockchain Infrastructures: Generativity through shifting objectives and forking. *Journal of the Association for Information Systems*, *20*, 9 (2019), 1242–1273.
6. Andersen, T.B. E-Government as an anti-corruption strategy. *Information Economics and Policy*, *21*, 3 (2009), 201–210.
7. Arayankalam, J.; Khan, A.; and Krishnan, S. How to deal with corruption? Examining the roles of e-government maturity, government administrative effectiveness, and virtual social networks diffusion. *International Journal of Information Management* (2020), 102203.
8. Ashforth, B.E.; and Anand, V. The normalization of corruption in organizations. *Research in Organizational Behavior*, *25*(2003), 1–52.
9. Avgerou, C. Explaining trust in IT-mediated elections: A case study of e-voting in Brazil. *Journal of the Association for Information Systems*, *14*, 8 (2013), 420–451.
10. Avgerou, C.; and Bonina, C. Ideologies implicated in IT innovation in government: A critical discourse analysis of Mexico's international trade administration. *Information Systems Journal*, *30*, 1 (2020), 70–95.
11. Bahoo, S.; Alon, I.; and Paltrinieri, A. Corruption in international business: A review and research agenda. *International Business Review*, *29*, 4 (2020), 101660.
12. Bai, C.; and Sarkis, J. A supply chain transparency and sustainability technology appraisal model for blockchain technology. *International Journal of Production Research* (2020), 1–21.
13. Bailey, D.; Faraj, S.; Hinds, P.; von Krogh, G.; and Leonardi, P. Special issue of organization science: emerging technologies and organizing. *Organization Science*, 30, 3 (2019), 642–646.
14. Barrett, M.; Heracleous, L.; and Walsham, G. A rhetorical approach to IT diffusion: Reconceptualizing the ideology-framing relationship in computerization movements. *MIS Quarterly*, *37*, 1 (2013), 201–220.
15. Bartelt, V.L.; Urbaczewski, A.; Mueller, A.G.; and Sarker, S. Enabling collaboration and innovation in Denver's smart city through a living lab: A social capital perspective. *European Journal of Information Systems* (2020), 1–19.

16. Beck, R.; Avital, M.; Rossi, M.; and Thatcher, J.B. Blockchain technology in business and information systems research. *Business & Information Systems Engineering*, *59*(2017), 381–384.
17. Beck, R.; Müller-Bloch, C.; and King, J.L. Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*, 10 (2018), Article 1.
18. Bernstein, E.S. Making transparency transparent: The evolution of observation in management theory. *Academy of Management Annals*, *11*, 1 (2017), 217–266.
19. Bertot, J.C.; Jaeger, P.T.; and Grimes, J.M. Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, *27*, 3 (2010), 264–271.
20. Bray, J. *Facing up to Corruption 2007: A Practical Business Guide*. London: Control Risks, 2007.
21. Breit, E.; Lennerfors, T.T.; and Olaison, L. Critiquing corruption: A turn to theory. *Ephemera: Theory and Politics in Organization*, *15*, 2 (2015), 319–336.
22. Castro, A.; Phillips, N.; and Ansari, S. Corporate corruption: A review and an agenda for future research. *Academy of Management Annals*, *14*, 2 (2020), 935–968.
23. Chanson, M.; Bogner, A.; Bilgeri, D.; Fleisch, E.; and Wortmann, F. Blockchain for the IoT: Privacy-preserving protection of sensor data. *Journal of the Association for Information Systems*, *20*, 9 (2019), 1274–1309.
24. Charoensukmongkol, P.; and Moqbel, M. Does investment in ICT curb or create more corruption? A cross-country analysis. *Public Organization Review*, *14*, 1 (2014), 51–63.
25. Cho, Y.H.; and Choi, B.D. E-government to combat corruption: The case of Seoul metropolitan government. *International Journal of Public Administration*, *27*, 10 (2004), 719–735.
26. Dawes, S.S. Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly*, *27*, 4 (2010), 377–383.
27. Dong, W.; Liao, S.; and Zhang, Z. Leveraging financial social media data for corporate fraud detection. *Journal of Management Information Systems*, *35*, 2 (2018), 461–487.
28. Drescher, D. Blockchain Basics: A Non-Technical Introduction in 25 Steps. Berkeley, CA: Apress, 2017
29. Fedotov, Y. Remarks at the Twenty-First session of the Commission on Crime Prevention and Criminal Justice. https://www.unodc.org/unodc/en/speeches/2012/remarks-at-21stccpcj.html, 2012
30. Felin, T.; and Lakhani, K. What problems will you solve with blockchain? *MIT Sloan Management Review*, *60*, 1 (2018), 32–38.
31. Garcia-Murillo, M. Does a government web presence reduce perceptions of corruption? *Information Technology for Development*, *19*, 2 (2013), 151–175.
32. Garud, R.; Hardy, C.; and Maguire, S. Institutional entrepreneurship as embedded agency: An introduction to the special issue. *Organzation Studies*, *28*, 7 (2007), 957–969.
33. Glaser, F. Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis. In T. Bui, and R. Sprague (eds.), *Proceedings of the 50th Hawaii International Conference on System Sciences* Hilton Waikoloa Village, Hawaii, USA, 2017, pp. 1543–1552.
34. Hahn, E.D.; Doh, J.P.; and Bunyaratavej, K. The evolution of risk in information systems offshoring: The impact of home country risk, firm learning, and competitive dynamics. *MIS Quarterly*, *33*, 3 (2009), 597–616.
35. Hastig, G.; and Sodhi, M.S. Blockchain for supply chaintraceability: Business requirements and critical success factors. *Production and Operations Management*, *29*, 4 (2020), 935–954.
36. Haveman, H.A.; and Rao, H. Structuring a theory of moral sentiments: Institutional and organizational coevolution in the early thrift industry. *American Journal of Sociology*, *102*, 6 (1997), 1606-1651.
37. Hileman, G.; and Rauchs, M. Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance*, *33* (2017).
38. Hood, C.; and Heald, D. *Transparency: The Key to Better Governance?* Oxford University Press for The British Academy, 2006.

39. Jabbar, K.; and Bjørn, P. Permeability, interoperability, and velocity: Entangled dimensions of infrastructural grind at the intersection of blockchain and shipping. *ACM Transactions on Social Computing*, *1*, 3 (2018), 1–22.
40. Jain, A.K. Corruption: A review. *Journal of Economic Surveys*, *15*, 1 (2001), 71–121.
41. Jensen, T.; Hedman, J.; and Henningsson, S. How TradeLens delivers business value with blockchain technology. *MIS Quarterly Executive*, *18*, 4 (2019), 221–243.
42. Kaufmann, D. Governance Matters VI: Aggregate and Individual Governance Indicators, 1996–2006. Washington, DC: World Bank Publications, 2007
43. Kim, C.K. Anti-corruption initiatives and e-government: A cross-national study. *Public Organization Review*, *14*, 3 (2014), 385–396.
44. Kim, S.; Kim, H.; and Lee, H. An institutional analysis of an e-government system for anti-corruption: The case of OPEN. *Government Information Quarterly*, *26*, 1 (2009), 42–50.
45. Kock, N.; and Gaskins, L. The mediating role of voice and accountability in the relationship between internet diffusion and government corruption in Latin America and Sub-Saharan Africa. *Information Technology for Development*, *20*, 1 (2014), 23–43.
46. Köhler, S.; and Pizzol, M. Technology assessment of blockchain-based technologies in the food supply chain. Journal of Cleaner Production, 229 (2020), 122193
47. Krastev, I. Shifting Obsessions: Three Essays on the Politics of Anticorruption. Budapest, Hungary: Central European University Press, 2004
48. Lacity, M.C. Addressing key challenges to making enterprise blockchain applications a reality. *MIS Quarterly Executive*, *17*, 3 (2018), 201–222.
49. Lange, D. A multidimensional conceptualization of organizational corruption control. *Academy of Management Review*, *33*, 3 (2008), 710–729.
50. Leng, K.; Bi, Y.; Jing, L.; Fu, H.-C.; and Van Nieuwenhuyse, I. Research on agricultural supply chain system with double chain architecture based on blockchain technology. *Future Generation Computer Systems*, *86*(2018), 641–649.
51. Lennerfors, T.T. The transformation of transparency–on the act on public procurement and the right to appeal in the context of the war on corruption. *Journal of Business Ethics*, *73*, 4 (2007), 381–390.
52. Levy, K. B*eating the box: Surveillance and resistance in the US trucking industry*. Rochester, NY: Rochester Institute of Technology, 2016.
53. Levy, K.E. The contexts of control: Information, power, and truck-driving work. *The Information Society*, *31*, 2 (2015), 160–174.
54. Li, D.D.; Feng, J.; and Jiang, H. Institutional entrepreneurs. *American Economic Review*, *96*, 2 (2006), 358–362.
55. Lio, M.C.; Liu, M.C.; and Ou, Y.P. Can the internet reduce corruption? A cross-country study based on dynamic panel data models. *Government Information Quarterly*, *28*, 1 (2011), 47–53.
56. Loklindt, C.; Moeller, M.-P.; and Kinra, A. How blockchain could be implemented for exchanging documentation in the shipping industry. In M. Freitag, H.-D. Haasis, H. Kotzab, and J. Pannek (eds.), *International Conference on Dynamics in Logistics*. Bremen, Germany: Springer, 2018, pp. 194–198.
57. Longo, F.; Nicoletti, L.; Padovano, A.d; Atri, G.; and Forte, M. Blockchain-enabled supply chain: An experimental study. *Computers & Industrial Engineering*, *136*(2019), 57–69.
58. Mackey, T.K.; and Cuomo, R.E. An interdisciplinary review of digital technologies to facilitate anti-corruption, transparency and accountability in medicines procurement. *Global Health Action*, *13*, sup1 (2020), 1695241.
59. Malaurent, J.; and Avison, D. Reconciling global and local needs: A canonical action research project to deal with workarounds. *Information Systems Journal*, *26*, 3 (2016), 227–257.
60. Martinsons, M.G. Relationship-based e-commerce: theory and evidence from China. *Information Systems Journal*, *18*, 4 (2008), 331–356.
61. Min, H. Blockchain technology for enhancing supply chain resilience. *Business Horizons*, *62*, 1 (2019), 35–45.

62. Misangyi, V.F.; Weaver, G.R.; and Elms, H. Ending corruption: The interplay among institutional logics, resources, and institutional entrepreneurs. *Academy of Management Review*, *33*, 3 (2008), 750–770.
63. Mistry, J.J. The role of eGovernance in mitigating corruption. *Accounting and the Public Interest*, *12*, 1 (2012), 137–159.
64. Montecchi, M.; Plangger, K.; and Etter, M. It's real, trust me! establishing supply chain provenance using blockchain. *Business Horizons*, *62*, 3 (2019), 283–293.
65. Montiel, I.; and Husted, B.W. The adoption of voluntary environmental management programs in Mexico: First movers as institutional entrepreneurs. *Journal of Business Ethics*, *88*, 2 (2009), 349–363.
66. Nærland, K.; Müller-Bloch, C.; Beck, R.; and Palmund, S. Blockchain to rule the wavesnascent design principles for reducing risk and uncertainty in decentralized environments. In Y.J. Kim, R. Agarwal, and J.K. Lee (eds.), *International Conference on Information Systems*, Seoul, Korea, 2017.
67. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; and Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton University Press, 2016.
68. O'Higgins, E.R. Corruption, underdevelopment, and extractive resource industries: Addressing the vicious cycle. *Business Ethics Quarterly*, *16*, 2 (2006), 235–254.
69. OECD. *Business approaches to combating corrupt practices*. OECD Publishing, 2003.
70. Perboli, G.; Musso, S.; and Rosano, M. Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. *IEEE Access*, *6*(2018), 62018–62028.
71. Pierce, L.; Snow, D.C.; and McAfee, A. Cleaning house: The impact of information technology monitoring on employee theft and productivity. *Management Science*, *61*, 10 (2015), 2299–2319.
72. Pu, S.; and Lam, J.S.L. Blockchain adoptions in the maritime industry: A conceptual framework. *Maritime Policy & Management* (2020), 1–18.
73. Raghupathi, W.; and Wu, S.J. The relationship between information and communication technologies and country governance : An exploratory study. *Communication of the Association for Information Systems 28*, 12 (2011), 181–198.
74. Rossi, M.; Mueller-Bloch, C.; Thatcher, J.B.; and Beck, R. Blockchain research in information systems: current trends and an inclusive future research agenda. *Journal of the Association for Information Systems*, *20*, 9 (2019), 1390–1405.
75. Rousseau, J.-J. *The Social Contract and other Later Political Writings*. Cambridge, UK: Cambridge University Press, [1762] 2018.
76. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; and Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*, 7 (2019), 2117–2135.
77. Santiso, C. Will blockchain disrupt government corruption. Stanford Social Innovation Review. Retrieved April 10, 2019, from Stanford Social Innovation Review: https://ssir. org/articles/entry/will_blockchain_disrupt_government_corruption
78. Sarker, S.; and Sarker, S. Exploring agility in distributed information systems development teams: An interpretive study in an offshoring context. *Information Systems Research*, *20*, 3 (2009), 440–461.
79. Sarker, S.; Chatterjee, S.; Xiao, X.; and Elbanna, A. The sociotechnical axis of cohesion for the IS discipline: Its historical legacy and its continued relevance. *MIS Quarterly*, *43*, 3 (2019), 695–720.
80. Scott, A.; Balthrop, A.; and Miller, J.W. Unintended responses to IT-enabled monitoring: The case of the electronic logging device mandate. *Journal of Operations Management* (2020).
81. Senior, I. Corruption, the Goverment and the private sector: Why IT matters and what can be done. *Economic Affairs*, *24*, 2 (2004), 22–29.
82. Silva, L.; and Hirschheim, R. Fighting against windmills: Strategic information systems and organizational deep structures. *MIS Quarterly*, *31*, 2 (2007), 327–354.

83. Singh, G.; Pathak, R.D.; Naz, R.; and Belwal, R. E-governance for improved public sector service delivery in India, Ethiopia and Fiji. *International Journal of Public Sector Management*, *23*, 3 (2010), 254–275.
84. Srivastava, S.C.; Teo, T.S.; and Devaraj, S. You can't bribe a computer: dealing with the societal challenge of corruption through ICT. *MIS Quarterly*, *40*, 2 (2016), 511–526.
85. Sullivan, C.; and Burger, E. E-residency and blockchain. *Computer Law & Security Review*, *33*, 4 (2017), 470–481.
86. Sun Yin, H.H.; Langenheldt, K.; Harlev, M.; Mukkamala, R.R.; and Vatrapu, R. Regulating cryptocurrencies: A supervised machine learning approach to de-anonymizing the bitcoin blockchain. *Journal of Management Information Systems*, *36*, 1 (2019), 37–73.
87. Transparency-International. 2009. Retrieved January 20, 2020 from https://www.transparency.org/en/cpi/2009
88. Vogl, F. Waging War on Corruption: Inside the Movement Fighting the Abuse of Power. Lanham: Rowman & Littlefield Publishers, 2012
89. Walsham, G. Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems*, *4*, 2 (1995), 74–81.
90. Walsham, G. Doing interpretive research. *European Journal of Information Systems*, *15*, 3 (2006), 320–330.
91. Wang, L.; Luo, X.R.; and Jurkat, M.P. Understanding inconsistent corruption control through e-government participation: Updated evidence from a cross-country investigation. *Electronic Commerce Research* (2020), 1–28.
92. Wang, S.; and Qu, X. Blockchain applications in shipping, transportation, logistics, and supply chain. In *Smart Transportation Systems 2019*: Springer, 2019, pp. 225–231.
93. Wolfensohn, J. A back-to-basics anti-corruption strategy: Economic perspectives. *Electronic Journals of the United States Information Agency*, *3*, 5 (1998), 17–19.
94. WorldBank. *The World Bank Annual Report 2012*. The World Bank, 2012.
95. Yang, C.-S. Maritime shipping digitalization: Blockchain-based technology applications, future improvements, and intention to use. *Transportation Research Part E: Logistics and Transportation Review*, *131*(2019), 108–117.
96. Zammuto, R.F.; Griffith, T.L.; Majchrzak, A.; Dougherty, D.J., and Faraj, S. Information technology and the changing fabric of organization. *Organization Science*, *18*, 5 (2007), 749–762.
97. Ziolkowski, R.; Miscione, G.; and Schwabe, G. Decision problems in blockchain governance: Old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems*, *37*, 2 (2020), 316–348.

About the Authors

Suprateek Sarker is Rolls-Royce Commonwealth Commerce Professor at the McIntire School of Commerce, University of Virginia. His research, which largely uses qualitative or mixed- method approaches, has been published in many leading journals. He serves (or has served) on a number of editorial boards, including *Information Systems Research, Journal of Management Informatio Systems* (as a member of the editorial board), *MIS Quarterly, Decision Sciences, Information & Organization* (as a senior editor), and *Journal of the AIS* (as the editor-in-chief). He is President-Elect and a Fellow of the Association for Information Systems. He has been awarded honorary doctorates by the University of Jyväskylä (2016) and by Copenhagen Business School (2020, to be conferred).

Stefan Henningsson is a Professor at Department of Digitalization, Copenhagen Business School, Denmark. His research addresses managerial aspects of IT in contexts that include corporate mergers and acquisitions, international trade processes, and the digital transformation of firms. His work has been published in academic journals including *Journal of Management Information Systems, Journal of Information Technology, European Journal of Information Systems, Information Systems Journal*, and *Journal of Strategic Information Systems*, and has also appeared in practice-oriented journals such

as *MISQ Executive* and *Cutter Business Technology Journal*. Dr. Henningsson is an associate editor of *Information Systems Journal* and *MISQ Executive*.

Thomas Jensen is an Assistant Professor at Copenhagen Business School's Department of Digitalization. Previously, he was an industrial researcher at Maersk, where his research led to the innovations later developed as TradeLens. He has worked at a variety of IT firms, including Microsoft and SAP. His research interests focus on ERP systems, international trade, information infrastructures and platforms, blockchain-based technology, and e-commerce.

Jonas Hedman is a Professor at the Department of Digitalization, Copenhagen Business School. He received a Ph.D. University of Lund, Sweden. Dr. Hedman's research interests include cashless society, business models, payment eco-systems, and sport digitalization. His work has appeared in *European Journal of Information Systems, Information Systems Journal, Journal of Information Technology, MIS Quarterly Executive*, and othervenues. He is an associate editor of *Information Systems Journal* and *Electronic Commerce Research and Applications*.