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

ABSTRACT

Blockchain is a technology intended for sharing data across a broad network of untrusted entities in a decentralized manner. It first gained recognition as the technology behind Bitcoin, but is seeing fast adoption in other areas including supply chain management, insurance, and banking. Our aim is to investigate the potential of blockchain technology when applied in an inter-organizational setting. To this end, the paper provides a review of management accounting literature on inter-organizational relationships (IORs), and identifies areas that may be significantly impacted by blockchain technology. The objective is not to present an exhaustive review of this field, but instead to outline and scrutinize topics and issues related to IORs where capabilities of blockchain can have the most significant impact. Based on the synthesis of the reviewed literatures, we offer several propositions, which are intended to provide a starting point for future research exploring blockchain in the context of IORs.

Keywords: Blockchain; inter-organizational relationships; management control; management accounting; information systems.
I INTRODUCTION

The motivation behind this paper stems from the rise to prominence of an innovative and arguably organizationally disruptive distributed database technology, colloquially referred to as blockchain, and its potential in an inter-organizational setting. Based on its core attributes, blockchain technology seems highly suitable for such a setting, where legally autonomous partnering firms essentially play a “mixed motive game”, in which they have overlapping (to a greater or a lesser extent), but ultimately separate profit motives (Anderson, Christ, Dekker, and Sedatole 2014). These collaborative arrangements are most often referred to in the literature as inter-organizational relationships (IORs). They can be defined as voluntarily initiated cooperative arrangements between 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). In our analysis, we outline four main areas within the IOR literature, namely collaboration, trust, inter-organizational control and information exchange, which we find to be the most relevant to investigate in relation to blockchain technology. We first review literatures within each of these areas, identify recurring issues, and consider how each could be impacted by the blockchain. Based on this discussion, we develop several propositions that constitute a research agenda intended to serve as a guide for future research within the identified areas.

The first successful use case for blockchain technology was Bitcoin, a digital currency based on a peer-to-peer network and cryptographic tools (Nakamoto, 2008). The Bitcoin blockchain allows its users to exchange non-duplicable digital tokens carrying monetary value in an environment consisted of disparate pseudonymous\(^1\) actors, which is assumed to be inherently

\(^1\) Every Bitcoin user is tied to a specific alphanumerica address, and can choose to remain anonymous or reveal their identity to others (Iansiti and Lakhani 2017).
adversarial. In an inter-organizational setting, blockchain technology allows partners to transfer digital assets or business-relevant information (e.g. about orders, receipts, payments, etc.) across firm boundaries through a shared, tamper-resistant distributed ledger (Kumar, Liu, and Shan 2019). In other words, blockchain technology enables decentralized management of digital assets, algorithmic enforcement of shared agreements in the form of software programs, and verifies the ordering of data records in an adversarial environment (to a higher or a lesser degree, depending on the use case) (Meunier and Zhao-Meunier 2019). This is achieved without reliance on centralized trusted authorities like governments, banks or payment services to serve as guarantors of the correctness of records or facilitators of transactions between parties. 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 technology on the other hand offers a radically different (i.e. distributed) alternative for recording information 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. Furthermore, due to its ability to implement atomic transactions\(^2\), build a tamper-resistant audit trail\(^3\), and simplify settlement and reconciliation across organizations, blockchain technology has seen fast adoption and experimentation particularly within the areas of finance and accounting (Catalini and Gans 2016).

\(^2\)Catalini and Gans (2019) define atomic transactions as those that can be fully executed and enforced through a distributed ledger, and whose key attributes can be verified through the same ledger without interference of a third party intermediary.

\(^3\)An audit trail has been defined as the documented flow of a transaction used to investigate how a source document was translated into an account entry, and from there was inserted into the financial statements as an entity. It can be used in reverse, to track backwards from a financial statement item to the originating source document. An audit trail is used by both external and internal auditors to trace transactions through an accounting system, as well as the staff to track down errors and the causes of variances in the financial statements (Accounting Tools 2018), quoted in Power (2019).
The success of Bitcoin has prompted further investigation into the usefulness of blockchain technology in other business settings (Coyne and McMickle 2017; Wörner, Von Bomhard, Schreier, and Bilgeri 2016). Depending on the peculiarities of a given use case, practitioners who leverage the technology to develop new business models have relied either on all of its aspects (i.e. including a native digital token), or have mobilized its distributed database, governance and algorithmic enforcement components (e.g. supply chain platforms such as TradeLens, developed by IBM and Mærsk). Implications of these efforts are increasingly being discussed by policy makers, legislators, and researchers from various fields ranging from computer science to accounting and economics.

In a recent global benchmarking study of the cryptoasset ecosystem, Rauch et al. (2018) find that the aggregate market capitalization of cryptoassets has skyrocketed from $30 billion in the first quarter of 2017, to a peak of more than $800 billion in January 2018, before coming down to levels of around $300 billion in summer 2019. Rauch and colleagues further find that the number and geographical dispersion of participants in these networks has increased significantly in recent years, to (at the time of writing) 139 million user accounts with at least 35 million identity-verified users coming from all of the major regions in the world. Furthermore, many established firms such as banks (e.g. JPMorgan Chase), accounting firms and consultancies (e.g. Deloitte, EY), retailers (e.g. Walmart), logistics and supply chain companies (e.g. Mærsk), and many other are involved in trials of blockchain technology, or have major commercial projects already in production. Each of these projects brings together tens, or even hundreds of firms, which work collaboratively on the development and deployment of different blockchain-based solutions for their inter-organizational environments. While blockchain technology is unquestionably still in the experimental phase of development, and surrounded by technological, economic, and operational uncertainties, the developments listed above, as well as an several recent studies (e.g. Allen, Berg, Markey-
Towler, Novak and Potts 2020; Werbach 2018) suggest that it is emerging as an economically significant technology with salient real-world business implications.

The examples listed above speak to the fact that blockchain is by design a multi user technology. It is intended for continuous, non-centrally governed interaction among heterogeneous groups of participants. Moreover, it supports the independent development and deployment of autonomous, collaborative and highly interoperable services by every entity that uses the system (Glaser 2017). Certain functionalities of blockchain technology (i.e. smart contracts, discussed in more detail below) could have important ramifications for organizational theory and practice, since they could significantly influence the level of frictions and costs in transactions between firms. These functionalities fundamentally represent a routinisation of certain processes, which reduces those processes to a set of articulated conditions, monitoring of those conditions, and execution based on those conditions (Murray, Kuban, Josefy, and Anderson 2019). This suggests that the use of blockchain technology could have a notable effect on transaction costs and, in turn, firm boundaries and the nature of inter-firm governance. These issues are most commonly discussed in the management accounting literature, in particular in the area pertaining to accounting and control in IORs.

Contemporary accounting studies, however, mostly explore the use of blockchain technology within the context of financial accounting. Perhaps because of the intuitive link between the concept of the blockchain ledger and accounting ledgers, some considered the possibility of blockchain technology becoming a more secure, immutable alternative to current ledger database solutions (Coyne and McMickle 2017). Most frequently discussed benefits 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, which could be programmed onto the blockchain (Krahel 2012). Dai and Vasarhelyi (2017) further argue that blockchain could
facilitate “triple-entry 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 booking system could have a corresponding blockchain account. The area of management accounting on the other hand, at present remains largely underexplored regarding blockchain, its possible uses, and their implications. Therein lies a research gap that we attempt to address in this paper.

Studies of IORs (e.g. Grafton and Mundy 2017; Anderson et al. 2014; Chen, Park and Newburry 2009; Kajüter and Kulmala 2005; Häkansson and Lind 2004; Litwak and Hylton 1962) 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 forms of IORs (e.g. supply-chain relationships, strategic alliances, outsourcing agreements) represent organizational arrangements which exist in conditions of somewhat unstructured authority. Collaboration between partners is necessary to preserve these organizational forms, yet it is often the case that no single entity involved in the relationship possesses sufficient formal authority to be able to impose collaboration through fiat (Litwak and Hylton 1962). Existing research in accounting and economics (e.g. Baiman and Rajan 2002; Oxley 1997; Williamson 1993; Dekker 2004; Clemons and Hitt 2004) discusses opportunism as a notable management control problem with implications for practice and theory related to IORs. The concept of “opportunism” itself has been defined as self-interest seeking with guile, and it more generally refers to the deliberate incomplete or distorted disclosure of information between partners (Williamson 1985). Examples of opportunism discussed in the literature further include ex ante behavior such as deliberate misrepresentation of a firm’s true attributes prior to the signing of a contract, termed “pre-contract hidden information” (Arrow 1985), misappropriation of information by the recipient that cannot be legally prevented and benefits from which cannot be contracted on
The examples also include ex post shirking on quality, effort or information provision known as “hidden action” and “ex post hidden information” respectively (Holmström 1982). These can create tension between partners, which necessitates that different formal and/or informal safeguards and control mechanisms be put in place to manage the IOR. However, at this point it is important to note that inherent complexity and the state of partial conflict present in IORs need not necessarily cause an organizational breakdown. The nature of IORs and mechanisms that have been developed to establish and manage them allow, and sometimes even encourage a certain level of conflict in the relationships (Litwak and Hylton 1962). The growing strand of literature in accounting and several other disciplines concerning IORs proves helpful in articulating and addressing our research aims. A guiding framework including the major themes in these literatures has been developed to facilitate the analysis.

[Insert Figure 1 about here]

II GUIDING FRAMEWORK

Given that the body of literature on IORs has become quite large and diverse, we find it useful to narrow our focus to particular areas, which might be impacted by blockchain technology. The analysis uncovers four main areas that are seen as the most relevant to explore in this regard. These areas are presented in figure 1. It is important to note however, that these topics do not exist in isolation, but are highly interrelated, and considerable overlap between the relevant theoretical concepts was found in the reviewed literature.

Collaboration is the first area identified within the literature on inter-organizational relationships. Since blockchain technology is, by design, a multi-party system (Glaser 2017),
some level of collaboration will be necessary both during the implementation of the technology, as well as during its operational phase. When setting up a common IT infrastructure, based on blockchain, the implementing partners will likely need to identify the potential future benefits and clarify expectations for the relationship ex ante. Following from this, two sub-areas, or “facets of collaboration” (Gulati, Wohlgezogen, and Zhelyazkov 2012), emerged within this broader area, namely cooperation and coordination. Blockchain is often described as a “trust-less” technology (e.g. Xu et al. 2017), able to replace trust in an intermediary with trust in inherent consensus rules and underlying code (Catalini and Gans 2018). Although this may not be the case with permissioned blockchains, where a “gatekeeper” grants participants access to the systems (Rauchs et al. 2018), the concept of trust (e.g. Luhman 1979; Giddens 1990; Rousseau, Sitkin, Burt, and Camerer 1998) is critical to explore, and was identified as the second area. As blockchain’s “immutable” audit trail could serve as a powerful control mechanism, inter-organizational control was identified as the third high-level area, which may be impacted by the technology. Implementations of blockchain technology will inevitably involve creating a network of partners, so the literatures on contracting (e.g. Anderson and Dekker 2005, Poppo and Zenger 2002; Reuer and Ariño 2007; Ding, Dekker, and Groot 2013; Costello 2013) and partner selection (e.g. Dekker 2008; Neumann 2010; Dekker and Van den Abbeele 2010) prove to be particularly informative sub-areas to explore, and are especially relevant in the early stages of a project. The primary reason for companies to implement blockchain technology may be the desire for a trustworthy and reliable exchange of information, so information exchange is the fourth area discussed in this review.

The paper is structured as follows. First, we conceptualize blockchain technology, identify its different characteristics, and the design choices available to entities that seek to implement it. Second, we return to the guiding framework, and review literatures within the four proposed areas. We then identify the most prevalent issues within each of these fields, which are the
most likely to be affected by the use of blockchain technology. Finally, based on the identified issues, and blockchain capabilities, we develop a number of propositions and present a research agenda, which could be a useful guide for further studies in this area.

III CONCEPTUALIZING BLOCKCHAIN

Blockchain is an emerging technology used for sharing transactional data across a broad network of untrusted participants in a decentralized manner. It allows for new designs of distributed software architectures, in which the consensus on the states of the shared database can be reached without needing to rely on a trusted central integration point (Xu et al. 2017). Since custody and exchange of assets on a blockchain can take place without traditional intermediaries, for the first time in history the technology enables reliable transfers of value and digital assets between parties without the need to rely on any outside institution or organization (Catalini and Tucker 2018; Tasca and Tessone 2018).

The name “blockchain” refers to a chain of blocks, each of which contain several transaction records (Nærland, Müller-Bloch, Beck, and Palmund 2017) for a specific period of time and their attributes (Catalini and Gans 2018). The transactional data is protected by cryptographic hash functions (Nærland et al. 2017). Hash values are unique and any modifications to a block would instantly alter the corresponding hash value, which serves to ensure that all blocks are formed according to the underlying protocol and not tampered with (Beck, Czepluch, Lollike, and Malone 2016). Every block is also linked to the preceding block, because it includes the hash of the prior block, in addition to the actual hashed transaction data (Nærland et al. 2017), therefore achieving a temporal ordering of transactions (Glaser 2017; Xu et al. 2017). Since any modification in the transaction information included in a given block would change the
hash, it would also irreparably break the chain of consensus connecting that block with all the preceding ones (Catalini and Gans 2016). Such an approach assures the integrity of the complete blockchain, all the way to the first block, also known as the “genesis block”. Every block also contains a timestamp and a nonce, which is an arbitrary number for authenticating the hash (Nofer, Gomber, Hinz, and Schiereck 2017).

The blockchain is distributed across a network of computers called “nodes”. Each node maintains an identical copy of the blockchain ledger. The nodes are incentivized to reach an agreement on the state of the blockchain (Nærland et al. 2017). If the majority of nodes in the blockchain network reaches a consensus about the validity of transactions in a block, as well as the validity of the block itself, the block is included in the chain (Nofer et al. 2017). Consequently, every node on the network shares an identical copy of the blockchain record. If one node attempts to dishonestly and one-sidedly modify its version of the blockchain, that version would be discarded by the other nodes (Nærland et al. 2017). In combination with computational restrictions and incentive schemes related to formation of blocks, this concept can restrict tampering and alteration of information recorded on the blockchain (Xu et al. 2017).

Blockchain functionalities are akin to a distributed ledger that is collectively kept, updated, and validated by the parties within a network (Risius and Spohrer 2017). Rauchs et al. (2018) define Distributed Ledger Technology (DLT) as “a system of electronic records that enables a network of independent participants to establish a consensus around the authoritative ordering of cryptographically-validated (“signed”) transactions. These records are made persistent by replicating the data across multiple nodes, and tamper-evident by linking them through cryptographic hashes. The shared result of the reconciliation/consensus process—the ‘ledger’—serves as the authoritative version for these records” (p. 98). The authors also argue that ambiguous terminology and fuzzy boundaries resulted in “DLT” becoming an umbrella
term, used to label several loosely related concepts which, among others, include blockchains. Brief histories of blockchain and DLT can be found in appendix A.

Blockchain characteristics

Different authors often emphasize different characteristics of blockchain technology, but the most commonly identified are peer-to-peer (P2P) transmission, distributed database, immutability, consensus mechanisms, transparency with pseudonymity, and computational logic (e.g. Iansiti and Lakhani 2017). The communication on the blockchain network occurs directly between participants. Users generate transactions by placing raw data into a standardized format, including a cryptographic signature for the purposes of authentication, and broadcast it to other nodes in the blockchain network (Glaser 2017). The signature, which is created by a private key, serves as the users’ authorization for the system to request an entry for the corresponding transaction. A valid signature presents the cryptographic guarantee that the initiator of the transaction is authorized to execute a given ledger entry (Rauchs et al. 2018). Some authors argue that blockchain’s ability to bypass the trusted third parties can diminish the risk of security breaches (Nofer et al. 2017), curtail corruption or failure of storage systems (Beck, Avital, Rossi, and Thatcher 2017), and decrease costs related to intermediation (Nofer et al. 2017).

A blockchain network allows multiple parties to jointly generate, maintain, and update a shared set of authoritative records (Rauchs et al. 2018). Certain iterations of blockchain technology, such as Bitcoin’s, use the process of “mining” to append new blocks to the blockchain. In such a blockchain network, miners bundle valid transactions into blocks and then add them to the blockchain. New blocks are broadcasted along the entire network, in order to enable every node to keep a copy of the complete data structure (Xu et al. 2017). In other incarnations of
blockchains, only full members in a protocol, also called “full nodes”, hold a copy of the entirety of the shared database and broadcast new transactions to other nodes in the network (Catalini and Tucker 2018). Unlike centralized systems, the network functionalities remain intact even if certain nodes fail. This concept can enhance trust, since network participants do not need to determine the trustworthiness of a given intermediary or other participants in the network. It is sufficient to develop trust in the system as a whole (Nofer et al. 2017).

Since transactions recorded on a blockchain are cryptographically linked to prior entries (Catalini and Tucker 2018), any attempt to alter previous transactions requires reprocessing of all the subsequent blocks in the chain. Such reprocessing would also need to outpace the rate at which new blocks are being appended to the chain (Coyne and McMickle 2017). Moreover, due to its distributed architecture, any changes to transactions in a single node would produce invalid states if one would recalculate the current state from prior transactions (Glaser 2017). These features have prompted some authors (e.g. Beck et al. 2016; O’Leary 2017) to describe the blockchain as “immutable” or immune to manipulation, and therefore reliably secure (White 2016). The notion of immutability however, might not necessarily be entirely correct.

Different incarnations of blockchain technology provide different levels of transaction finality, contingent on the design of the system. Although a transaction is confirmed and executed, it could potentially still be subject to reversal (Rauchs et al. 2018). Moreover, if the attacker were to gain control of 51% of the computing power in the network (also known as the 51% attack), alterations to the blockchain could arise (Coyne and McMickle 2017). Therefore, it might be more accurate to describe the blockchain technology as “tamper-resistant” and “tamper-evident”, as its architecture allows for participants in the network to detect non-consensual, trivially-applied changes to the records (Rauchs et al. 2018), reliably observe and analyze them, and therefore be more confident in uncovering instances of fraudulent behavior (Szabo 2017).
The records on a blockchain are subject to network consensus, meaning that they must adhere to the rules of the protocol. At a fundamental level, they cannot contain any conflicting or invalid transactions, which also must be correctly formatted (Rauchs et al. 2018). Swanson (2015), describes the consensus mechanism 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 coherent set of facts between multiple participating nodes” (p. 4). In the case of permissionless blockchains⁴, consensus can be achieved without reliance on a single party, and in the absence of prior trusted relationships. Within permissioned blockchains, consensus is reached through several producers of records who have been authorized and/or obligated by a contract or some other kind of an agreement to assume this role (Rauchs et al. 2018). The most commonly used and discussed consensus protocols are Proof of Work (PoW) used, for example, in Bitcoin and Litecoin, and Proof of Stake (PoS) used in Ethereum, which are all public, permissionless blockchains. We discuss consensus mechanisms in more detail in the next section.

Transactions in an open permissionless blockchain network, and their values, are visible to anyone who has access to the system. This allows each participant to independently verify the validity of transactions and the integrity of the ledger (Rauchs et al. 2018). In some variations of blockchain technology, the users are pseudonymous, meaning that their identity is concealed behind a public key, but other transaction attributes are shared publically (Gordon and Catalini 2018). Every node on such a blockchain has a unique alphanumeric address that identifies it, and participants can decide to stay anonymous or reveal their identity to others (Iansiti and Lakhani 2017). It should however be noted that even though public permissionless blockchains, such as Bitcoin’s, are assumed to provide anonymity to its users, research has shown that it is

---

⁴ A type of blockchain that does not require any permission to join. The concept is discussed in more detail in the remainder of the text
technically possible to establish a connection between Bitcoin transactions and the identity of a participant (e.g. at the behest of law enforcement agencies), thereby to an extent compromising the absolute anonymity of its users (Xu et al. 2017).

Some types of blockchain systems allow for new ways of decentralization and delegation of services, which are enacted through autonomous interacting pieces of code, also referred to as smart contracts (Glaser 2017). A smart contract is a set of rules, which encompass the terms that relevant parties have agreed to. Even though smart contracts are not an essential requirement of blockchain technology, they can be embedded into the blockchain and are triggered when pre-defined conditions are fulfilled (Kokina, Mancha, and Pachamanova 2017).

The concept of smart contracts is not new. It was introduced already in 1994 by Nick Szabo\(^5\), but is gaining in popularity with the advent of blockchain technology, since smart contracts can be implemented more easily as compared to the technology which was available at the time of their invention (Nofer et al. 2017). Risius and Spohrer (2017) claim that smart contracts can allow parties who do not completely trust each other to handle and control mutual transactions without needing to depend on any trusted intermediary. Conversely, several authors (e.g. Rauchs et al. 2018; Xu et al. 2017) comment that such contracts are not actually fully autonomous or adaptive, nor are they contracts in a strict legal sense of the word. The attributes of smart contracts described above are applicable only when the data they are connected to (i.e. input and output) are endogenous to the blockchain system (i.e. exist only within its boundaries).

**Blockchain design choices**

---

\(^5\) For additional information see: [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo_best.vwh.net/smart.contracts.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo_best.vwh.net/smart.contracts.html)
When conceptualizing blockchain technology, several authors start by describing a decentralized, public permissionless blockchain, such as Bitcoin’s blockchain. Some papers additionally categorize blockchains as permissioned and permissionless (e.g. Catalini and Tucker 2018), or public and private (e.g. O’Leary 2017). However, when designing a blockchain system, the designers are presented with several different options that they need to consider (Catalini and Gans 2018; Xu et al. 2017). There are inherent trade-offs related to these choices, as specific functionalities of the technology will inevitably come at the expense of others (Rauchs et al. 2018). Designers of early blockchain systems have emphasized keeping all elements of their system “decentralized” in order to enhance the censorship resistance of the network. Full decentralization however, brought about its own set of difficulties, such as inherent scaling limitations, inefficient data redundancy, slow confirmation speed, and high energy costs for the validators (Xu et al. 2017; Rauchs et al. 2018). Subsequently developed blockchain systems have been aimed to address these issues, but different design choices inevitably come at the cost of other system properties, or result in an increase in the level of centralization in the system (Rauchs et al. 2018). We analyze design choices on the dimensions most critical when considering blockchain technology in the context of IORs, namely decentralization, consensus protocols, and exogenous and endogenous data references.

The concepts of “centralization” and “decentralization” must be seen as falling along a continuum, rather than being binary. The level of de/centralization is a continuous variable emerging from the interaction of the system components, hierarchies, and power structures (Rauchs et al. 2018). A recurring theme across different definitions of “decentralization” is whether the system allows open and free participation, instead of entrusting system management and decision making to a set of fixed entities (Coyne and McMickle 2017; Rauchs et al. 2018; Xu et al. 2017). Public, permissionless blockchains such as Bitcoin’s, aim for full decentralization, in order to attain censorship resistance: no single node can unilaterally shut
down the system, censor transactions, or manipulate the ledger (Rauchs et al. 2018). They allow anyone to participate, as long as they follow the protocol rules (Catalini and Tucker 2018). Such a setup however, may decrease the validation speed, reduce allowed size of transactions that are processed on-chain, and can deter actor participation because the costs of operating full nodes can become prohibitively costly over time (Rauchs et al. 2018). Other blockchain designs may prioritize validation speed, which could come with the expense of added size and complexity of the ledger. This could also reduce the overall security of the system, if the network is centralized (Rauchs et al. 2018). Such blockchains (often referred to as “permissioned” or “private”), allow greater control to certain participants, and could limit the ability to write or read particular data to a specific group of trusted nodes. As such, they are similar to the distributed databases companies have already been using for decades, and it is still not clear how much value they add compared to these contemporary solutions (Catalini and Tucker 2018; O’Leary 2017). Because of this, some authors (e.g. Glaser 2017) argue that the sole reason to choose this type of blockchain is its immutable transaction log for audibility purposes. Another concern related to centralized blockchains is that a central authority may manipulate the entire system, effectively making it a single point of failure (Xu et al. 2017).

Choosing an appropriate consensus protocol is another important decision in designing the blockchain system. Consensus algorithms can be categorized based on their level of difficulty (Rauchs et al. 2018), and the choice of consensus protocol has an impact on security and scalability (Xu et al. 2017). Within the Proof of Work (PoW) consensus protocol, miners solve a computationally intensive task (Kokina et al. 2017) to generate a new block. Computers must make recurrent guesses to solve a complex mathematical puzzle, as no inferable answer to the problem exists. Transaction verification must thus take time and require computational power, which is the premise of PoW (Coyne and McMickle 2017). These “mathematical puzzles” are easy to verify (once solved), but solving them difficult (Rauchs et al. 2018). Bitcoin miners,
for example, compete to solve this puzzle for each block, using large amounts of computing power (and hence electricity) to increase their chances of winning the competition to validate a new block. The investment incurred by miners to participate in this process provides economic incentives, which serve to align interests of miners and the proper operation of the system as a whole (Xu et al. 2017). Due to concerns about the high-energy requirements of PoW, several other consensus protocols have been developed. The most commonly mentioned alternative is the Proof-of-Stake (PoS) protocol, which selects the node that is to confirm new transactions based on the level of their holdings of the native digital currency of the blockchain network. For example, the miners in Peercoin need to prove the ownership of a certain amount of Peercoin currency to be allowed to confirm transactions (Xu et al. 2017). Under the PoS protocol, the miners do not receive rewards for mining a block (as they do in PoW-based blockchains), but for verifying transactions. Blocks of transactions are assigned to be verified by a participant using a probabilistic algorithm that accounts for the wealth (i.e. stake) of participants in the network (Kokina et al. 2017). While some designers might opt for PoS over PoW in order to improve speed and reduce energy consumption, this may impact the system’s incentive scheme as it pertains to the participants, and thus affect the security and tamper resistance of the system (Rauchs et al. 2018). Catalini and Gans (2018) suggest that from a game theoretic perspective, it is exactly the energy “wasteful” nature of the mining computations that defends the ledger from an attack: i.e. the sunk, irreversible commitment to the audit trail constitutes the cost a bad actor would have to sustain to manipulate it. Permissioned and closed systems generally do not require this component, as Sybil attacks (where attackers create many hostile anonymous nodes) are prevented by carefully vetting entities before granting them the permission to join the network and produce records (Rauchs et al. 2018). This incurs additional design tradeoffs, but can positively affect the reliability of
the system, if it is consisted of actors that have engaged in prior interactions and share a certain level of trust ex ante.

The final core design choice in a blockchain network pertains to the nature of data that is being exchanged between participants. Namely, records on a blockchain may reference “endogenous data” and/or “exogenous data”. Endogenous data refers to the information that comes exclusively from within the core blockchain system. Exogenous data refers to data that tracks information about the same entity or a relationship that is external to the blockchain system (Rauchs et al. 2018). Blockchain only has fully effective enforcement capabilities (i.e. the ability to automatically execute decisions) with regards to endogenous data (i.e. internal references that exclusively exist within the boundaries of the system). The states of external systems are not directly accessible by the blockchain system (Xu et al. 2017), which means that interfacing with an external source of data requires a gateway and additional protocols. This often necessitates that the notion of IORs and some level of traditional management controls be considered and possibly introduced (Szabo 2017).

IV A CLOSER LOOK INTO THE FRAMEWORK

Inter-organizational relationships

Collaborative arrangements between legally autonomous parties in the form of formal contractual relationships that do not readily fit the “market-hierarchy” dichotomy (e.g. Coase 1937; Williamson 1975) have become central to economic activity (Oliveira and Lumineau 2019). Consequently, they have sparked research interest and are recognized as distinct kind of organizing, called “hybrids” (Holmström and Roberts 1998). In this context, in line with Ménard (1995), we define an “organization” as an arrangement designed to make possible the
conscious and deliberate coordination of activities within identifiable boundaries, in which members associate on a regular basis through a set of implicit and explicit agreements, commit to collective actions for the purpose of creating and allocating resources and capabilities by a combination of command and cooperation. “Hybrid” arrangements between organizations can take a variety of forms (e.g. joint ventures, strategic alliances, networks, coalitions, industry consortia, outsourcing agreements, and supply-chain relationships), and have been referred to in the literature as “inter-organizational relationships”, “inter-firm settings”, “hybrid organizational forms”, and “networks” (Anderson and Sedatole 2003; Caglio and Ditillo 2008). Therefore, these terms are here seen as synonyms and, as such, are used interchangeably throughout the paper. In some of these IORs like joint ventures or franchises, the formal, legally enforceable, contractual framework that the partners use to formalize such arrangements represents their governance structure, while others like strategic alliances and industry consortia may operate without recourse to legal enforcement mechanisms, but still employ formal control processes to manage the alliance (Parkhe 1993; Gulati and Singh 1998; Anderson and Sedatole 2003). This suggests that these organizational forms do not represent mere deals and strategic agreements, but are also entities characterized by boards, boundary spanning individuals, information-sharing and decision-making processes, databases and integrated computer systems, as well as other material and immaterial resources, all of which entail practical organizational challenges (Gulati et al. 2012). Such relationships enable organizations to gain access to technologies, competencies, and economies of scale and scope of trading partners in more efficient ways than is in many cases possible through arm’s-length transactions (i.e. market), or vertical integration (i.e. hierarchy) (Coad and Cullen 2006).

In this setting, the use of new information systems and production technology has increased interdependence of organizational tasks; prompting otherwise independent firms to engage in simultaneous cooperation and competition, sometimes termed “co-opetition” (Ireland, Hitt, and
Vaidyanath 2002; Grafton and Mundy 2017). Moreover, frequent exchange of lateral information between many organizations to ensure effective integration and coordination has become a necessity (Hopwood 1996). Consequently, the accounting, management and information systems literatures have seen “information openness” become an important theme related to the functioning of these collaborative relationships (Caglio and Ditillo 2012). Transfers of information of varying types has been shown to work well even without vertical integration. Moreover much of this information is accounting based, albeit sometimes modified to deal with the localized nature of information transfers (Miller, Kurunmäki, and O’Leary 2008).

Conversely, the new collaborative environment that spans organizational borders presents management control challenges for the firms involved (Coletti, Sedatole and Towry 2005). In this setting, the coordination and control of the common activities cannot be completely handled internally, nor can this be achieved by market forces alone. The reason is that these activities, even when they are complementary, need to be performed by different companies, which means that the partners’ plans must be in accordance with each other (Håkansson and Lind 2004). Research has found that innovations in management control play an important role in establishing and maintaining these organizational forms, and have made them more durable (Anderson and Dekker 2014). Furthermore, greater collaboration intensity was found to be associated with greater information system integration as well as the implementation of a larger portfolio of controls between partners, making the establishment of a common information infrastructure a salient issue in this context. 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; Ozcan and Santos 2015).

In the remainder of this chapter, we return to the guiding framework outlined above, and review literatures in each of the four identified areas, namely collaboration, trust, inter-organizational
control, and information exchange. The ensuing discussion in which we identify and scrutinize major topics examined in these literatures is additionally informed by our preceding analysis of blockchain technology. The explicit goal of this discussion is to synthesize the existing knowledge about these concepts, focusing on the implications of blockchain technology for each of the four main areas of the framework. Major arguments resulting from the discussion are distilled into several propositions, which are intended to serve as building blocks of a research agenda, a prolegomena of sorts, for future efforts in blockchain-related management accounting research. It is our contention that this research agenda could help to equip accounting scholars with “instruments” to critically study IORs as an important organizational form as it increasingly becomes interrelated with an emerging technological phenomenon that is blockchain technology.

Collaboration

Collaboration between firms is an important source of competitive advantage for many companies, because it enables value creation through accessing and combining complementary resources and capabilities from partnering firms (Dyer and Singh 1998). At the same time, inter-firm collaboration can be very risky and complex (Gulati et al. 2012). It necessitates that relationship partners are capable of communicating, developing and maintaining an inter-organizational interface and internally adapting in response to relationship partner’s actions or changing external environment (White 2005). Gulati et al. (2012) identify cooperation and coordination as two distinct yet complementary facets of inter-firm collaboration. They define cooperation as “joint pursuit of agreed-on goal(s) in a manner corresponding to a shared understanding about contributions and payoffs”. The reasons why companies engage in cooperation normally involve sharing of investment risk and pursuing a number of technological, commercial and operational gains that they might be unable to obtain through transactional relationships (Oliver 1990; Gulati et al. 2012).
Smith, Carroll, and Ashford (1995) distinguish between formal and informal cooperation. While the former is characterized by contracts and formal structures, the latter involves flexible arrangements, where behavioral norms determine the inputs of the parties. According to Gulati (1995), formal cooperation can evolve to informal cooperation over time, contingent on the frequency of prior interactions. The evolution of cooperative relationships is an interesting concept to address. Ring and Van de Ven (1994) for example, suggest that cooperative relationships are constantly re-evaluated and readjusted by actions and interpretations of involved parties. They propose that cooperative relationships go through stages of emergence, evolution and dissolution. Zajac and Olsen (1993) similarly advocate for a dynamic perspective, and propose that cooperative relationships go through stages of initializing, processing and reconfiguration, with feedback loops to prior stages. In such a relationship, participants continually evaluate if the cooperation is still worthwhile. Smith et al. (1995) however, warn that there is insufficient empirical evidence of influence of such feedback mechanisms on cooperation. McAllister (1995) for example, includes affect-based trust in his model, indicating that cooperative relationships are less cognitive and calculated than perspective of constant re-evaluation and readjustment would suggest. Doz (1996) also investigated the evolution of cooperation in strategic alliances, particularly how evolution is constrained by the terms agreed at the outset of the alliance. He found that viewing such relationships as either static or evolutionary is too simplistic, and suggested that alliances are neither simple implementations of initial conditions, nor are they evolving independently from them. Instead, he argues that initial conditions are the main facilitator of alliance evolution, enabling a sequence of learning cycles.

Explicit definition of terms is important in IORs, as they provide a clear framework, defining each party’s rights and obligations, as well as the principles and procedures of the cooperation (Luo 2002). This is even more critical when introducing blockchain technology in the IOR,
because it creates a shared information infrastructure between partners and allows for programmable enforcement of rules. Moreover, implementing partners would need to invest significant resources in developing and implementing the system. This runs contrary to the notion that partners in an IOR initially start with small informal deals, involving little risk (Friedman 1991, Van de Ven 1976). These higher initial investments however, may lead to increased commitment to a joint project, and enhance cooperation. Information, recorded on the blockchain, may also enable the establishment of more reliable feedback loops, and increase transparency within the IOR, thereby contributing to firms’ confidence in their partners’ goodwill, which further promotes cooperation.

**Proposition 1: Implementing blockchain in IORs will require commitment from partners at the onset of the relationship, but will foster cooperation as the partnership develops**

As partners agree on the on the inputs and outputs of the relationship, a mutual interdependence is created (Pfeffer and Salancik 1978), a situation in which one partner is vulnerable to the actions of the other (Parkhe 1993). This issue is particularly salient in alliances formed between competitors. On the one hand, a firm’s rivals can possess necessary capabilities needed for a joint project. On the other hand, past rivalry might have cultivated the lack of trust and personal dislike (Trapido 2007). According to Davis, Kahn, and Zald (1990), however, competitors are more likely to become aware of one another through professional associations, than 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 efforts. This argument is known as “Competitive Embeddedness”, a notion that competition increases mutual awareness, which in turn breeds familiarity and knowledge-based trust (Trapido 2007).
Many blockchain projects we observe today (e.g. TradeLens, B3i)\(^6\) are a result of cooperation between competitors. Rival companies form initiatives and consortia in order to address industry inefficiencies with the use of blockchain. Competitive embeddedness (Trapido 2007) is crucial to form these alliances, as partners get acquainted via professional associations (Davis et al. 1990) and discuss pressing issues within their industries. At the same time, blockchain technology allows them to share their data in a secure manner. Since confidentiality and control of the data is a major issue (Bechini, Cimino, Marcelloni, and Tomasi 2008), introducing a reliable and trustworthy technology like blockchain may facilitate new cooperative relationships, which were previously not feasible, due to concerns over data security.

**Proposition 2: Introducing blockchain is facilitated by existing cooperative relations, and may facilitate new ones**

Several researchers have emphasized the critical importance of cooperation in achievement of organizational goals (Smith et al. 1995). Buckley and Casson (1988) found that cooperative relationships can provide cost savings, and decrease monitoring costs. Contractor and Lorange (1988) further found a positive relationship between inter-firm cooperation and the levels of profitability and efficiency. Cooperative relationships however, bring about their own set of difficulties. The central problem of cooperation is that firms often have only partly overlapping goals, and will tend to pursue incongruent goals if left to their own devices (Ouchi 1980). Axelrod and Keohane (1985) further argue that cooperation is only possible in situations where there is a combination of complementary and opposing interests. In this context, cooperation can take place, when actors adapt their behavior to actual or expected preferences of their relationship partners. Misaligned interests may cause partners to shirk or try to claim more benefits than initially agreed, through holdup or misappropriation of partners’ resources (Gulati

---

\(^6\) For additional information see: [https://www.tradelens.com/](https://www.tradelens.com/) and [https://b3i.tech/home.html](https://b3i.tech/home.html)
et al. 2012). Smith et al. (1995) further outline some other issues related to cooperation, such as exhaustion related to collectivist tendencies, “groupthink” and coordination of pricing (Scherer and Ross 1990).

To help explain the success or failure of the cooperation Axelrod and Keohane (1986) identified three dimensions: The pattern of payoffs, the shadow of the future and the number of players. Payoffs strongly influence the development and maintenance of cooperation as each relationship partner expects to attain a net positive value from the alliance (Parkhe 1993). The shadow of the future argument suggests that considerations about the future promote cooperation (Axelrod and Keohane, 1985), as firms compare immediate benefits from deceiving the partners with the loss of potential future gains resulting from breaking an agreement (Telser 1980). 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. The implementation will require significant investments, so partners will likely need to precisely determine payoffs for each party, before they commit to the project. Moreover, payoffs will depend on the success or failure of the entire network, rather than on individual partners, which should help align their goals and induce cooperation. As records on the blockchain are tamper evident, the “shadow of the future” should dissuade actors from engaging in opportunistic behavior. Similarly, blockchain’s inherent transparency would allow to easily identify and sanction any party breaking an agreement, irrespective of the number of actors in the network.
Proposition 3: The economic benefits incurred by implementing partners will depend on the success or failure of the entire blockchain network, which will help to align their goals and foster cooperation

Even though inter-firm cooperation may lead to different outcomes, one of the most desirable results is achieving effective coordination (Smith et al. 1995). IORs require that at least some of the activities are split between the relationship partners (Sobrero and Schrader 1998). This division of labor requires relationship partners to coordinate disparate operations, administrative systems, production philosophies and similar (Borys and Jemison 1989). Gulati et al. (2012) define inter-firm coordination as “deliberate and orderly alignment or adjustment of partners’ actions to achieve jointly determined goals”. They suggest that coordination is normally associated with sharing of information, decision-making and feedback mechanisms, which aim to align partners’ efforts and combine their resources in a productive manner. Sobrero and Schrader (1998) differentiate between contractual and procedural coordination. They define contractual coordination as a reciprocal distribution of rights among involved partners, and suggest that such distribution is the main determinant of how coordination can develop. Procedural coordination on the other hand, involves mutual exchange of information between the parties. It refers to day-to-day communication between employees involved in the relationship, which allows them to learn and adapt their activities to one another (Hamel, Doz, and Prahalad 1989; Sobrero and Schrader 1998).

Blockchain establishes a common information infrastructure, meaning that all the relevant partners share identical data. This might lead to a significant reduction in the need for procedural coordination, particularly in terms of information sharing and feedback mechanisms. Moreover, programmable rules (i.e. smart contracts) might result in automation of several day-to-day procedures, making their execution more efficient, as well as more reliable.
Proposition 4: Implementing blockchain in an IOR will decrease the need for procedural coordination

The need for coordination stems from the fact that IORs are characterized by mutual interdependence, meaning that each firm is vulnerable to its partners (Ireland et al. 2002). Coordination scholars have suggested that higher levels of interdependence, along with higher uncertainty and asset specificity, demand more comprehensive forms of coordination (Dyer 1996; Gulati et al. 2012). Grandori and Soda (1995) further argue that practically all approaches to coordination between firms are concerned with the governance of interdependence. Pooled interdependence exists in alliances where “each part renders a discrete contribution to the whole, and each is supported by the whole” (Thompson 1967). It occurs where companies pool their resources to reach a common strategic goal (Gulati and Singh 1998). Coordination requirements for this type of interdependencies are low, as there is little need for serial ordering of activities (Dekker 2004; Thompson 1967). The mechanisms to achieve a coordinated outcome in pooled interdependencies are therefore least costly, and involve communication, rules and procedures and some dedicated common staff (Grandori 1997; Gulati and Singh 1998). In cases of sequential interdependence, partners’ activities are distinct and sequentially ordered, meaning that the output of one relationship partner is the input of another (Grandori 1997). Sequential interdependencies require higher degree of coordination than pooled interdependence (Gulati and Singh 1998). Cross-activity programming has been suggested as an efficient coordination mechanism for these type of interdependencies (Grandori 1997; Thompson 1967). In alliances characterized by reciprocal interdependencies, partners exchange the outputs with one another simultaneously, meaning that partners produce inputs for other entities and use outputs from them (Grandori 1997; Gulati and Singh 1998). Reciprocal interdependencies require more complex coordination mechanisms (Dekker 2004), as relationship partners must continuously communicate and adapt to one another (Gulati and
Singh 1998). The challenges associated with interdependencies have also been referred to as coordination costs (McCann and Galbraith 1981) by organization design scholars, and are especially salient in alliances, because they encompass considerable coordination activities among partners and across organizational boundaries (Gulati and Singh, 1998).

Blockchain enables new kinds of distributed architectures, where partners operate in a shared network. This mandates that partners standardize their data and align their processes already in the startup phase. After the network becomes operational, relevant relationship partners will need to reach a consensus about the validity of transactions before they are recorded on the blockchain (Nofer et al. 2017). This implies that a blockchain implementation project will change the nature of interdependencies between partners in the pertinent network, as the partners will be required to both carefully develop a network at the outset of the project, as well as jointly maintain it after it becomes operational.

**Proposition 5: Blockchain will change the nature of interdependencies between IOR partners both in the startup phase (standardizing data and aligning processes), as well as in the operational phase (reaching consensus)**

Coordination of IORs can pose challenge for the organizations, because both conflict and cooperation are present at the same time, and because there is a lack of formal authority structure (Litwak and Hylton 1962). Even in situations where there is a complete trust and alignment of interests among partners, they still need to divide their activities and effectively coordinate to accomplish their tasks (Gulati and Singh 1998; Gulati et al. 2012). Failure to coordinate may lead to significant negative consequence for IORs, result in delays and inefficiencies and can obstruct partners to reach alliance goals (Mohr and Spekman, 1994). Gulati et al. (2012) identify several ways in which coordination failures can be avoided, and organize them into structural, institutional and relational school of thought. Structural
perspective argues that coordination failures can be mitigated by an appropriate organizational and job design, as formal contracts and JV structures can mirror main elements of hierarchy (Stinchcombe 1985). Institutional perspectives suggest that coordination failures can be circumvented, not just by explicit rules, but also by means of implicit assumptions and informal norms (Gulati et al. 2012), assumed by broad societal institutions (DiMaggio 1997). The relational school of thought on the other hand, argues that a significant part of inter-firm coordination is spontaneously achieved by individuals or groups (Gulati et al. 2012), as alliance managers directly interact with others to address uncertainties and interdependencies (Follett and Urwick 1949). Gulati et al. (2012) also analyze coordination mechanisms along different stages of alliance. First, in the partner selection stage, organizations may look for partners based not only on their competence, but also on the compatibility concerning processes, resources and culture (Stuart 1998), which might be used a proxies for ex-ante coordination concerns (Gulati et al. 2012). During the stage of alliance design, partners need to determine the proper enforcement mechanisms, authority structures and dedicate appropriate staff that fits the purpose of the relationship (Gulati and Singh 1998). Creating comprehensive contracts, outlining partners’ roles, task, responsibilities and information feedback channels, can help them mitigate some of the coordination problems (Reuer and Ariño 2007). Finally, during post-formation dynamics, alliance partners’ motivation are put to the test (Gulati et al. 2012). As the relationship develops, partners may choose to alter some of the agreements for which an initial consensus has been reached in order to enhance the performance of the alliance (Gulati et al. 2012). Partners’ learning will ultimately be integrated into relationship routines that can enhance coordination (Reuer and Ariño 2007).

Specific rules can be programmed and enforced on a blockchain network, which may imply that the technology has the potential to mirror the formal hierarchy structure (Stinchcombe 1985). Because of these capabilities, blockchain may be able to serve as a coordination
mechanism, as advocated by the structural school of thought (Gulati et al. 2012). Programmable rules and automatic enforcement of agreements indicate that the first two stages of an alliance, as proposed by Gulati et al. (2012), namely partner selection and alliance design, are particularly important for achieving effective coordination via blockchain. Selecting an appropriate partner with compatible processes and the ability to commit sufficient resources needed for data and process standardization, could significantly alleviate the implementation and decrease coordination concerns. Later, during the alliance design stage, partners also need to carefully determine the rules and procedures, which will be programmed on the blockchain, and serve as an enforcement mechanism.

**Proposition 6: Blockchain can act as a coordination mechanism in IORs by mirroring formal organizational structure**

**Trust**

The concept of trust has been widely discussed across several different disciplines, particularly within areas such as psychology, sociology and philosophy. Within other disciplines, such as business management, conceptualizing of trust developed considerably during the 1980s, followed by a number of empirical studies in the late 1990s (Wennblom 2012). In the context of IOR, researchers have studied trust in areas such as supplier relations, joint ventures and strategic alliances in general (Ireland et al. 2002). This wide-ranging interest in the concept of trust across disciplines has resulted in several different definitions. While some scholars define trust broadly as trustor’s expectation about the probability of having a desirable action performed by the trustee, others propose a more narrow definition, in terms of trustor’s evaluation of trustee’s reliability and goodwill (Das and Teng 1998). Rousseau et al. (1998) analyzed the meaning of trust across disciplines, and concluded that basic elements and
definitions are “not so different after all” across different fields. They define trust as “psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behavior of another” (p. 394). In IORs, trust represents a firm’s expectation that its relationship partner will not act opportunistically (Gulati 1995) and will behave as anticipated (Poppo, Li, and Zhou 2016).

Development of inter-firm trust is often argued to be the basis for maximizing alliance value (Ireland et al. 2002). It can reduce transaction costs (Gulati 1995), spur desirable behavior (Madhok 1995), lead to decreased levels of conflict (Gulati and Sytch 2008), enable greater knowledge and information transfer (Poppo et al. 2016), increase managerial flexibility (Friedman 1991) and reduce concerns about opportunistic behavior (Gulati et al. 2012). Trust is especially important in IORs characterized by high volatility and uncertainty (Neumann 2010), where rapidly changing circumstances make it difficult for firms to depend on formal controls alone (Kamminga and Van der Meer-Kooistra 2007). In such environments, reliance on trust can decrease the perceived need for formal legal structures and safeguards (Ring and Van de Ven 1994). Granovetter (1985) on the other hand, warns that the development of trust is insufficient to ensure trustworthy behavior. He points out that high trust increases the potential gains from betrayal of that trust. McAllister (1995) further argues that high levels of cognition-based trust could be the main predictor of free riding and social loafing. Ring and Van de Ven (1994) also caution against situations, where IOR emerge out of previous friendships, and where parties intentionally leave details loose, without the formal controls to safeguard their expectations. Such circumstances can lead to significant imbalances between legal arrangements and informal ties, and may result in the breach of trust and ultimately the dissolution of the relationship.

There are different forms of trust, contingent on the bases from which it is reached (Wennblom 2012). A commonly used classification (e.g. Das and Teng 1998; Langfield-Smith 2008; Vélez,
Sánchez, and Álvarez-Dardet (2008) differentiates between competence trust and goodwill trust. While the former relates to partner’s technical ability to perform activities as agreed in the contract (Langfield-Smith 2008), the latter refers to firm’s confidence in predicting partner’s intentions to act as agreed (Ring and Van de Ven 1994). Emsley and Kidon (2007) further argue that different types of trust are relevant at different levels of the company. They suggest that goodwill trust is particularly important at the executive level, while competence trust is more relevant for the operational level. It should be pointed out however, that this is neither the only categorization found in the IOR literature, nor do all the authors use the same terminology. Vosselman and Van der Meer-Kooistra (2009) for example, make a distinction between thin and thick trust. Thin trust is achieved by formal contracts, resulting control structures (Minnaar, Vosselman, van Veen-Dirks, and Zahir-ul-Hassan 2016), and requires trust in institutions outside the relationship (Vosselman and Van der Meer-Kooistra 2009). Thick trust on the other hand, is produced through ongoing interactions between partners (Neumann 2010), and results in positive behavioral expectations about the behavior of other parties (Vosselman and Van der Meer-Kooistra 2009). Yet another classification is provided by Poppo et al. (2016), who distinguish between calculative trust, where managers believe that the costs of acting opportunistically will be greater than the benefits associated with it; and relational trust, which emerges from social relationships, where there is a strong belief about the goodwill and honesty of others. A useful categorization that encompasses several categorizations found in the IOR literature, is provided by Wennblom (2012), who classifies (reasons for) trust as rational and emotional. Rational trust reasons comprise of calculus-based trust, knowledge/competence trust and cognition based trust, while emotional trust includes identification-based trust and relational based trust.

Blockchain is often referred to as the “trust-less” technology (e.g. Xu et al. 2017) and the “trust machine” (The Economist 2015) which might imply it has the potential to replace trust within
and between organizations. This assertion may not necessarily be correct. While blockchain’s cryptography and consensus mechanisms are able to replace trusted intermediaries when transferring cryptocurrencies, the same does not apply to IOR. The label “trust-less” refers to the belief that a party cannot “double spend” the funds while transferring them via blockchain. It does not guarantee that an individual making the transfer actually owns these funds (someone could have stolen their private keys), or that they were not coerced to transfer them. Moreover, several blockchain implementations (e.g. within supply chains) refer to exogenous data. Unlike Cryptocurrencies, which only exist within a blockchain, economic transactions reside outside of accounting records (Coyne and McMickle 2017). While asset ownership might be verified by blockchain records, its condition, location and worth must still be assured (ICAEW 2017). Albeit the blockchain itself cannot ensure that a certain party will not break an agreement, or act opportunistically, inbuilt consensus mechanisms could decrease the possibilities for opportunism. Moreover, regular monitoring of immutable records, recorded on the blockchain, would increase the probability of such behavior being detected and sanctioned (Colletti et al. 2005), which might imply that goodwill trust will be (at least to a certain extent) replaced by calculative trust.

**Proposition 7: Introducing blockchain in IORs can replace goodwill trust with calculative trust**

One of the most debated topics within management accounting literatures related to IOR and trust, is the trust-control relationship. Researchers have long focused on this issue, because both trust and control are core elements of cooperation between firms (Long and Sitkin 2018). This relationship however, is not generally agreed upon, and different perspectives can be found in the literature. Emsley and Kidon (2007) claim that the field is far from understanding how control and trust coexist and several fundamental issues remain unresolved. The basic question related to this issue is whether control and trust are complements or substitutes (Long
The complementary perspective argues that trust and formal control are additively related and that an increase in the level of one will result in higher level of another (Poppo and Zenger 2002). Coletti et al. (2005) for example, indicate that control induces cooperation which in turn positively affects trust. Dekker (2004) further argues that mutual transparency between companies is an important basis for trusting relationship, and that formal controls add to this transparency. He considers information sharing between organizations as a form of formal control. Several authors (e.g. Catalan and Kotzab 2003; Dekker 2004; Mahama 2006; Baiman and Rajan 2002; Nicolaou et al. 2011) agree with this viewpoint, and further argue that information sharing enables partners to achieve a common understanding of their roles and responsibilities, allow for coordination of tasks, reduce information asymmetry and advance trust building, which reduces concerns about partner opportunism. The substitution perspective on the other hand, posits that control and trust are inversely related and that more trust implies less control and the other way around (e.g. Wicks, Berman, and Jones 1999; Van der Meer-Kooistra and Vosselman 2000). Tenbrunsel and Messick (1999) for example, argue that the mere presence of a control system changes how decision makers mentally frame the situation, which in turn causes them to perceive other collaborators as less trustworthy. Partners who rely solely on formal controls can hinder the development of a trusting relationship, by signaling they are wary of their exchange partners (Long and Sitkin 2018). Tomkins (2001) presents a different view on this relationship, and depicts a functional association between trust and information need as an inverted U-curve. He suggests that at the early stages of relationship, there will be a lower need for either trust or information as an uncertainty absorbing mechanism. As the relationship matures, the association between trust and information need will become positive, because trust itself cannot be increased without further information. Finally, as the trust becomes established, less information is needed to maintain the level of trust. Yet another view is presented by Das and Teng (1998), who suggest that
trust-control relationship is of a supplementary character. They argue that the two concepts exist in parallel, and that control mechanisms influence the level of trust, which in turn moderates the control mechanisms in determining the level of control.

Implementing blockchain within IOR establishes a shared information infrastructure in which all relevant relationship partners must validate the transaction before it is recorded on the blockchain. Once the data is recoded, any non-consensual changes applied to the records would be evident to participants in the network (Rauchs et al. 2018). As such, blockchain has the ability to reduce information asymmetry, which is viewed as an origin of power in relationships (Mahama 2006), and a main source of opportunism risk (Clemons and Hitt 2004). Blockchain could also be viewed as an accountability system (Mahama 2006), which facilitates information gathering and promote information sharing through feedforward and feedback loops. Resulting transparency could serve to align the efforts of relationship participants, ensure they equally take responsibility for producing collective benefits and reduce their tendency to engage in free-riding and social loafing (Mahama 2006).

**Proposition 8: Introducing blockchain in IORs will decrease information asymmetry and increase trust among partners**

**Inter-organizational control**

IORs allow firms to realize benefits such as reduced costs, risk sharing, access to valuable resources in the form of proprietary technology, knowledge and additional capital, as well as to strengthen their market position (Groot and Merchant 2000; Ding, Dekker, and Groot 2010). Nevertheless, numerous studies have documented a high failure rate for IORs, emphasizing their inherent complexity and describing them as arrangements fraught with issues because firms must rely on the cooperation, competence and a certain level of benevolence on the part of their partners to achieve stipulated alliance objectives (e.g. Das and Teng 1996; Chua and
Furthermore, the success of an IOR to a large extent depends on partners providing correct information to one another (Neumann 2010). However, due to issues such as pre-contractual information asymmetry and opportunism (Arrow 1985; Milgrom and Roberts 1992), firms often struggle to accurately assess partners’ resources and core competencies. An extensive body of literature primarily in management accounting and economics 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 (Anderson and Dekker 2005; Williamson 1985; Dekker 2004; Neumann 2010). Selecting an appropriate partner in an IOR has been identified as an important way in which firms can mitigate control problems, with some studies suggesting that identifying a suitable partner is critical for the success of IORs (e.g. Ireland et al. 2002), and that the partner selection phase can strongly influence latter stages of the collaboration since it precedes and informs the design of contractual and management control structures (Dekker 2004; 2008). “Partner selection” is here referred to as the process of searching for, evaluating, and ultimately selecting a transaction partner (Blumberg 2001; Dekker 2004, 2008; Ding, Dekker, and Groot 2013).

Prior studies analyze the partner selection process in terms of the time spent by firms to find exchange partners, the effort exerted to evaluate them (which includes the development of evaluation criteria), as well as the relative importance placed on different selection criteria in the choice of a partner, all of which are seen as inter-related aspects of the firms’ response to the underlying transaction hazards (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 (Mitchell and Fitzgerald 1997; Dekker and Van den Abbeele 2010). Furthermore, in these studies partner selection is
conceptualized as an explicit ex ante management control choice in IORs, closely related to contract complexity. Specifically, Ding et al. 2013 find that in IORs characterized by a high level of interdependence between partners, and a broad scope of collaboration, firms on the one hand carefully select partners by relying more strongly on reputation and trust-based criteria, and on the other hand make use of complex contracts. Blockchain architecture provides a resilient, replicated, sequentially ordered record of interactions between partners in IORs. On a blockchain, the process through which data is exchanged and recorded inherently implies mutual interdependence and sequential interaction between involved parties, as blockchain protocols rely on responsible and accurate record-keeping by a network of legally independent, and mutually constraining “record keepers”. The latter characteristic is related to the tamper-evident nature 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 records (i.e. the consensus mechanism). These characteristics significantly increase the reliability of records. Furthermore, the sequentially ordered history of interactions consisted of data in a standardized format that typifies a blockchain ledger makes ex post observation of prior interactions less costly and less time-consuming. Hence, in an IOR context, blockchain technology should have implications for the partner selection process. Namely, the combined effect of the reliability of records, and the greater ease of observability of prior interactions should improve the process of designing evaluation criteria for potential partners, and reduce partner search efforts in terms of search time.

**Proposition 9: Over time, blockchain technology mitigates ex ante control problems in IORs through improved partner selection**

Contracts are voluntarily initiated documented agreements between exchange partners that govern their relationship and incorporate procedures, incentives, mutual obligations and dispute-resolution mechanisms, thereby providing a framework for cooperation between those
partners (Schepker, Oh, Martynov, and Poppo 2014). Contracts are primarily used to control verifiable actions and outcomes. They can take a variety of forms, from standard, boilerplate to highly customized; from explicit and “complete” to more open, containing “incomplete” formulation of task execution and output; from arm’s length where the identity of the partners is irrelevant, to highly complex and multi-layered where factors such as prior interaction, reputation, and identity matter as parties need to continually adapt to changes in the environment (Schepker et al. 2014). Management accounting studies consider contracts to be an integral part of the management control structure of IORs. The theory further suggests that contracts can alleviate inter-partner frictions by specifying the nature of residual claims and the allocation of decision rights (Abdi and Aulakh 2017, Anderson and Dekker 2014; Aghion and Bolton 1992). A prominent stream of research focuses on contractual clauses that are aimed at aligning and safeguarding partners’ interests, and facilitating coordination and adaptation (e.g. Williamson 1975, 1985; Klein, Crawford, and Alchian 1978; Anderson and Dekker 2005; Reuer and Ariño 2007).

In a related study, Krishnan, Miller, and Sedatole (2011) discuss contracting in the presence of demand and task uncertainty. The authors argue that under these conditions, accounting performance measures could become all but useless for contracting purposes, driven by uncontrollability-induced observation difficulties. Other studies (e.g. Banker, Kalvenes, and Patterson 2006) emphasize that a shared information exchange infrastructure between partners enables greater contract completeness by making monitoring additional dimensions of supplier performance more economical. Here, the conceptualization of buyer-supplier contracts draws from the literature on incomplete contracts (e.g. Grossman and Hart 1986; Hart and Moore 1990; 1999; Milgrom and Roberts 1992), which deals with supplier monitoring costs, and expands on it by specifically distinguishing between aspects of suppliers’ activities that should be included in the contract, and those that should be monitored. As was argued above,
fundamental technical and governance characteristics of blockchain technology improve reliability and ex post observability of records shared between partners. Additionally, smart contracts enable the routinisation of inter-firm processes involving blockchain-endogenous data, reducing them to a set of articulated interaction patterns that are automatically executed when pre-defined conditions are met. The monitoring and the execution phase of this process incur no additional direct costs. Taken together, these functionalities should alleviate observation difficulties in IORs, and allow partners to more precisely specify activities that should (and can) be included in formal contracts.

**Proposition 10: Blockchain technology enables the design of more complete contracts in IORs**

Other studies (e.g. Reuer and Ariño 2007; Anderson and Dekker 2005) identify different dimensions of contracts that are interdependent and in combination serve to allow for greater coordination and adaptation between partners, and better enforcement of agreements. This is achieved through clear delineation of tasks, guidelines for partners’ activities, and establishment of communication routines, which simplifies decision-making and lowers the possibility that disputes will arise. These provisions can be further differentiated, with the former two pertaining to “contractual control”, and the latter pertaining to “contractual coordination” (Lumineau 2017; Schilke and Lumineau 2018). Contractual control is here seen as a mechanism that creates adherence to a desired outcome with a minimal amount of anomalous behavior through the exercise of authority or power mechanisms, while contractual coordination represents a means to achieve a desired collective outcome, and to facilitate goal congruence between partners (Lumineau and Malhotra 2011). The aforementioned standardization of data formats and execution patterns inherent to blockchain technology serve to make partner interactions in IORs more predictable, while the 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. Consequently, the use of blockchain technology in IORs should improve contractual coordination through the exercise of shared rules and “authority” that is distributed in nature.

**Proposition 11: Blockchain technology increases the level of contractual control between partners in IORs without increasing reliance on centralized authority structures**

**Information exchange**

Over the past several 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. As markets have become more competitive, interconnected, and in turn, interdependent, and as technology has advanced, collaborative arrangements between market actors have become in many cases preferable to outright vertical integration. The emergence of technologies for information collection, conversion, dissemination and monitoring within and across organizational boundaries has played an important role in these developments. Technology-enabled inter-organizational information systems (IIS) often represent a primary means of information exchange across firm borders in an alliance (Gulati and Singh 1998). As such, they play a significant role in the control of IORs, represent an important source of competitive advantage, and are ultimately critical to the success of inter-organizational collaboration (Anderson and Sedatole 2003; Nicolaou, Sedatole, and Lankton 2011). Recognizing these developments, since the mid-1990s scholars from several areas of organizational research have investigated issues related to exchange of decision-relevant information across organizational borders. At the most basic level, the purpose of adopting IIS is to implement computerized communications among partnering organizations. Studies investigating 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 IIS. Moreover, the throughput of this information forms a structural capability that addresses information-processing needs of partners (Schloetzer 2012; Narayanan, Marucheck, and Handfield 2009; Bensaou and Venkatraman 1995). 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; Kulp, Lee, and Ofek 2004; Bala and Venkatesh 2007). 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, IIS are defined as technology-enabled information systems used by two or more organizations that facilitate creation, storage, transformation, and transmission of operational, strategic, performance and accounting information, and provide an efficient coordination mechanism for transacting partners (Nicolaou et al. 2011; Christ and Nicolaou 2016) (see also: Riggins, Kriebel, and Mukhopadhyay 1994; Nicolaou and McKnight 2006). Such an information system thus represents not merely a set of computing devices for facilitating internal information processing activities, but rather a crucial means of establishing and maintaining effective inter-firm collaboration (Wang and Seidman 1995). These systems ultimately allow for the generation and manipulation of comprehensive virtual perspectives on the nature and flow of resources within and between organizations (Chapman 2005; Chapman and Kihn 2009). Blockchain technology essentially represents a new form of IIS. In that sense, it is comparable to other technologies which are intended for inter-firm communication, the
most prominent example being electronic data interchange (EDI). Existing IIS such as EDI enable point-to-point communication between firms, which makes them suitable for dyadic (i.e. one-to-one) or hub-and-spoke (i.e. one-to-many) IORs. Conversely, blockchain’s core attributes enable end-to-end, multi-lateral (i.e. many-to-many or network-based) information exchange between partnering firms. Moreover, the governance mechanism inherent to blockchain technology necessitates validation of actions (e.g. exchange of decision-relevant information) by multiple independent entities, thereby increasing 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. The records in a blockchain network are considered valid only after a uniform view on the state of the shared ledger and the order of events (i.e. a consensus) has been reached on a network level. This mechanism entails high overhead costs, since the same data records need to be replicated and maintained by multiple parties. Conversely, the use of blockchain technology is likely to significantly reduce the costs and task complexity related to reconciliation of records, as it essentially collapses the two processes of data exchange and reconciliation of records into one.

**Proposition 12: Blockchain technology enables many-to-many information exchange between partners and thus facilitates the establishment of network-based IORs**

The information exchanged via IIS has itself been an important topic of inquiry among management accounting scholars. Here, a distinction has been made between coordination and control uses of information exchanged between partners. 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).
Inherent technical attributes of blockchain technology entail that the shared, mutually agreed-upon, tamper-evident 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 these 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, programmable self-executing rules (i.e. smart contracts) enable automated enforcement of standardized, routine interactions between partners. A primary way in which control is implemented via IIS 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 technology as the IIS in IORs should reduce control complexity through improved monitoring, self-disciplining mechanisms, and simplified performance evaluation.

**Proposition 13: Once operational, blockchain technology reduces information exchange-related control complexity in IORs**

Existing research on IIS focuses on the issues of adoption, use, and value of IIS in IOR. Furthermore, it discusses the role of IIS infrastructure on IOR governance issues, including the development of IIS standards, as this has been found to be a crucial determinant of making inter-firm processes efficient and performance-enhancing (Bala and Venkatesh 2007; Markus, Steinfield, Wigand, and Minton 2006).

Early studies investigated the antecedents and consequences of the initial establishment of IIS between partners. Building on prior literature, which has explored the “critical mass” and “start-up” problems of networks (e.g. Rohlf 1974; Oren and Smith 1981), Riggins et al. (1994) argue that the inter-organizational nature of IIS implies that network externalities play a major
role in how firms realize potential benefits from these systems. The study finds that after an initial stage of spontaneous network growth, the growth of the network may stall. A possible explanation for this finding is offered in a related study. Here, unlike Riggins et al. (1994), Wang and Seidman (1995) recognize that participants in a given network are either trading partners or competitors, making their identity a critical factor in determining any individual firm’s willingness to join. The main focus of the study is on the strategic side of IIS implementation and the structure and effects of electronic integration. The findings suggest that buyers sometimes use fewer suppliers in spite of the reduction in transaction costs associated with IIS adoption because of a combined effect of a decreasing marginal profitability for the buyer, and negative externalities imposed on other suppliers with each new supplier joining the network beyond a certain threshold. Further explanation for these issues is offered in a study by Barua and Lee (1997). Their results suggest that as IIS converge toward a uniform standard, the importance of investment incentives is reduced, since the investment stops being relationship-specific and can, as such, be used by the suppliers in multiple supply chain relationships. Consequently, it is argued that as IIS continue to develop and the investment by the suppliers in the system increases, that the relationship-specific part of the investment may actually be reduced. Other studies put IIS in a broader context of IORs, focusing on the relationships among partners (Nicolaou and McKnight 2006). As was discussed previously, important aspects of IORs are different characteristics of information (e.g. amount, type, timing) that is being exchanged between the contracting parties, and the network infrastructure that the partners put in place to facilitate this exchange. Earlier accounting studies, which have investigated the value of information systems (e.g. Feltham 1968) have been extended in the context of IIS and IORs to include concepts such as partner opportunism in information exchange (e.g. Clemons and Hitt 2004; Zaheer and Venkatraman 1994; Baiman and Rajan 2002), and coordination and cooperation among partners (Gulati and Gargiulo 1999). Empirical
studies in this research stream (e.g. Kulp et al. 2004) suggest that information sharing is a necessary condition for IORs and partner firms to remain competitive, however it is not sufficient to achieve supranormal profitability. This indicates that the majority of benefits from IIS relate to the establishment of a common information infrastructure, which largely depends on collaborative practices between partners, rather than solely on information exchange per se (Kulp et al. 2004). The underlying issues related to opportunism in inter-firm information exchange are information asymmetry between partners, and the inability of partners to easily enforce property rights (i.e. prevent information misappropriation) over exchanged information and directly monitor its use (Baiman and Rajan 2002; Clemons and Hitt 2004). As was discussed earlier, a blockchain represents a common information infrastructure in the sense that all the involved parties share an identical record of data that has been exchanged according to a network-wide protocol. Furthermore, the blockchain ledger possesses a critical attribute of tamper-evidence, which improves monitoring through higher transparency of data and self-regulating mechanisms. The blockchain’s inherent data sharing and governance protocol, the sequential nature of the data recording process, as well as the auditability of the shared ledger should also enable partners to improve their ability to enforce property rights over their data, to the extent that it is exchanged through a blockchain-based IIS.

**Proposition 14: Blockchain technology reduces the level of information exchange-related opportunism in IORs**

An aspiration to improve inter-organizational coordination through the use of IIS 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, due to factors such as heterogeneity of interests among partners (Markus et
al. 2006; Axelrod, Mitchell, Thomas, Bennett, and Bruderer 1995), high cost of implementation and low reuse value of the investment for smaller partners (Steinfield, Markus, and Wigand 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 (Ozcan and Santos 2015; Simcoe 2012; Steinfeld et al. 2011).

Formation of industry-wide standard setting consortia has been proposed as a way to address these issues. Using Olson’s (1965) seminal work on collective action as a theoretical basis, Weiss and Cargill (1992) suggest that standards development consortia have an incentive to limit membership to 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). Basic requirements for the feasibility of the use of blockchain technology include standardization (e.g. of data formats and consensus mechanisms), wide adoption, and interoperability between different individual platforms. This implies that, in blockchain-based IIS networks, most of the benefits are expected only after the compatible blockchain platforms have reached a high level of diffusion.

Proposition 15: Blockchain technology is best suited for IORs that involve a large number of partners

---

7 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.
V CONCLUSION

Blockchain technology promotes systems that establish an open, democratic, and scalable digital economy (Wang, Chen, and Xu 2016). Beck et al. (2017) argue that blockchain is a multi-faceted innovation, namely technical (a new distributed version of a transactional database), economic (offering a reliable record of transactions in a decentralized, adversarial environment), and organizational, given that it may fundamentally change how we organize interpersonal and inter-organizational relationships. The purpose of this paper has been to review management accounting and organizational research that has examined various aspects of IORs, focusing on the areas that could significantly be impacted by blockchain technology. To that end, we have identified four areas, namely collaboration, trust, inter-organizational control, and information exchange. Within each of these areas, we have outlined some of the most common recurring issues found in the literatures, and developed various propositions, based on blockchain capabilities, indicating how the technology could have an impact in the described settings.

This should by no means be considered a comprehensive literature review about the topic of IORs, as it is limited to particular areas most likely to be influenced by blockchain technology in the future, according to our analysis. Moreover, blockchain technology is itself not yet at an optimal maturity level, and organizations aiming to implement it should first conduct meticulous feasibility studies (Wang et al. 2016). Nevertheless, several leading companies (e.g. IBM, Walmart, Microsoft, Deloitte, Mærsk) have already started to experiment with the technology, and the amount of blockchain related research is emerging at an increasingly fast pace, and in various academic fields (Nærland et al. 2017). As such, we believe that blockchains will have a significant impact on how the companies structure their IORs in the future. Furthermore, we consider an analysis of the sort provided in this paper could be
important for management accounting scholars in particular, as IORs are an important topic in this field. We hope that the propositions developed in this paper will lay the groundwork for management accounting researchers interested in blockchain in the context of IORs, and open interesting new avenues for future research.
References


[https://scholarspace.manoa.hawaii.edu/handle/10125/41815](https://scholarspace.manoa.hawaii.edu/handle/10125/41815)


Murray, A., S. Kuban, M. Josefey, 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. Published Online: 17 Apr 2019.


Scherer, F.M. and D. Ross. 1990. Industrial market structure and economic performance. *University of Illinois at Urbana-Champaign's Academy for entrepreneurial leadership historical research reference in entrepreneurship*.


**Figure 1:** Areas identified in the literature on inter-organizational relationships, which are likely to be impacted by blockchain technology.
Appendix A:

The history of blockchain

Blockchain acquired fame as the underlying technology behind Bitcoin (Beck and Müller-Bloch 2017), a purely peer-to-peer payment system, introduced in a whitepaper by Satoshi Nakamoto in 2008. The first generation of blockchains, like Bitcoin’s, provided a public ledger to store cryptographically signed financial transactions (Swan 2015). At that time, there was very limited capability to support programmable transactions, and only very small pieces of auxiliary data could be embedded in the transactions to serve other purposes, such as representing digital or physical assets. The second generation of blockchains, such as Ethereum’s, provided a general-purpose programmable infrastructure with a public ledger that records the computational results (Xu et al. 2017).

The earliest identified occurrences of the concept of a ‘blockchain’ however, can be traced further back to Haber and Stornetta (1990) and Bayer, Haber, and Stornetta (1993) who introduced the notion of a chain of cryptographically-linked data blocks to efficiently and securely timestamp digital data in distributed systems using cryptographic hashing functions and Merkle trees (Rauchs et al. 2018). The first cryptocurrency for electronic cash was already described at the dawn of the web in 1990. Further evolutions and refinements of the hash chain concept were introduced in a paper by Neil Haller on the S/KEY application of a hash chain for Unix login, in 1994 (Tasca and Tessone 2018).

The concept of DLT can be traced back even further. The Byzantine Generals Problem theorized by Lamport, Shostak, and Pease (1982) described how ‘computer systems must handle conflicting information in an adversarial environment. Subsequent research led to the emergence of the first algorithm for “highly available systems that tolerate Byzantine faults”

---

8 For more information see: https://brilliant.org/wiki/merkle-tree/
with little increase in latency (Castro and Liskov 2002). Nakamoto’s paper however, was the first to combine these concepts, and propose electronic currency based on the blockchain (Tasca and Tessone 2018).