Blockchain Technology, Inter-organizational Relationships and Management Accounting

A Synthesis and a Research Agenda

Kostic, Nikola ; Sedej, Tomaz

Document Version
Accepted author manuscript

Published in:
Accounting Horizons

DOI:
10.2308/HORIZONS-19-147

Publication date:
2022

Blockchain technology, inter-organizational relationships and management accounting: A synthesis and a research agenda

Nikola Kostić*
Copenhagen Business School
nk.acc@cbs.dk

Tomaz Sedej
Copenhagen Business School
tse.acc@cbs.dk

*Corresponding author

ABSTRACT

Blockchain technology is increasingly emerging as an important organizational phenomenon, especially for collaboration across firm boundaries. Over the past three decades, accounting scholars have shown significant interest in management accounting and control mechanisms that are used by actors to sustain inter-organizational relationships. We outline fundamental technical features and limitations of permissioned blockchain technology and analytically propose blockchain as an empirical concept with implications for management accounting practices that underpin inter-organizational collaboration, trust, control, and information exchange. Particular focus of the analysis is on the interplay between the technical capabilities of blockchain technology and inter-organizational management control procedures. Based on this analysis, we develop a series of propositions that theorize how these procedures affect the way in which blockchain is enacted in inter-organizational relationships, and how they are affected by blockchain in turn. The paper concludes with a research agenda for accounting scholars and offers directions for further research.

Keywords: Blockchain; Management Accounting; Inter-organizational Relationships; Management Control; Information Systems; Collaboration.

I. INTRODUCTION

This paper is motivated by the rise to prominence of an innovative and arguably organizationally disruptive distributed database technology colloquially referred to as blockchain, and its potential in inter-organizational relationship (IOR) settings. In the IOR literature it is generally understood that legally autonomous firms essentially play a "mixed motive game" (Schelling 1960), which entails a mixture of mutual dependence and conflict, of partnership and competition. In other words, IOR partners have overlapping but ultimately separate profit motives (Anderson, Christ, Dekker, and Sedatole 2014). Blockchain technology's core attributes allow legally independent parties that may or may not fully trust each other to conduct and reliably control mutual interactions without reliance on a single controlling entity (Risius and Sproher 2017). This makes blockchain highly suitable for IORs, where a mix of private and common goals is inherently present (Castañer and Oliveira 2020). Against this backdrop, we conceptualize blockchain technology as an inter-organizational information infrastructure and analyze its potential and ramifications in IOR settings, with a specific focus on the management control and governance implications. We define IORs as voluntarily initiated collaborative arrangements between legally independent firms that involve information exchange, sharing or co-development of products and services, and can include partner contributions of technology, capital, or firm-specific assets (Gulati and Singh 1998; Dekker 2004). More specifically, in our analysis we focus on formal, purposeful, non-equity-based contractual IORs resulting from negotiations between organizations that remain legally independent in the access to, exchange, and/or joint generation of resources (Caglio and Ditillo 2008; Castañer and Oliveira 2020). This refers to IOR forms involving transactional types of interactions[1] (e.g. strategic alliances, supply chain relationships, networks, coalitions, industry

[1] The concept of a "transaction" is understood as occuring "when a good or service is transferred across a technologically separable interface" (Williamson 1985, 1).

consortia, outsourcing agreements), and excludes those where at least one of the negotiating organizations ceases to operate as a distinct legal entity as a result of those negotiations (e.g. mergers and acquisitions) (Castañer and Oliveira 2020).

Organizing transactions between firms involves significant control challenges that have been the topic of extensive research by management accounting scholars (Baiman and Rajan 2002; Dekker 2004; Reusen and Stouthuysen 2020). This topic is particularly salient in inter-firm interactions involving blockchain, since the technology allows for multilateral collaborative arrangements that can encompass several traditional IOR forms. Examples of a blockchain project can include a strategic alliance between an IT vendor and a client, through which a solution is developed that is, in turn, partly governed through a consortium that includes the client's industry rivals (Jensen, Hedman, and Henningsson 2019). The solution is used to foster interactions between traditional supply chain partners, but also independent bodies such as authorities and regulators from different countries (Jensen et al. 2019; Zavolokina, Ziolkowski, and Bauer 2020). To focus the analysis, based on a review of IOR literature we outline collaboration, trust, inter-organizational control, and information exchange as the four areas that are the most relevant to investigate in relation to blockchain technology. We analyze literatures within each of these areas with a focus on management control issues, identify recurring and pertinent themes, and consider how each could be impacted by blockchain. Based on this discussion, we develop theoretical propositions that collectively inform a research agenda for accounting scholars.

Our paper makes several contributions. Firstly, we contribute to the accounting literature on management control in inter-firm settings. We analytically specify blockchain as an inter-organizational information infrastructure and propose it as an empirical concept with implications for transaction hazards (Williamson 1985) and the corresponding formal and informal management control remedies in IOR settings, namely trust, partner selection, and contracting (Dekker 2004, 2008; Ding, Dekker, and Groot 2013; Anderson, Chang, Cheng, and

Phua 2017a). In doing so, we discuss the interplay between the technical capabilities, operational realities and limitations of blockchain technology, and inter-firm management control procedures that both impact how blockchain is enacted in IORs and are themselves impacted by blockchain. In discussing technical capabilities of blockchain technology, we focus on permissioned blockchains and emphasize tamper evidence and reliability of records, multi-party consensus and automatic execution of agreements codified in smart contracts as technological attributes salient for IORs. Accordingly, we discuss their limitations. Further, we discuss governance choices in IORs in the presence of blockchain, namely partner selection, specification of procedures for information exchange and the determination of the nature and scope of the collaboration between partners. Additionally, we analyze the interplay between blockchain and inter-firm controls and provide novel insights on the multilateral effects of blockchain on trust between IOR partners, and the design and implementation of inter-firm contracts.

Secondly, we analyze different strands of accounting literature that often explore management control issues separately, and supplement the analysis with contributions from organizational and information systems studies on the origins, nature and dynamics of inter-firm collaboration, as well as issues regarding inter-firm information exchange. We synthesize the arguments in a theoretically consistent manner in the form of a series of propositions. By integrating and recombining evidence from existing literature on IORs and blockchain, we offer novel insights on two complex technological and organizational phenomena, and take a step towards formulating new theory on management control implications of blockchain technology in IORs.

Thirdly, we contribute to the growing literature that examines blockchain technology as an organizational phenomenon (Beck, Müller-Bloch, and King 2018; Murray, Kuban, Josefy, and Anderson 2019; Kumar, Liu, and Shan 2020; Lumineau, Wang, and Schilke 2020). We explicitly focus on permissioned blockchains and provide a discussion of their technical capabilities and limitations in the context of inter-firm transacting. In other words, the paper contributes to advancing our understanding of what blockchains can and cannot do in an IOR context, and outlines an agenda for future research on blockchain in management accounting.

The remainder of the paper is structured as follows. First, we review the literature that marks a point of departure for our overarching argument that blockchain is an important inter-organizational and management accounting phenomenon, focusing on permissioned blockchains. Generic terms like "blockchain technology" or "blockchain" are used for ease of exposition throughout the paper. Second, we outline an organizing framework based on an analysis of literature on IORs in management accounting and related fields. Third, we identify and discuss the most prevalent issues within each of the outlined areas most likely to be impacted by the use of blockchain technology. Based on this discussion, we develop a series of theoretical propositions. We conclude with a synthesis of outlined arguments and present a research agenda for accounting scholars.

II. BLOCKCHAIN AS AN INTER-ORGANIZATIONAL AND ACCOUNTING PHENOMENON

Blockchain technology enables multiple independent parties to jointly generate, maintain, synchronize, and update a shared set of authoritative records. Further, it facilitates decentralized management of information and supports algorithmic enforcement of shared agreements in the form of smart contracts (Rauchs et al. 2018b). A smart contract is a means by which obligations can be recorded, triggering other obligations that can be set up to operate in an automated way (Gans 2019). Benefits stemming from blockchain's distributed data management, consensus mechanisms, and automated execution through smart contracts are viable primarily for transactions that can be handled exclusively through blockchain (i.e. endogenously), but also for highly standardized, verifiable and codifiable transactions, as those can be reliably referenced on the blockchain even though the original data sources are exogenous to it[2]. In IOR settings blockchain provides the infrastructure for proprietary databases of IOR partners to interact, thereby allowing the partners to transfer business-relevant information (e.g. about orders, receipts, payments, etc.) or digital assets across firm boundaries without sacrificing data privacy (Cao, Cong, and Yang 2019; Kumar et al. 2020).

Thanks to its ability to build a tamper-resistant[3] audit trail and simplify settlement and reconciliation between organizations, blockchain has seen fast adoption particularly within the areas of supply chain management, finance, and accounting (Yermack 2017; Lacity and Van Hoek 2021a). Blockchain has attracted interest of many established firms that have engaged in advanced trials or have major commercial projects in production. Examples include but are not limited to logistics and supply chain companies (Jensen et al. 2019; Lacity and Van Hoek 2021a), pharmaceutical firms (Mattke, Maier, Hund, and Weitzel 2019), car industry actors (Zavolokina et al. 2020), banks (e.g. JPMorgan Chase[4]), accounting firms and consultancies (e.g. Deloitte[5], EY[6]), and retailers (e.g. Walmart) (Lacity and Van Hoek 2021a, 2021b; Lumineau, Wang, Schilke, and Huang 2021). Each of these projects brings together up to hundreds of heterogeneous partners that work collaboratively on the development and deployment of different blockchain-based solutions for their inter-organizational environments. A recent study by Stratopoulos, Wang and Ye (2021) analyzes corporate disclosures from the SEC Edgar database and finds that blockchain is increasingly adopted as a fundamental technology that improves business processes, further classifying it as a "relatively mature technology". These developments suggest that blockchain has emerged as

[2] See Appendix A for a discussion on some fundamental blockchain and smart contract characteristics, as well as relevant transaction characteristics for blockchain-based transacting in IORs.
[3] The records on a blockchain are made persistent by replicating the data across multiple nodes, and tamper-evident by linking them through cryptographic hashes (Rauchs et al. 2018b).
[4] For more details see: https://www.jpmorgan.com/global/technology/blockchain
[5] For more details see: https://www2.deloitte.com/content/dam/insights/us/articles/2019-global-blockchain-survey/DI_2019-global-blockchain-survey.pdf
[6] For more details see: https://www.ey.com/en_gl/blockchain

an economically significant technology with salient real-world business implications, although it is worth noting that in some cases it is still in the experimental phase, and surrounded by technological, economic, and operational uncertainties.

Blockchain in accounting research

The Institute of Chartered Accountants in England and Wales (ICAEW), one of the world's oldest and largest accounting organizations describes blockchain as "[…] an accounting technology, […] concerned with the transfer of ownership of assets, and maintaining a ledger of accurate financial information. For accountants, using blockchain provides clarity over ownership of assets and existence of obligations" (ICAEW 2018, 3). Financial records have traditionally been maintained by individual entities in a centralized manner, exhibiting an orientation to accounting practices that Hopwood (1996) described as being hierarchical in nature. Blockchain on the other hand offers a radically different (i.e. distributed) alternative for transaction recording in a multi-party setting. According to some authors (e.g. Abadi and Brunnermeier 2018), this could revolutionize recordkeeping of financial transactions and ownership of data.

Contemporary accounting studies predominantly examine the use of blockchain technology within the context of financial accounting. Perhaps because of the intuitive link between the concept of a blockchain ledger and accounting ledgers, Coyne and McMickle (2017) considered the possibility of blockchain becoming a more secure, immutable alternative to current ledger database solutions. Most frequently discussed benefits of blockchains are increased speed and reduced costs of maintaining and reconciling ledgers (Dai and Vasarhelyi 2017), real-time accounting (Yermack 2017), increased security and control (Peters and Panayi 2016) and automation of accounting and auditing rules that could be programmed onto the blockchain. Dai and Vasarhelyi (2017) further argue that blockchain could facilitate "tripleentry accounting" by acting as a "neutral intermediary" that would enhance the reliability of firms' financial statements. The authors suggest that each account in a contemporary double-entry bookkeeping system could have a corresponding blockchain account. Cao et al. (2019) consider the use of permissioned blockchains and zero-knowledge proof algorithms in accounting and auditing and show that blockchain adoption can lower both regulatory and auditing costs, and increase audit quality. The study further sheds light on how accounting data and their management affect the behaviors of firms and their monitors/regulators by providing an infrastructure for independent databases to interact without sacrificing proprietary data privacy.

In summary, the existing literature offers a developing understanding of the effects of blockchain technology on financial reporting practices of firms and real-time reconciliation and auditing of accounting records. It remains largely unknown, however, how blockchain adoption impacts inter-organizational management control mechanisms that are used to support IORs. Therein lies the research gap that we address in this paper. Our study responds to Caglio and Ditillo's (2020) recent call for management accounting and control research to explain the changes brought forth by the use of blockchain technology pertaining to how firms interact, and organize and control IORs. To the best of our knowledge, ours is the first study to perform a systematic examination of the interplay between blockchain technology and both formal and informal management accounting and control mechanisms in IORs, and formulate actionable theoretical propositions for accounting scholars. We further highlight how collaboration and information-exchange issues manifest in and are affected by firms' adoption and use of blockchain technology, thereby contributing to the growing literature on the organizational implications of blockchain-based systems.

III. ORGANIZING THEORETICAL FRAMEWORK

In this section we analyze the literature on IORs in accounting and related fields and delineate an organizing theoretical framework consisting of four main areas to explore when considering the implications of the use of blockchain technology in IORs. The framework is presented in Figure 1. It is important to note that these topics do not exist in isolation but are strongly interrelated, with considerable overlap between the relevant theoretical concepts.

[Insert Figure 1 here]

Collaborative arrangements between legally autonomous parties that do not readily fit the “market-hierarchy” dichotomy (Coase 1937; Williamson 1985) have become central to economic activity (Salvato, Reuer, and Battigalli 2017; Anderson and Dekker 2014). Consequently, they have been recognized as a distinct kind of “hybrid” organizing (Williamson 1985, 1991). These hybrid organizational arrangements can take a variety of forms (e.g. strategic alliances, supply chain relationships, networks, coalitions, industry consortia, outsourcing agreements), and have been referred to by authors as “inter-organizational relationships”, “inter-firm settings”, “hybrid organizational forms”, and “networks” (Caglio and Ditillo 2008). We adopt inter-organizational relationships as a universal term. Understood in this way, IORs do not represent mere deals and strategic agreements, but are also entities characterized by information-sharing and decision-making processes, boundary spanning individuals, boards and committees, databases and integrated computer systems, as well as other material and immaterial resources, all of which entail practical organizational challenges (Gulati, Wohlgezogen, and Zhelyazkov 2012).

Management accounting and control studies of IORs (e.g. Håkansson and Lind 2004; Kajüter and Kulmala 2005; Anderson et al. 2014; Grafton and Mundy 2017) find that a situation of partial conflict exists between partners even when collaboration comes with unambiguous and observable advantages and strong incentives for partners to establish and maintain the partnership. Moreover, some IOR forms (e.g. supply-chain relationships, networks, strategic alliances, outsourcing agreements) exist in conditions of somewhat unstructured authority. Litwak and Hylton (1962) observe that collaboration between partners is necessary to preserve these IORs, yet it is often the case that no single entity possesses sufficient formal authority to be able to impose collaboration through fiat. Since blockchain is by design a multi-party system (Glaser 2017) with functionalities that inherently imply mutual interdependence and sequential interaction between parties, a certain level of collaboration between partners is necessary both ex-ante, and after the blockchain solution becomes operational. Collaborating firms that implement a blockchain system will likely need to identify potential future benefits and clarify expectations for the collaboration ex-ante. Accordingly, inter-firm collaboration is the first area of the framework.

Research in accounting and economics (e.g. Baiman and Rajan 2002; Williamson 1993; Clemons and Hitt 2004; Dekker 2004) discusses opportunism and coordination as notable management control issues with implications for IOR theory and practice. The concept of "opportunism" refers to the deliberate incomplete or distorted disclosure of information (Williamson 1985). Examples of opportunism discussed in the literature include ex-ante behavior such as deliberate misrepresentation of a firm's true attributes (Arrow 1985), and misappropriation of information by the recipient that cannot be legally prevented, and benefits from which cannot be contracted on (Baiman and Rajan 2002; Clemons and Hitt 2004). The examples also include ex-post shirking on quality, effort or information provision (Baiman and Rajan 2002). These can create transaction hazards (Williamson 1985; Dekker 2004; Reusen and Stouthuysen 2020) and tension between partners, which necessitate that different formal and/or informal safeguards and control mechanisms be put in place to mitigate the hazards and manage the IOR.

An important informal management control remedy for transaction hazards is inter-firm trust (Dekker 2004). Blockchain is often described as a "trust-less" technology able to replace trust in an intermediary with trust in consensus rules and underlying code (Catalini and Gans 2020). In the case of permissioned blockchains this can additionally involve trust in a "gatekeeper" that grants access to the system (Rauchs et al. 2018b), and other firms that participate in the network. Consequently, some level of familiarity and ex-ante trust needs to be established between partners. This makes the concept of trust (Rousseau, Sitkin, Burt, and Camerer 1998) critical to analyze in our context, and was identified as the second area of the framework.

Unlike inter-organizational arrangements backed by extensive contracts such as franchise agreements, IORs that are in the focus of this study do not rely solely, or sometimes even primarily, on extensive contracts to achieve control or coordination (Anderson, Dekker and Van den Abbeele 2017b). Incomplete contracts that typify IORs (Baiman and Rajan 2002) and the associated residual risks that in some cases preclude inter-firm transacting are made sustainable through the use of management control mechanisms such as improved measurement of actions and outcomes, and joint collaborative practices that enhance information sharing across firm boundaries and opportunities for formal and informal monitoring (Dekker 2004; Ding et al. 2013; Anderson et al. 2017a). Implementation of blockchain technology inevitably involves creating a network of partners, which in turn involves the use of formal controls, making literatures on partner selection (Dekker 2008; Dekker and Van den Abbeele 2010; Neumann 2010), and inter-firm contracting (Poppo and Zenger 2002; Anderson and Dekker 2005; Reuer and Ariño 2007; Ding et al. 2013) particularly salient sub-areas to analyze. It is in this space, termed "inter-organizational control" in our framework, that management accounting studies have made notable contributions to understanding the nature of IORs as a modern, interconnected organizational form (Anderson and Dekker 2014).

Management accounting research has identified "information openness" as an important theme related to the functioning of different forms of IORs such as supply chain relationships (Baiman and Rajan 2002; Schloetzer 2012; Reusen and Stouthuysen 2020), networks (Håkansson and Lind 2004; Kajüter and Kulmala 2005), and alliances (Nicolaou, Sedatole, and Lankton 2011; Christ and Nicolaou 2016). Christ and Nicolaou (2016) find greater collaboration intensity[7] to be associated with greater information system integration as well as the implementation of a larger portfolio of controls between partners in an alliance[8]. This further makes the establishment of a common information infrastructure a salient issue in the context of IORs. Common information infrastructure is here seen as the "blueprint" for the interaction patterns through which collaborating firms share the risks and govern the partnership (Christ and Nicolau 2016). Given that blockchain technology enables transparent, reliable and efficient exchange of information in networks of legally independent organizations, we conceptualize it as a common information infrastructure in IORs and specifically discuss management control implications of blockchain-enabled information exchange as the fourth major area of the framework.

IV. DISCUSSION

In this section we scrutinize literatures on collaboration, trust, inter-organizational control, and information exchange. The explicit goal of the ensuing discussion is to critically analyze the existing knowledge about these concepts, focusing on the implications of blockchain technology for each of the four main areas of the organizing framework. Major arguments resulting from the discussion are synthesized into theoretical propositions intended to serve as building blocks of a research agenda for future efforts in blockchain-related management accounting research. It is our contention that this research agenda could help to equip

[7] Christ and Nicolaou (2016) describe collaboration intensity as referring to the importance of multiple alliance objectives to a firm.
[8] The authors use "alliance" as an aggregate term to connote inter-organizational relationships ranging from joint ventures to strategic partnerships and supply chain relationships.

accounting scholars with “instruments” to critically study management accounting and control issues in IORs as this important organizational form increasingly becomes interrelated with an emerging technological phenomenon that is blockchain.

Collaboration

Inter-firm collaboration is an important source of competitive advantage for organizations because it enables value creation through accessing and combining complementary resources and capabilities of partnering firms (Coletti et al. 2005). At the same time, Gulati et al. 2012 warn that inter-firm collaboration can be very risky and complex. White (2005) suggests that collaboration necessitates that relationship partners are able to develop and maintain an inter-organizational interface for communication, and internally adapt in response to relationship partners’ actions or the changing external environment.

Cooperation and coordination have been identified in the IOR literature as two distinct yet complementary facets of inter-firm collaboration (Salvato et al. 2017; Gulati et al. 2012). In line with Castañer and Oliveira (2020) and Gulati et al. (2012) we define cooperation as a complex concept including a willingness to work toward the achievement of agreed-on goal(s) in a manner corresponding to a shared understanding about contributions and payoffs, as well as actions taken by the partners to achieve the stipulated collective goal(s). The reasons for firms to engage in cooperation normally involve sharing of investment risks and pursuing a number of technological, commercial and operational goals that they might be unable to obtain through arm’s-length transactional relationships (Gulati et al. 2012). Explicit definition of terms is important in IORs, as they provide a clear framework that defines each party’s rights and obligations, as well as the principles and procedures of the cooperation (Luo 2002; Anderson and Dekker 2005). This is even more critical when introducing blockchain in IORs because of the formalized nature of data exchange, validation, and governance mechanisms. Moreover, blockchain creates a common information infrastructure between partners in the sense that all the relevant parties share an identical record of data that have been exchanged according to a network-wide protocol.

As partners agree on the inputs and outputs of the relationship, a mutual interdependence is created (Pfeffer and Salancik 1978). This represents a situation in which partners are dependent on one another in various ways to accomplish organizational goals (Reusen and Stouthuysen 2020), and become vulnerable to the actions of the other (Parkhe 1993). This issue is particularly salient in IORs formed between competitors. On the one hand, a firm's rivals can possess the necessary capabilities and/or resources needed for a joint project. On the other hand, past rivalry can cultivate a lack of trust (Trapido 2007). Interestingly, Davis, Kahn, and Zald (1990) point out that competitors are more likely to become aware of one another through professional associations than are non-competitors. Stuart (1998) further argues that competitors often choose to cooperate because they are "better able to evaluate and internalize the know-how of technologically similar firms", and to avoid duplication of effort. This argument is known as "competitive embeddedness", a notion that competition increases mutual awareness, which in turn breeds familiarity and knowledge-based competence trust (Trapido 2007). Many blockchain projects we observe today are a result of multilateral cooperation between heterogeneous actors including industry competitors (Jensen et al. 2019; Mattke et al. 2019), alliance and supply chain partners (Jensen et al. 2019), financial institutions such as banks[9] and insurance firms[10], as well as authorities and research and educational institutions (Zavolokina et al. 2020). Rival companies form initiatives and consortia (Lacity 2018; Mattke et al. 2019) to address industry inefficiencies with the use of blockchain. Notable examples of blockchain-enabled supply chain applications include TradeLens, a supply chain platform intended for

[9] For recent examples see: https://www.crowdfundinsider.com/2020/03/158652-standard-chartered-joins-tradelens-a-leading-blockchain-based-supply-chain-management-solution-developed-by-ibm-maersk/ and https://www.ledgerinsights.com/hsbc-production-contour-blockchain-trade-finance/

[10] For more details see: https://smartmaritimenetwork.com/2021/03/30/tradelens-electronic-bills-of-lading-approved-by-international-group-of-pi-clubs/

secure exchange of documentation across global supply chains (Jensen et al. 2019), and IBM Food Trust, a solution for tracking product provenance (Lacity and Van Hoek 2021a). In these projects[11], rival companies collaborate to create value for a wide ecosystem of organizations.

Taken together, the factors described above should alleviate some adverse selection concerns that would otherwise present obstacles for initiating cooperation. Further, blockchains can employ encryption methods such as zero-knowledge protocols[12] that allow information providers in a blockchain system to safeguard proprietary information, while verifying transactions (Cao et al. 2019). Confidentiality and control of the data are major issues in inter-firm cooperation, especially between competitors (Bechini, Cimino, Marcelloni, and Tomasi 2008). At the same time, competitive embeddedness is crucial for establishing cooperation in these cases, as partners get acquainted via professional associations and discuss pressing issues within their industries (Trapido 2007). Accordingly, we predict existing cooperation in IORs to be conducive to the introduction of blockchain technology. Furthermore, we contend that blockchain facilitates new cooperative relationships that were previously not feasible due to concerns over data security and the inability to integrate numerous and heterogeneous sets of actors.

***Proposition 1*: Introduction of blockchain technology is facilitated by existing cooperative relations in IORs, and facilitates new ones both in number and nature.**

On the one hand, cooperative relationships can provide cost savings such as a decrease in

[11] Technologically, both projects are based on Hyperledger fabric, an open source protocol developed through a collaborative effort hosted by the Linux Foundation and supported by firms such as IBM, Intel, and SAP (Stratopoulos and Calderón 2020). For a detailed description of how a complete blockchain transaction is initiated, validated, and recorded on the blockchain [hyper]ledger see Calderón and Stratopoulos (2020).
[12] A zero-knowledge protocol (ZKP) is a set of cryptographic algorithms that can ensure both the validity and confidentialiy of records on a blockchain. Cao et al. (2019) describe a ZKP as a proof of a statement by one party (the prover) to another party (the verifier) without conveying any additional information to the verifier, other than the correctness of the statement.

monitoring costs, which can lead to increases in efficiency and profitability (Smith, Carroll, and Ashford 1995). On the other hand, the central problem of cooperation is that firms often have only partly overlapping interests, and may pursue incongruent goals if left to their own devices (Schelling 1960). Axelrod and Keohane (1985) further argue that cooperation is only possible in situations where there is a combination of complementary and opposing interests. Misaligned interests may cause partners to shirk or try to claim more benefits than initially agreed through holdup or misappropriation of partners' resources (Gulati et al. 2012). To help explain the success or failure of inter-firm cooperation Axelrod and Keohane (1985) identified three dimensions: (1) the pattern of payoffs; (2) the shadow of the future; and (3) the number of players. Payoffs strongly influence the development and maintenance of cooperation as each relationship partner expects to attain a net positive value (Parkhe 1993). The shadow of the future argument suggests that considerations about the future promote cooperation, as firms compare immediate benefits from deceiving the partners with the loss of potential future gains resulting from breaking the agreement (Axelrod and Keohane 1985). The number of actors and the structuring of their relations can also play a role in inducing cooperation, as it might be difficult to detect and punish the potential defectors when many parties are involved (Axelrod 1979).

The three dimensions proposed by Axelrod and Keohane (1985) are relevant to consider when implementing blockchain in IORs. Participating in a blockchain network requires a priori investments and acceptance of the predefined rules by a given partner firm, which signals a "credible commitment" (Williamson 1983) to the joint project. This can include significant upfront costs to develop and implement the blockchain system. For firms with complex legacy systems that would need to be completely replaced or made compatible with blockchain this could also include significant switching costs. This means that, in order to justify those investments, firms will likely need to determine payoffs for each party before they fully commit to the project. Moreover, development of a blockchain network requires joint efforts across organizational boundaries, making the potential benefits of the solution contingent on the status of network adoption. This means that the payoffs will depend on the success or failure of the entire network, rather than on individual partners, which should help to align their goals and induce cooperation. The blockchain ledger possesses a critical attribute of tamper-evidence, which improves monitoring through higher transparency of data. Consequently, the "shadow of the future" should dissuade actors from engaging in opportunistic behavior. Similarly, blockchain's inherent data sharing and governance protocols, the sequential nature of the data recording process, as well as the auditability of the shared ledger should enable partners to inexpensively and reliably identify a party trying to submit erroneous transactions, irrespective of the number of actors in the network.

***Proposition 2*: Blockchain use has a positive effect on goal alignment and fosters cooperation in IORs because the economic benefits incurred by partners depend on the success or failure of the entire blockchain network.**

One of the most desirable results of inter-firm cooperation is achieving effective *coordination* (Smith et al. 1995). In line with Castañer and Oliveira 2020 and Gulati et al. 2012, we define inter-firm coordination as deliberate and orderly alignment or adjustment of partner's actions in the process of determining common IOR goals. Coordination is normally associated with information sharing, decision-making and feedback mechanisms, which aim to align partners' efforts and combine their resources in a productive manner (Gulati et al. 2012). Regular exchange of information between partners in an IOR has been termed "procedural coordination" by Sobrero and Schrader (1998). It refers to day-to-day communication that allows partners to adapt their activities to one another and handle disputes and exceptions.

Blockchain establishes a common information infrastructure, meaning that all the relevant partners share identical data references. It further enables new kinds of distributed architectures, as the process through which data is exchanged and recorded relies on responsible and accurate record-keeping by a network of legally independent and mutually constraining "record keepers". This should lead to a significant simplification of procedural coordination, particularly in terms of information sharing and the handling of disputes. A practical illustration of this point are notable efficiency gains in handling shipments between supply chain partners, which have in the past involved (and in many cases still do) numerous ad-hoc manual follow-ups through email, phone calls and the like. On the other hand, within a blockchain-based network, mutually agreed upon decision-relevant data references are made available to all the pertinent parties for given events in near real-time (Jensen et al. 2019)[13]. For accounting scholars, and accountants more generally, such an effect is salient because it can markedly improve performance of administrative work in participating firms (Anderson and Lanen 2002; Lacity and van Hoek 2021b). Moreover, programmable rules (i.e. smart contracts) could be used to automate several routine day-to-day procedures even when the data being exchanged is not fully endogenous to the blockchain system. The latter is feasible for highly verifiable and codifiable transactions, which alleviates the "oracle problem"[14]. It is further enabled through standardization of data formats, network-wide protocol rules, and tamper-evidence of the ledger, thereby making the execution of these procedures more efficient, as well as more reliable.

***Proposition 3*: Implementing blockchain in IORs simplifies procedural coordination between partners.**

Trust

[13] For a detailed technical description of an operational application of a permissioned blockchain and smart contracts in a supply chain context, see Lacity and Van Hoek (2021b).
[14] For a brief discussion on the oracle problem see Appendix A.

The concept of trust has been widely discussed in the literature in the fields including accounting, economics, psychology, sociology, and philosophy. Rousseau et al. (1998) analyzed the meaning of trust across these disciplines and defined it as a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behavior of another. Development of inter-firm trust is often argued to be the basis for maximizing the value of IORs (Ireland et al. 2002; Dekker 2004). The presence of inter-firm trust can reduce transaction costs (Gulati 1995), spur desirable behavior, lead to decreased levels of conflict, facilitate coordination by enabling greater knowledge and information transfer (Poppo, Li, and Zhou 2016), increase managerial flexibility, and reduce concerns about opportunistic behavior (Gulati et al. 2012). Since it is most often impossible to manage all risks through formal agreements and controls, firms at least partly rely on trust to sustain IORs (Dekker 2004; Reusen and Stouthuysen 2020). Existing research has identified different forms of trust, contingent on the bases from which it is reached. A prominent classification relevant for management accounting studies of IORs differentiates between *competence trust* and *goodwill trust* (Dekker 2004; Anderson et al. 2017b; Reusen and Stouthuysen 2020). While competence trust refers to a partner's technical *ability* to perform activities as agreed in the contract (Dekker 2004), goodwill trust refers to a firm's confidence in predicting partner's *intentions* to act as agreed (Nicolaou et al. 2011).

Williamson (1993) discusses calculative aspects of IORs involving trust where managers believe that the costs of acting opportunistically, which refer to the forgone future value of transactions, will be greater than benefits associated with opportunistic actions. Susarla, Holthacker, and Krishnan (2020) outline two major sources of trust in this context. The first reflects the potential for future economic gains from continued exchange, which has an important disciplining effect on exchange partners to adhere to informal agreements (Baker, Gibbons, and Murphy 2002) and show willingness to be vulnerable to the actions of the other. Axelrod and Keohane (1985) refer to this disciplining effect as the "shadow of the future".

More specifically, this effect refers to the threat of the collaboration being terminated, which further entails that the partners could forego all potential future benefits resulting from it (Gibbons and Henderson 2012). The second source is partners' bilateral reputation for satisfactory performance in prior contracting, which assuages partners' fear of performance failure despite full cooperation, or in other words reduces performance risk (Anderson and Dekker 2009; Susarla et al. 2020). This reputation represents an intangible economic asset (Klein and Leffler 1981; MacLeod 2007) and arises as partners observe each other's performance over repeated interactions, from which they infer commitment to uphold contractual agreements (Susarla et al. 2020).

Blockchain is often referred to as a "trust-less" technology (Xu et al. 2017), which might imply that it has the potential to replace trust within and between organizations. However, while blockchain's cryptography and consensus mechanisms are able to replace trusted intermediaries when transferring cryptocurrencies, the same does not fully apply to IORs. Namely, entries in permissioned blockchains (e.g. in supply chains) often refer to exogenous data sources. While asset ownership might be verified by blockchain records, their condition, location and worth must still be assured (ICAEW 2018). Although the blockchain, in and of itself, cannot prevent a party from breaking an agreement, or act opportunistically, inbuilt mechanisms could decrease the *possibilities* for opportunism. Research has found that third-party information based on a partner's history of cooperation with other firms, even in the absence of own knowledge based on prior interactions, enables the formation of trust through a *transference process* (McEvily, Perrone, and Zaheer 2003), where third parties "roll over expectations" from existing relationships to newly formed ones (Uzzi 1997).

In permissioned blockchains, network participants are often "competitively embedded" (Trapido 2007) vetted partners. Reusen and Stouthuysen (2020) find that third-party information has a significant effect on partners' level and dimensions of trust through "trust transfer”. The premise behind this “trust transfer” is that, other than being based on own prior experience with a given partner, initial trust impressions are also influenced by the cues provided by third parties, such as other firms in an industry (Reusen and Stouthuysen 2020). More specifically, simply knowing other firms that trusted an IOR partner is sufficient for participants’ *competence trust* to increase. In a blockchain network, such “third-party” information can be obtained simply by observing successfully executed transactions between other (vetted) participants, even when a given partner is not privy to specific information to which only directly participating or otherwise designated parties may have read, write and/or validation rights. On the other hand, *goodwill trust* is only found to increase when information about positive outcomes are available (Reusen and Stouthuysen 2020). Achieving this effect in a blockchain network of vetted participants is likely, although it might necessitate more detailed information about interactions beyond mere successful transaction execution in some cases. Combined, these features imply that while the transacting parties in a blockchain network still need to establish expectations regarding partners’ behavior and goodwill, as this represents an important aspect of the “network configuration”, they no longer need to do so solely based on direct past experience or the ongoing direct interactions with those partners (Lumineau et al. 2020). Regular monitoring of tamper-evident blockchain records, coupled with the disciplining effect of “trust transfer”, would increase the probability that opportunistic behavior will be detected and sanctioned not just by the parties directly involved in a given transaction, but by the entire blockchain network. Moreover, the transference effect of trust (McEvily et al. 2003; Reusen and Stouthuysen 2020) between network participants could help establish a multilateral reputation system (Susarla et al. 2020) in the network, thereby increasing the overall level of both competence and goodwill trust.

Proposition 4**: Introducing blockchain in IORs increases the level of both competence and goodwill trust among partners.**

Inter-organizational control

An extensive body of literature in management accounting examines governance choices of firms in IORs, explicitly recognizing the conditions that precede and largely determine these choices (e.g. the threat of partner opportunism and coordination of inter-firm tasks), as well as ways in which firms acquire information about their partners (Dekker 2004; Anderson and Dekker 2005; Neumann 2010). Selecting an appropriate partner in IOR settings is an important way in which firms can mitigate control problems, with some authors suggesting that identifying a suitable partner is critical for the overall success of an IOR (Ireland et al. 2002). Dekker (2004, 2008) further shows that the partner selection process strongly influences latter stages of the collaboration since it precedes and informs the design of contractual and other management control structures used to sustain IORs. Accordingly, "partner selection" is here referred to as the process of searching for, evaluating, and ultimately selecting a transaction partner (Dekker 2004, 2008; Ding, et al. 2013). Management accounting studies (Dekker 2008; Ding et al. 2013) conceptualize partner selection as an explicit formal ex-ante management control choice in IORs in response to the underlying transaction hazards. In these studies, the partner selection process is analyzed in terms of the time spent by firms to find exchange partners, the effort exerted to evaluate them (including the development of evaluation criteria), as well as the relative importance placed on different selection criteria in the choice of a partner (Dekker 2008; Dekker and Van den Abbeele 2010; Ding et al. 2013). The evaluation criteria include those that relate to partners' reliability and technological competencies, as well as screening of multiple suppliers and information search in networks of related parties to acquire relevant information (Dekker and Van den Abbeele 2010).

Transacting partners in a blockchain network are obligated to behave according to the collective agreement (i.e. the network configuration), as deviating behaviors would not be verified neither by the algorithm, nor other nodes in the system (Catalini and Boslego 2019). The underlying logic is not to engage in formulating elaborate terms that could be used to seek legal recourse for ex-post breaking of agreements, but rather to regulate the actions of partners from the outset (Lumineau et al. 2020). Blockchain infrastructure provides a resilient, replicated, sequentially ordered record of interactions between partners maintained by a network of legally independent actors. The latter characteristic is related to tamper-evidence of a blockchain ledger, meaning that relevant parties can readily observe and prevent potential malfeasance through some form of a "majority" vote on the state of the records (i.e. the consensus mechanism). These characteristics significantly increase the reliability of records and make ex-post observation of prior interactions less costly and less time-consuming. Reliable records validated in a decentralized manner provide a robust "third party" signal of competence and benevolence of transacting partners for the entire network (Reusen and Stouthuysen 2020), in most cases irrespective of specific levels of data-access authorization. This can, in combination with the reliability of blockchain records, mitigate transaction hazards by building a credible reputation system for IOR partners in a blockchain network. Similarly, joining the blockchain network implies that a given partner accepts the predefined governance rules (Lumineau et al. 2020). As such, the willingness of a partner to participate in a network characterized by tamper-evident records and involving automated execution of codified agreements can be seen as a precommitment not to behave opportunistically in the future (Yermack 2017), and a signal both of the intention and the ability of partners to honor the agreements (Lumineau et al. 2020) Hence, in an IOR context, blockchain technology could have profound implications for the partner selection process. Namely, the combined effect of reliability of records, ex-ante deterrence of potentially opportunistic actors, and the greater ease of observability of prior interactions should improve the process of informing and designing evaluation criteria for potential partners, and reduce partner search and selection costs in IORs.

***Proposition 5*: Blockchain technology mitigates control problems in IORs through improved partner selection.**

Contracts represent an integral part of the management control structure of IORs. Contracts are legally enforceable, voluntarily initiated documented agreements between exchange partners that provide a governance framework for their relationship and incorporate procedures, incentives, mutual obligations and dispute resolution mechanisms (Schepker, Oh, Martynov, and Poppo 2014). Contracts help partners to achieve cooperation and coordination by specifying rights and responsibilities of each party, particularize the deliverable outcomes, clarify procedures for monitoring and penalties for non-compliance, and put forth conflict resolution procedures (Poppo and Zenger 2002; Ding et al. 2013). As such, they are primarily used to control verifiable actions and outcomes. Contract complexity refers to the number and stringency of provisions in a contract (Reuer and Ariño 2007). Complex contracts understood this way are detailed and costly to develop and implement, as they include a large number of specific terms, clauses and covenants, and contain detailed agreements that serve to clarify monitoring procedures for non-compliance, and describe conflict resolution procedures that are collectively used to mitigate potential transaction hazards (Luo 2002; Ding et al. 2013). A prominent stream of research (Williamson 1985; Anderson and Dekker 2005; Reuer and Ariño 2007) focuses on contractual clauses aimed at aligning and safeguarding partners' interests, and facilitating coordination and adaptation. Banker, Kalvenes, and Patterson (2006) distinguish between aspects of activities that should be included in the contract, and those that should be monitored and suggest that a shared information exchange infrastructure enables greater contract completeness by making monitoring additional dimensions of partner performance more economical.

Fundamental technical and governance characteristics of blockchains improve reliability and ex-post observability of records. Additionally, smart contracts enable the routinization of inter-firm processes involving blockchain-endogenous data and explicit exogenous (i.e. standardized, codifiable and verifiable) data references, reducing them to a set of articulated interaction patterns that are automatically executed when predefined conditions are met. The monitoring and the execution phase of this process incur no additional direct costs. Standardization of data formats and execution patterns serves to make transactional interactions between partners in IORs more predictable, while decentralized governance mechanisms establish clear decision-making rules regarding the data exchanged in the network. Furthermore, sequential ordering of redundantly stored data among participants in the network, and the resulting tamper-evidence of the records greatly simplify dispute resolution. Taken together, and to the extent that they refer to blockchain-endogenous or otherwise explicit transactions, blockchain functionalities and smart contracts allow for more partner activities to be reliably monitored. Taking the argument one step further, the introduction of blockchain could induce firms to preemptively change their transactional practices to fit the requirements of standardization, codifiability and verifiability[15], in essence changing the nature of the transactions. Accordingly, this would enable the scope of the activities that can be reliably automatically executed, enforced and monitored through blockchain to be expanded even further. At the same time, Sheldon (2019) cautions that the proper functioning of blockchain and smart contracts depends on a secure internal controls environment. Concerns over access to transactional data and smart contracts in IORs result in a need for increased scrutiny regarding internal control over financial reporting. This can increase the complexity of the overall IT governance in an IOR, as effective controls in and "around" the blockchain and smart contracts need to be put in place in a setting involving multiple legally independent organizations (Sheldon 2019). On the other hand, Sheldon (2019) points out that this

[15] For more details on different transaction types in a blockchain environment see Appendix A.

blockchain-related increase in internal control complexity is at least partially offset by the minimization of risks related to modification of historical data, the need for data backups, batch processing between blockchain nodes, and disaster recovery of data and programs enabled by blockchain and smart contracts.

Anderson and Dekker (2005) suggest that greater exchange hazards induce firms to invest in more complex contracts. Relatedly, we contend that the functionalities of blockchain technology and smart contracts narrow the domain around which parties can be opportunistic (Poppo and Zenger 2002) and reduce information asymmetry between partners in IORs. This, in turn, lowers transaction hazards, increases the level of control over verifiable actions and outcomes and reduces the scope of activities that IOR partners need to include in formal contracts, ultimately leading to lower demand for highly complex contracts in IORs.

***Proposition 6*: Blockchain technology enables the design of less complex contracts in IORs.**

Information exchange

Over the past three decades the boundaries of a single organization have lost some of their explanatory power in defining the relevant entity for management control in many firms. The emergence of technologies for information collection, conversion, dissemination and monitoring within and across organizational boundaries has played an important role in enabling inter-organizational collaboration. A technology-enabled inter-organizational information system (IIS) often represents a primary means of information exchange across firm boundaries in IORs (Gulati and Singh 1998). As such, IISs play a significant role in the control of IORs (Nicolaou et al. 2011).

At the most basic level, the purpose of adopting IISs is to implement computerized communications among partnering organizations. Studies that investigate control and performance implications of IIS use broadly identify information sharing, standardization and process integration as practices that facilitate mutual value creation. In this context, information sharing reflects the extent to which partners exchange decision-relevant information via IISs (Schloetzer 2012). Process integration is here referred to as the extent to which partners standardize and synchronize inter-firm processes, which are in turn defined as a set of interrelated and sequential activities that are shared and executed by two or more trading entities (Schloetzer 2012). In the IIS context, standards are defined as a set of technical specifications that are agreed upon and used by IIS developers to describe data formats and communication protocols, which enable computer-to-computer communication, and in turn facilitate inter-organizational information exchange (David and Greenstein 1990; Zhu, Kraemer, Gurbaxani, and Xu 2006). For the purposes of this paper, IISs are defined as technology-enabled information systems used by two or more organizations that can facilitate creation, storage, and transmission of different types of information (e.g. operational, accounting, performance, contractual and/or strategic information) across firm boundaries (Nicolaou et al. 2011; Christ and Nicolaou 2016).

Blockchain records are considered valid only after a uniform view on the state of the ledger and the order of events (i.e. a consensus) has been reached on a collective level. This mechanism could entail high overhead costs, since the same data records need to be replicated and maintained by multiple parties (Kumar et al. 2020). Concomitantly, that same mechanism increases data integrity and reliability, as data points from multiple independent sources converge towards shared, mutually agreed upon, authoritative sequential states of records valid for the entire network. As a result, the use of blockchain is likely to significantly reduce the costs and task complexity related to the reconciliation of records, as it essentially collapses the two processes of data exchange and reconciliation of records into one. This is especially relevant in IORs, where partner interactions can be multi-tiered, and between heterogeneous parties (e.g. alliance partners from different industries, multiple suppliers, service providers, regulators). Studies have shown that a centralized (e.g. hub-and-spoke) design is pervasive in existing IIS solutions (Hart and Saunders 1997; Kumar et al. 2020), including data exchange on a point-to-point basis (e.g. through electronic data interchange (EDI) or Extensible Markup Language (XML)-based standards) (Steinfield et al. 2011). This makes the flow of information between partners less than seamless, especially in multi-tier IORs such as extended supply chains (Steinfield et al. 2011), and increases the marginal costs of integrating new partners (Babich and Hilary 2020). Taken together, this promotes an increase in transaction hazards and results in management control issues.

In the context of IORs, blockchain can be seen as a new form of an IIS. In that sense, it is comparable to other technologies which are intended for inter-firm communication, the most prominent example being EDI. EDI enables standardized point-to-point communication between independent computerized information systems, which makes them suitable for dyadic (i.e. one-to-one) or hub-and-spoke information exchange between partners (Anderson and Lanen 2002). EDI is a widely used and mature technology that can be highly effective in standardized exchanges of information such as procurement orders (Clemons, Reddi, and Row 1993). However, EDI mainly serves as a support tool in inter-firm information exchange because it lacks the ability to automatically enforce agreements (Kumar et al. 2020; Lumineau et al. 2020). The capability of autonomous enforcement without recourse to external governance apparatus (i.e. the legal system) represents a unique characteristic of smart contracts that run on blockchain, which differentiates it from other IIS solutions like EDI (Lumineau et al. 2020). Although limited by the issues of endogeneity of data references and the overall transaction standardization, codifiability and verifiability, this is nevertheless a very promising feature in the context of IORs. In sum, blockchain's core attributes enable end-to-end, multilateral (i.e. network-based) information exchange between partnering firms, as well as implementation and autonomous enforcement of agreements/business logic codified in smart contracts (Beck et al. 2018; Kumar et al. 2020), which makes them suitable for multilateral collaboration among partners in IORs.

***Proposition 7*: Blockchain technology enables network-based information exchange between partners and thus facilitates multilateral collaboration in IORs.**

The information exchanged via an IIS has itself been an important topic of inquiry among management accounting scholars. A distinction was made between coordination and control uses of information. Regarding the former, information is used as a means of planning and coordinating the interdependent activities that the collaborating parties collectively engage in (Nicolaou et al. 2011). When the primary goal of information use is control, the information is used to verify and evaluate the actions of the partner, usually by monitoring performance information with the goal of incentivizing or compelling the partner into achieving desirable or predetermined results (Nicolaou et al. 2011).

Technical attributes of blockchain technology entail that records of exchanged information contain the attributes of transparency, auditability, and consistency across databases of the involved parties. These attributes have a disciplining effect on parties by imposing high costs (e.g. exclusion from the network) on individual participants (or an insufficiently large group of participants) that attempt to unilaterally make changes to the records or propose fraudulent claims. Furthermore, smart contracts enable automated enforcement of interactions between partners. A primary way in which control is implemented via IISs is by using the system as a diagnostic tool, which means that performance information is gathered and monitored after the actions have been taken (Baiman and Demski 1980; Nicolaou et al. 2011). Consequently, introducing blockchain as the IIS in IORs should reduce control complexity through improved monitoring, self-disciplining mechanisms, and simplified performance evaluation.

***Proposition 8*: Blockchain technology reduces information exchange related control complexity in IORs.**

An aspiration to improve inter-organizational coordination through the use of IISs exhibited by an increasing number of firms has led to the development of new network standards (Zhu et al. 2006). Studies focusing on the development and diffusion of data and process standards beyond a dyadic buyer-supplier relationship (i.e. "extended supply chain" or industry level) have reported that achieving the goal of establishing a common information infrastructure is fraught with difficulties. These include factors such as heterogeneity of interests among partners (Markus et al. 2006), high cost of implementation and low reuse value of the investment for smaller partners (Steinfield et al. 2011), and difficulties in reaching an agreement on design, governance structure, and ownership of the solution. This can result in a vicious cycle where partners hold off investments, possibly rendering the whole collaboration unsuccessful (Steinfeld et al. 2011). Formation of industry-wide standard setting consortia has been proposed as a way to address these issues. Leveraging Olson's (1965) seminal work on the theory of collective action, Weiss and Cargill (1992) suggest that standards development consortia[16] have an incentive to limit membership to a group of participants with a compatible preference structure, especially large firms because they are more likely than smaller ones to influence others to adopt the standard. Furthermore, developing industry-wide IIS standards requires joint efforts across organizational boundaries, making the potential benefits of the solution contingent on the status of network adoption by the rest of the firms in the industry (Zhu, Kraemer, and Xu 2003).

[16] Weiss and Cargill (1992) refer to consortia that include organizations whose primary role is to facilitate the adoption of standards through promotional activities and compatibility testing, and those that are actively developing the technology that represents the basis of either de facto or voluntary consensus standards.

Basic requirements for the feasibility of blockchain technology include standardization (e.g. of data formats and consensus mechanisms), wide adoption, and interoperability between different platforms (Lacity 2018; Kumar et al. 2020). Kumar et al. (2020) suggest that after standards have been developed by consortia that individually could include a limited number of large firms (Weiss and Cargill 1992), the rollout of the technology is regardless likely to happen on a much wider scale and in collaboration with IT vendors and different actors in a given industry. Since blockchain interoperability is one of the key requirements for the success and the diffusion of the technology (Kumar et al. 2020), cross-platform and cross-consortia collaboration will be a major factor in its adoption (Bear and Rauchs 2020). Taken together, these arguments imply that, in blockchain-based IIS networks, most of the benefits are expected after the compatible blockchain platforms have reached a high level of diffusion. Moreover, due to the novelty of the technology and the associated lack of technical capabilities within some firms, setup costs of a blockchain network might be higher than for existing technological solutions (Kumar et al. 2020). These can be exacerbated by blockchain's inherent replicated storage requirements. Consequently, it is reasonable to expect that in situations where marginal overhead costs of running transactions are high as well as when difficulties with integrating different IOR partners exist, a more mature technology such as EDI might still prevail. We therefore suggest that wide adoption characterized in some combination by the number and heterogeneity of participants represents a major factor for blockchain adoption.

***Proposition 9*: Blockchain technology is best suited for IORs that involve numerous and/or heterogeneous partners.**

V. CONCLUSION

Blockchain is a multi-faceted innovation, namely: (1) technical - a new distributed version of a transactional database; (2) economic - offering a reliable record of transactions in a decentralized, potentially adversarial environment; and (3) organizational - given that it may fundamentally change how firms organize IORs. It is therefore likely to play an important role in major organizational and technological developments in the future. The issues related to formation and evolution of novel organizational forms have been the topic of extensive research in management accounting and control studies, making scholars in the field uniquely equipped to make sense of these important forward-looking trends. We propose that future research on blockchain in IORs should approach these issues from three perspectives: (1) dynamics of inter-firm collaboration in the presence of blockchain; (2) strategies for the design and use of formal and informal management control mechanisms in IORs; (3) the impact of distributed network-based exchange and governance of decision-relevant information. Propositions developed above act in concert to provide insights across the three perspectives. We argue that combining these insights provides a foundation for generating an understanding of the overall impact of blockchain technology in IORs.

The first suggested area for research could look in more detail into the processes leading to the development of collaboration and formation of IORs, as well as the scope of collaboration in existing IORs. Blockchain gives rise to new questions in regards to the temporal, relational and management control dynamics of inter-firm collaboration. An example of temporal dynamics are expectations about the future. Blockchain promotes collective outcomes, where expected future payoffs for collaborating firms depend on the success of the entire network, potentially leading to reversed causality effects such that future expectations shape present behavior. Scholars could explore how relational dynamics such as previous interactions and the associated levels of goodwill and competence trust between IOR partners interrelate with firms' future expectations to inform the design of formal ex-ante (criteria for partner selection) and ex-post (contracts) management control mechanisms in the presence of blockchain.

Relatedly, blockchain promotes the expansion of the pool of potential collaborators with no prior ties through the standardization of information exchange and management protocols, reliability of records and ledger auditability and tamper-resistance. Mitigating transaction hazards, and aligning and safeguarding partners' interests in such settings usually involves specification of mutual obligations and deliverable outcomes through contracts. A topic that could be investigated in this context are the control implications of expanding the pool of collaborators that can include heterogeneous sets of actors by leveraging a blockchain-based common information infrastructure and multilateral information exchange. The use of blockchain technology and smart contracts in IORs could have a notable effect on the level of frictions and transaction hazards. In turn, research should examine the implications of these changes in transaction hazards on firm boundaries and the nature of formal and informal management control mechanisms used to sustain traditional IOR forms in those new circumstances. Looking ahead, an interesting avenue for research could involve exploring these issues beyond traditional IOR settings discussed in this paper, and focus on new and emerging IOR forms such as digital platforms and ecosystems.

The second area for research could investigate how blockchain technology influences the way in which firms navigate around processes of developing and maintaining trust. Further, researchers could explore how those processes affect firms' strategies for designing formal management control mechanisms. Blockchain establishes a reliable "third party" source of information (Reusen and Stouthuysen 2020) and a "multilateral reputation system" (Susarla et al. 2020), which can have profound effects on inter-firm trust (Dekker 2004). Scholars could examine how multilateral information flows enabled by blockchain dynamically influence both competence and goodwill trust during the different stages of IORs. Similarly, a salient topic in this context is determining the levels of trust necessary to initiate new cooperative relations with heterogeneous partners. Further, studies could elucidate whether, or to what extent, trust in the overall IOR context shifts from trust between organizations to "trust in the blockchain system" (Catalini and Gans 2020) that is established through collective consensus and governance decisions pertaining to technical design characteristics of blockchain in a given case.

Blockchain simultaneously narrows the domain for opportunism and expands the scope of activities that can be reliably monitored. Smart contracts further allow for automatic execution of agreements. Combined, these functionalities suggest that inter-firm contract complexity in terms of the number and stringency of contract provisions can be reduced. On the other hand, these mechanisms will potentially increase the complexity of the internal control environment. Future research could therefore explore the effects of formalization and automation of processes and day-to-day communication through blockchain on the administrative work of accountants and the design of internal control procedures.

A third promising avenue for research could focus on the impact of new ways of exchanging and governing decision-relevant information enabled by blockchain. Exchange of information between IOR partners has been extensively studied by management accounting scholars (Baiman and Rajan 2002; Christ and Nicolaou 2011; Schloetzer 2012). While notable contributions have been made in this research stream, Caglio and Ditillo (2008) point out that, with a few exceptions, most of these studies focus on dyadic or one-to-many inter-firm relations, typically from the viewpoint of a dominant IOR partner. As a result, the conceptualization of management control mechanisms has been wedded to the notions of hierarchy and efficiency in strictly defined IOR forms (e.g. strategic alliances, buyer-supplier relationships) (Hopwood 1996). Blockchain technology as a common information infrastructure enables multilateral collaboration between partners from different IORs, as traditionally defined. Researchers should focus their attention on examining the circumstances in which blockchain could be superior to or preferred over existing solutions such as EDI. Such research could hone in on elucidating how pre-existing contractual arrangements and trust influence the design of the blockchain system. Additionally, Caglio and Ditillo (2020) point out that blockchain could question some of the conclusions of the existing management accounting literature in terms of how to control IORs. Taking into consideration the heterogeneity of actors in new collaborative arrangements enabled by blockchain, research is needed to understand how primary control mechanisms discussed in this paper may change in this context.

Looking beyond the context of the present study and our specific focus on permissioned blockchains, technological advances in the blockchain space warrant consideration as they might have implications for the arguments we presented. The vast majority of enterprise blockchain networks in the current landscape are "private" and permissioned, and are typically organized around a narrow use case with one or a few entities exerting a disproportionate influence over the network (Bear and Rauchs 2020). However, this may change in the future, and the next generation of enterprise blockchains could at least partially rely on public networks (Lacity and Van Hoek 2021a). Ernst & Young (EY), for instance, recently launched Nightfall, a set of protocols supporting private transactions on a public Ethereum blockchain (Lacity, Steelman, and Cronan 2019) in anticipation of a market pivot from private to public networks (Lacity and Van Hoek 2021a). The idea behind Nightfall is essentially to create a "virtual private blockchain", akin to a virtual private network (VPN) connected to the public internet (Lacity et al. 2019; Lacity and Van Hoek 2021a). Bear and Rauchs (2020) similarly predict the rise of semi-public (permissioned), application-agnostic "super networks", which will support the development of numerous novel use cases, possibly operating beyond industry boundaries. These developments might have interesting implications for the issues discussed in this paper and offer exciting opportunities for researchers to extend our arguments.

For almost three decades, management control issues in IORs have been an important topic of inquiry among accounting scholars. We hope that the propositions developed in this paper, together with the suggested areas for further research, will support laying the groundwork for management accounting researchers interested in blockchain in the context of IORs. The research agenda outlined in this section is aimed at inspiring novel and impactful research that could significantly increase our understanding of blockchain technology as an inter-organizational phenomenon and develop a more comprehensive notion of IORs and management controls that are used to sustain them in the ever-changing technological and organizational landscape.

REFERENCES

Abadi, J., and M. Brunnermeier. 2018. Blockchain economics. *National Bureau of Economic Research*. https://scholar.princeton.edu/sites/default/files/markus/files/blockchain_paper_v7a.pdf

Albizri, A., and D. Appelbaum. 2021. Trust but Verify: The Oracle Paradox of Blockchain Smart Contracts. *Journal of Information Systems* (forthcoming).

Anderson, S. W., and W. N. Lanen. 2002. Using Electronic Data Interchange (EDI) to Improve the Efficiency of Accounting Transactions. *The Accounting Review* 77 (4): 703-729.

Anderson, S. W., H. F. Chang, M. M. Cheng, and Y. S. Phua. 2017a. Getting to Know You: Trust Formation in New Interfirm Relationships and the Consequences for Investments in Management Control and the Collaboration. *Contemporary Accounting Research* 34 (2): 940-965.

Anderson, S. W., M. H. Christ, H. C. Dekker, and K. Sedatole. 2014. The Use of Management Controls to Mitigate Risk in Strategic Alliances: Field and Survey Evidence. *Journal of Management Accounting Research* 26 (1): 1-32.

Anderson, S. W., and H. C. Dekker. 2005. Management Control for Market Transactions: The Relation Between Transaction Characteristics, Incomplete Contract Design, and Subsequent Performance. *Management Science* 51 (12): 1733-1902.

Anderson, S. W., and H. C. Dekker. 2009. Strategic Cost Management in Supply Chains, Part 1: Structural Cost Management. *Accounting Horizons* 23 (2): 201-220.

Anderson, S. W., and H. C. Dekker. 2014. The Role of Management Controls in Transforming Firm Boundaries and Sustaining Hybrid Organizational Forms. *Foundations and Trends® in Accounting* 8 (2): 75-141.

Anderson, S. W., H. C. Dekker., and A. Van Den Abbeele. 2017b. Costly Control: An Examination of the Trade-off Between Control Investments and Residual Risk in Interfirm Transactions. *Management Science* 63 (7): 2163-2180.

Arrow, K. 1985. The Economics of Agency. In *Principals and Agents: The Structure of Business,* edited by J. Pratt, and R. Zeckhauser. Cambridge, Mass: Harvard University Press.

Axelrod, R. 1979. The Rational Timing of Surprise. *World Politics* 31 (2): 228-246.

Axelrod, R., and R.O. Keohane. 1985. Achieving Cooperation Under Anarchy: Strategies and Institutions. *World politics* 38 (1): 226-254.

Babich V., and G. Hilary. 2020. Distributed Ledgers and Operations: What Operations Management Researchers Should Know About Blockchain Technology. *Manufacturing & Service Operations Management* 22 (2): 223–240.

Baiman, S., and J. S. Demski. 1980. Economically Optimal Performance Evaluation and Control Systems. *Journal of Accounting Research* 18: 184-220.

Baiman, S., and M. V. Rajan. 2002. The Role of Information and Opportunism in the Choice of Buyer-Supplier Relationships. *Journal of Accounting Research* 40 (2): 247-278.

Baker, G., R. Gibbons, and K. J. Murphy. 2002. Relational Contracts and the Theory of the Firm. *The Quarterly Journal of Economics* 117 (1): 39-84.

Banker, R. D., J. Kalvenes, and R. A. Patterson. 2006. Information Technology, Contract Completeness and Buyer-Supplier Relationships. *Information Systems Research* 17 (2): 180–193.

Bear, K., and M. Rauchs. 2020. Financial Services Leads The Development Of Enterprise Blockchain. *A Research Vignette for Global Digital Finance*. https://www.gdf.io/wp-content/uploads/2020/11/GDF-FS-Leads-The-Development-of-Enterprise-Blockchain-Vignette-October-2020.pdf

Bechini, A., M. G. Cimino, F. Marcelloni, and A. Tomasi. 2008. Patterns and technologies for enabling supply chain traceability through collaborative e-business. *Information and Software Technology* 50 (4): 342-359.

Beck, R., C. Müller-Bloch, and J. L. King. 2018. Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems* 19 (10):1020-1034.

Caglio, A., and A. Ditillo. 2008. A review and discussion of management control in inter-firm relationships: Achievements and future directions. *Accounting Organizations and Society* 33 (7-8): 865– 898.

Caglio, A., and A. Ditillo. 2020. Reviewing Interorganizational Management Accounting and Control Literature: A New Look. *Journal of Management Accounting Research* (forthcoming).

Castañer, X., and N. Oliveira. 2020. Collaboration, Coordination and Cooperation between Organizations: Establishing the Distinctive Meanings of These Terms through a Systematic Literature Review. *Journal of Management* 46 (6): 965-1001.

Cao, S., L. W. Cong, and B. Yang. 2019. Financial Reporting and Blockchains: Audit Pricing, Misstatements, and Regulation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248002

Catalini, C., and J. Boslego. 2019. Blockchain Technology and Organization Science: Decentralization Theatre or Novel Organizational Form? *Working Paper, Massachusetts*

Institute of Technology, Cambridge.

Calderón, J., and T. C. Stratopoulos. 2020. What Accountants Need to Know about Blockchain. *Accounting Perspectives* 19 (4): 303-323.

Catalini, C., and J. S. Gans. 2020. Some Simple Economics of the Blockchain. *Communications of the ACM* 63 (7): 80-90

Christ, M. H., and A. I. Nicolaou. 2016. Integrated information systems, alliance formation, and the risk of information exchange between partners. *Journal of Management Accounting Research* 28 (3): 1-18.

Clemons, E. K., S. P. Reddi, and M. C. Row. 1993. The Impact of Information Technology on the Organization of Economic Activity: The "Move to the Middle" Hypothesis. *Journal of Management Information Systems* 10 (2): 9-35.

Clemons, E. K., and L. M. Hitt. 2004. Poaching and the Misappropriation of Information: Transaction Risks of Information Exchange. *Journal of Management Information Systems* 21 (8): 87-107.

Coletti, A. L., K. L. Sedatole, and K. L. Towry. 2005. The effect of control systems on trust and cooperation in collaborative environments. *The Accounting Review* 80 (2): 477-500.

Coyne, J. G., and P. McMickle. 2017. Can Blockchains Serve an Accounting Purpose? *Journal of Emerging Technologies in Accounting* 14 (2): 101-111.

Coase, R. H. 1937. The Nature of the Firm. *Economica* 4 (16): 386-405.

Dai, J., and M. A. Vasarhelyi. 2017. Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems* 31 (3): 5-21.

David, P. A., and S. Greenstein. 1990. The Economics Of Compatibility Standards: An Introduction To Recent Research. *Economics of Innovation and New Technology* 1 (1-2): 3-41

Davis, G. F., R. L. Kahn, and M. N. Zald. 1990. Contracts, treaties, and joint ventures. In *Organizations and Nation States: New Perspectives on Conflict and Cooperation,* edited by R.L. Kahn and M.N. Zald, 19-54. San Francisco: Jossey-Bass.

Dekker, H. C. 2004. Control of inter-organizational relationships: Evidence on appropriation concerns and coordination requirements. *Accounting, Organizations and Society* 29 (1): 27–49.

Dekker, H. C. 2008. Partner selection and governance design in interfirm relationships. *Accounting, Organizations and Society* 33 (7-8): 915-941.

Dekker, H. C., J. Sakaguchi, and T. Kawai. 2013. Beyond the contract: Managing risk in supply chain relations. *Management Accounting Research* 24 (2): 122-139.

Dekker, H. C., and A. Van den Abbeele. 2010. Organizational Learning and Interfirm Control: The Effects of Partner Search and Prior Exchange Experiences. *Organization Science* 21 (6):1233-1250.

Ding, R., H. C. Dekker, and T. Groot. 2013. Risk, partner selection and contractual control in interfirm relationships. *Management Accounting Research* 24 (2): 140-155.

Doney, P. M., and J. P. Cannon. 1997. An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing* 61 (2): 35-51.

Dulleck U., R. Kerschbamer, and M. Sutter. 2011. The economics of credence goods: An experiment on the role of liability, verifiability, reputation, and competition. *American Economic Review* 101 (2): 526-555.

Gans, J. S., 2019. The Fine Print in Smart Contracts. *NBER Working Paper No. 25443*. https://www.nber.org/papers/w25443

Gibbons, R., and R. Henderson. 2012. Relational Contracts and Organizational Capabilities. *Organization Science* 23 (5): 1350-1364.

Glaser, F. 2017. Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis. *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS-50)*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3052165

Grafton, J., and J. Mundy. 2017. Relational contracting and the myth of trust: Control in a co-opetitive setting. *Management Accounting Research* 36: 24-42.

Gulati, R. 1995. Does familiarity breed trust? The implications of repeated ties for contractual choice in alliances. *Academy of Management Journal* 38 (1): 85-112.

Gulati, R., and H. Singh. 1998. The Architecture of Cooperation: Managing Coordination Costs and Appropriation Concerns in Strategic Alliances. *Administrative Science Quarterly* 43 (4): 781-814.

Gulati, R., F. Wohlgezogen, and P. Zhelyazkov. 2012. The Two Facets of Collaboration: Cooperation and Coordination in Strategic Alliance. *The Academy of Management Annals* 6 (1): 531-583.

Halaburda, H. 2018. Blockchain revolution without the blockchain. *Communications of the ACM* 61 (7): 27-29.

Hart, P., and C. Saunders. 1997. Power and Trust: Critical Factors in the Adoption and Use of Electronic Data Interchange. *Organization Science* 8 (1): 23-42.

Hopwood, A. G. 1996. Looking across rather than up and down: On the need to explore the lateral processing of information. *Accounting, Organizations and Society* 21 (6): 589-590.

Håkansson, H., and J. Lind. 2004. Accounting and network coordination. *Accounting, Organizations and Society* 29 (1): 51-72.

ICAEW. 2018. Blockchain and the future of accountancy. *ICAEW Thought Leadership - IT Faculty* (Institute of Chartered Accountants in England and Wales).

Ireland, R. D., M. A. Hitt, and D. Vaidyanath. 2002. Alliance Management as a Source of Competitive Advantage. *Journal of Management* 28 (3): 413–446.

Jensen, T., J. Hedman, and S. Henningsson. 2019. How TradeLens Delivers Business Value With Blockchain Technology. *MIS Quarterly Executive* 18 (4): 221-243.

Kajüter, P., and H. I. Kulmala. 2005. Open-book accounting in networks: Potential achievements and reasons for failures. *Management Accounting Research* 16 (2): 179-204.

Klein, B., and K. B. Leffler. 1981. The Role of Market Forces in Assuring Contractual Performance. *Journal of Political Economy* 89 (4): 615-641.

Kogut, B., and U. Zander. 1992. Knowledge of the firm, combinative capabilities, and the replication of technology. *Organization Science* 3 (3): 383-397.

Kokina, J., R. Mancha, and D. Pachamanova. 2017. Blockchain: Emergent Industry Adoption and Implications for Accounting. *Journal of Emerging Technologies in Accounting* 14 (2): 91-100.

Kumar, A., R. Liu, and Z. Shan. 2020. Is Blockchain a Silver Bullet for Supply Chain Management? Technical Challenges and Research Opportunities. *Decision Sciences* 51 (1): 8-37.

Lacity, M. 2018. Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality. *MIS Quarterly* Executive 17 (3): 201-222.

Lacity, M., and R. Van Hoek. 2021a. What We've Learned So Far About Blockchain for Businesses. *MIT Sloan Management Review*.

Lacity, M., and R. Van Hoek. 2021b. Requiem for Reconciliations: DL Freight, a blockchain-enabled solution by Walmart Canada and DLT Labs. *University of Arkansas Blockchain Center for Excellence Research White Paper*. https://dltlabsweb-media.s3.ca-central-1.amazonaws.com/docs/BCoE202101POSTFINAL-55dcfe44-e73c-4d83-be69-5cb888b7b539.pdf

Lacity, M., Z. Steelman, and P. Cronan. 2019. Blockchain Governance Models: Insights for Enterprises. *University of Arkansas Blockchain Center for Excellence Research White Paper*. https://cpb-us-e1.wpmucdn.com/wordpressua.uark.edu/dist/5/444/files/2019/11/BCCoEWhitePaper022019OPEN.pdf

Litwak, E., and L. F. Hylton. 1962. Interorganizational Analysis: A Hypothesis on Co-ordinating Agencies. *Administrative Science Quarterly* 6 (4): 395-420.

Lumineau, F., W. Wang, and O. Schilke. 2020. Blockchain Governance—A New Way of Organizing Collaborations? *Organization Science* 32 (2): 500-521.

Lumineau, F., W. Wang, O. Schilke, and L. Huang. 2021. How Blockchain Can Simplify Partnerships. *Harvard Business Review*.

Luo, Y. 2002. Contract, cooperation, and performance in international joint ventures. *Strategic Management Journal* 23 (10): 903-919.

MacLeod, W. B. 2007. Reputations, Relationships, and Contract Enforcement. *Journal of Economic Literature* 45 (3): 595-628.

Markus, M. L., C. W. Steinfield, R. T. Wigand, and G. Minton. 2006. Industry-Wide Information Systems Standardization as Collective Action: The Case of the U.S. Residential Mortgage Industry. *MIS Quarterly* 30: 439-465.

Mattke, J., C. Maier, A. Hund, and T. Weitzel. 2019. How an Enterprise Blockchain Application in the U.S. Pharmaceuticals Supply Chain is Saving Lives. *MIS Quarterly Executive* 18 (4): 245-261.

McEvily, B., V. Perrone, and A. Zaheer. 2003. Trust as an organizing principle. *Organization Science* 14 (1): 91-103.

Murray, A., S. Kuban, M. Josefy, and J. Anderson. 2019. Contracting in the Smart Era: The Implications of Blockchain and Decentralized Autonomous Organizations for Contracting and Corporate Governance. *Academy of Management Perspectives* (in press).

Neumann, K. 2010. Ex-ante governance decisions in inter-organizational relationships: A case study in the airline industry. *Management Accounting Research* 21 (4): 220-237.

Nicolaou, A. I., K. L Sedatole, and N.K. Lankton. 2011. Integrated Information Systems and Alliance Partner Trust. *Contemporary Accounting Research* 28 (3): 1018-1045.

Olson, M. 1965. The Logic of Collective Action: Public goods and the Theory of Groups. Harvard University Press.

Parkhe, A. 1993. Strategic alliance structuring: A game theoretic and transaction cost examination of interfirm cooperation. *Academy of Management Journal* 36 (4): 794-829.

Peters, G. W., and E. Panayi. 2016. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money* 239-278.

Pfeffer, J., and G. R. Salancik. 1978. The external control of organizations: A resource dependency perspective. New York: Harper & Row.

Poppo, L., and T. Zenger. 2002. Do formal contracts and relational governance function as substitutes or complements? *Strategic Management Journal* 23 (8): 707-725.

Poppo, L., K. Z. Zhou, and J. J. Li. 2016. When can you trust "trust"? Calculative trust, relational trust, and supplier performance. *Strategic Management Journal* 37 (4): 724-741.

Rauchs, M., A. Blandin, K. Klein, G. Peters, M. Recanatini, and B. Zhang. 2018 (a). 2nd Global Cryptoasset Benchmarking Study. *Cambridge Centre for Alternative Finance, Cambridge Judge Business School.* https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-%20global-cryptoasset-benchmark-study/#.YKkLT6gzaiN

Rauchs, M., A. Glidden, B. Gordon, G. Pieters, M. Recanatini, F. Rostand, K. Vagneur, and B. Zhang. 2018 (b). Distributed Ledger Technology Systems: A Conceptual Framework. *Cambridge Centre for Alternative Finance, Cambridge Judge Business School.* https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/distributed-ledger-technology-systems/#.YKkLi6gzaiO

Rauchs, M., A. Blandin, K. Bear, and S. McKeon. 2019. 2nd Global Enterprise Blockchain Benchmarking Study. *Cambridge Centre for Alternative Finance, Cambridge Judge Business School.* https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-enterprise-blockchain-benchmarking-study/

Reuer, J. J., and A. Ariño. 2007. Strategic alliance contracts: dimensions and determinants of contractual complexity. *Strategic Management Journal* 28 (3): 313-330.

Reusen, E., and K. Stouthuysen. 2020. Trust transfer and partner selection in interfirm relationships. *Accounting, Organizations and Society* 81: 101081.

Risius, M., and K. Spohrer. 2017. A blockchain research framework. *Business & Information Systems Engineering* 59 (6): 385-409.

Rousseau, D. M., S. B. Sitkin, R. D. Burt, and C. Camerer. 1998. Not so different after all: A cross-discipline view of trust. *Academy of Management Review* 23 (3): 393-404.

Salvato, C., J. J. Reuer, and P. Battigalli. 2017. Cooperation across Disciplines: A Multilevel Perspective on Cooperative Behavior in Governing Interfirm Relations. *Academy of Management Annals* 11 (2): 1-45.

Schepker, D. J., W. J. Oh, A. Martynov, and L. Poppo. 2014. The Many Futures of Contracts: Moving Beyond Structure and Safeguarding to Coordination and Adaptation. *Journal of*

Management 40 (1): 193-225.

Schelling, T. C. 1960. The Strategy of Conflict. Harvard University Press.

Schloetzer, J. D. 2012. Process Integration and Information Sharing in Supply Chains. *The Accounting Review* 87 (3): 1005-1032.

Sheldon, M. D. 2019. A Primer for Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit. *Current Issues in Auditing* 13 (1): A15-A29.

Smith, K. G., S. J. Carroll, and S. J. Ashford. 1995. Intra-and interorganizational cooperation: Toward a research agenda. *Academy of Management Journal* 38 (1): 7-23.

Sobrero, M., and S. Schrader. 1998. Structuring inter-firm relationships: A metaanalytic approach. *Organization Studies* 19 (4): 585-615.

Steinfield, C., M. L. Markus, and R. T. Wigand. 2011. Through a glass clearly: Standards, architecture, and process transparency in global supply chains. *Journal of Management Information Systems* 28 (2): 75-108.

Stratopoulos, T. C., and J. Calderón. 2020. Introduction to Blockchain for Accounting Students. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3395619

Stratopoulos, T. C., V. X. Wang, and H. J. Ye. 2021. Use of Corporate Disclosures to Identify the Stage of Blockchain Adoption. *Accounting Horizons* (forthcoming)

Stuart, T. E. 1998. Network positions and propensities to collaborate: An investigation of strategic alliance formation in a high-technology industry. *Administrative Science Quarterly* 43 (3): 668-698.

Susarla, A., M. Holzhacker, and R. Krishnan. 2020. Calculative Trust and Interfirm Contracts. *Management Science* 66 (11): 5465-5484.

Swanson, T. 2015. Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems. https://allquantor.at/blockchainbib/pdf/swanson2015consensus.pdf

Tasca, P., and C. J. Tessone. 2017. Taxonomy of Blockchain Technologies. Principles of Identification and Classification. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977811

Trapido, D. 2007. Competitive embeddedness and the emergence of interfirm cooperation. *Social Forces* 86 (1): 165-191.

Uzzi, B. 1997. Social structure and competition in interfirm networks: The paradox of embeddedness. *Administrative Science Quarterly* 42 (1): 35-67.

Weiss, M., and C. Cargill. 1992. Consortia in the standards development process. *Journal of the American Society for Information Science* 43 (8): 559-565.

White, S. 2005. Cooperation costs, governance choice and alliance evolution. *Journal of Management Studies* 42 (7): 1383-1412.

Williamson, O. E. 1983. Credible Commitments: Using Hostages to Support Exchange. *The American Economic Review* 73 (4): 519-540

Williamson, O. E. 1985. The economic institutions of capitalism. *The Free Press*, New York.

Williamson, O. E. 1991. Comparative economic organization: The analysis of discrete structural alternatives. *Administrative Science Quarterly* 36 (2): 269–297.

Williamson, O. E. 1993. Calculativeness, Trust, and Economic Organization. *The Journal of Law and Economics* 36 (1): 453-486.

Xu, X., I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba. 2017. A taxonomy of blockchain-based systems for architecture design. *Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA)*: 243-252.

Yermack, D. 2017. Corporate governance and blockchains. *Review of Finance* 21(1): 7-31.

Zavolokina, L., R. Ziolkowski, I. Bauer, and G. Schwabe. 2020. Management, Governance and Value Creation in a Blockchain Consortium. *MIS Quarterly Executive* 19 (1): 1-17.

Zhu, K., K. L. Kraemer, V. Gurbaxani, and S. X. Xu. 2006. Migration to Open-Standard Interorganizational Systems: Network Effects, Switching Costs, and Path Dependency. *MIS Quarterly* 30: 515-539.

Zhu, K., K. L. Kraemer, and S. X. Xu. 2003. Electronic business adoption by European firms: a cross-country assessment of the facilitators and inhibitors. *European Journal of Information Systems* 12 (4): 251–268.

APPENDIX A

BLOCKCHAIN AND SMART CONTRACT CHARACTERISTICS

Fundamental characteristics of blockchain technology include peer-to-peer transmission, shared recordkeeping, multi-party consensus[17], independent validation, tamper resistance, tamper evidence, and transparency (Rauchs, Blandin, Bear, and McKeon 2019).

Blockchain systems allow for new ways of decentralization and delegation of services that are enacted through smart contracts (Glaser 2017). Conversely, other authors (e.g. Gans 2019; Rauchs et al. 2018b; Xu et al. 2017) comment that such contracts are not strictly speaking fully autonomous and adaptive, nor do they at the moment necessarily represent legal agreements in most jurisdictions, and especially across jurisdictions. A fundamental requirement for smart contracts to be functional and cost-efficient is the ability to produce "hard evidence" of (non) performance on an obligation. When data is endogenous, the necessary evidence may be hard coded, however when contractual obligations rely on exogenous evidence, a blockchain system

[17] Swanson (2015) describes network consensus as the process in which a majority (or in some cases all) of network validators come to an agreement on the state of a ledger. It is a set of rules and procedures that allows maintaining a coherent set of facts between multiple participating nodes.

(and the corresponding smart contract) needs to create incentives and control mechanisms for disclosure of accurate information about contract performance (Gans 2019). Successful execution of transactions in IORs is based on critical information about responsibilities, procedures, and objectives of the parties involved, attributes that can be quite explicit for some, but also tacit for other transactions (Lumineau et al. 2020). Lumineau et al. (2020) build on the notion of "tacitness"[18] in transactions as a function of the transaction's level of *codifiability*[19] and *verifiability*[20]. To this we add the concept of *standardization*[21], as a multi-level construct salient in various contexts including transacting *within* an IOR (Steinfield, Markus, and Wigand 2011) or *across* different industry sectors (Markus, Steinfield, Wigand, and Minton 2006). Studies have referred to the issue with automatic execution based on data exogenous to blockchain as the oracle problem (Murray et al. 2019; Albizri and Appelbaum 2021). While this is undoubtedly a drawback of using blockchain technology in IOR settings where many data references are exogenous, the oracle problem is not impossible to address, nor are all types of transactions equally susceptible to it. In a permissioned blockchain environment consisting of vetted participants several management control mechanisms including trust (Halaburda 2018) can be used to reduce transaction hazards and thus address the oracle problem. Furthermore, it is important to note that in explicit transactions for which specific plans can be devised ex-ante (e.g. procurement of standardized materials from an alliance partner) the oracle problem represents less of an organizational challenge, and the benefits of using a blockchain could outweigh the associated risks (Lumineau et al. 2020). At the same time, the benefits of relying solely on blockchain in tacit transactions that include complex interdependent activities

[18] Tacitness refers to the difficulty of codifying key transaction attributes (Kogut and Zander 1992) or complications in encoding attributes such as responsibilities, procedures, and objectives.
[19] Codifiability represents the ability to characterize precisely product/service, delivery, and settlement requirements in an electronic format, and in a manner understandable to relevant parties (Lumineau et al. 2020).
[20] Verifiability signifies the extent to which transacting parties are able to observe and evaluate the quality of an item of exchange or adherence to specified requirements ex-post (Dulleck, Kerchbamer, and Sutter 2011).
[21] The issue of standardization in a broader blockchain context also refers to interoperability or "linking the chains" (Kumar et al. 2020).

requiring the ability of the partners to adapt to unforeseen events are less than clear primarily because of the standardization, codification and verification challenges involved in these transactions.

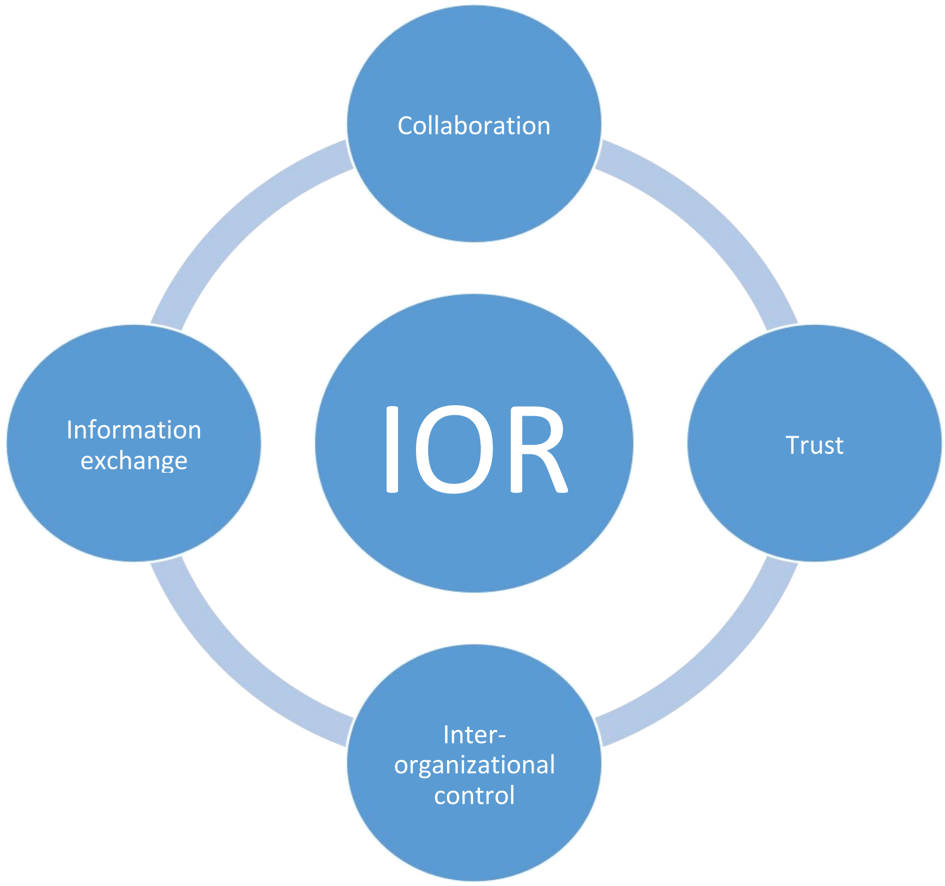

Figure 1: Organizing theoretical framework.