frontiers in Blockchain

ORIGINAL RESEARCH
published: 05 March 2020
doi: 10.3389/fbloc.2020.00005

Blockchain Applications and Institutional Trust

Martin Smits and Joris Hulstijn*

Tilburg School of Economics and Management, Tilburg, Netherlands

In the current discussions around Blockchain and distributed ledger technologies, we find a lack of theory to conceptualize and understand application scenarios. In this paper we propose to conceptualize distributed ledger technologies as trust mechanisms. Whereas, previously one had to rely on a trusted third party (e.g., notary), now one must trust a complex software system—the Blockchain and distributed ledger application—as well as the parties that host the software system and ensure its effectiveness. Based on theories of e-commerce, business networks, and trust, we explore relations between trust and Blockchain design. We analyze three case studies of Blockchain applications in the diamond industry. In each case we study two complementary research questions: (1) how does the blockchain application influence trust, and (2) how do trust based requirements affect the design of a blockchain application? We formulate two propositions and find dynamic interactions between trust requirements, blockchain application design, and transaction trust.

Keywords: blockchain, trust, distributed ledger technology, application scenarios, requirements

OPEN ACCESS

Edited by:
Andrej Zwitter,
University of Groningen, Netherlands

Reviewed by:
Michael Shea,
Independent Researcher, Litchfield, United States
Hyojung Sun,
Ulster University, United Kingdom

****Correspondence:***
Martin Smits
m.t.smits@uvt.nl

Specialty section:
This article was submitted to Blockchain for Good, a section of the journal Frontiers in Blockchain

Received: *19 August 2019*
Accepted: *30 January 2020*
Published: *05 March 2020*

Citation:
Smits M and Hulstijn J (2020) Blockchain Applications and Institutional Trust. Front. Blockchain 3:5. doi: 10.3389/fbloc.2020.00005

INTRODUCTION

The popularity of Blockchain and distributed ledger technologies for business applications has increased substantially over the past years. Partly, this is due to a hype, fueled by the rising and dropping value of Bitcoin. But apart from the Bitcoin hype, how can we understand the attractiveness of distributed ledger technologies for its use in business applications? A recent claim is that Blockchain applications may enhance trust in inter-organizational relationships and business transactions. For instance, Meijer and Ubacht (2018) reviewed recent publications, and show that Blockchain is often referred to as a "trust mechanism." Regarding Blockchain as trust mechanism suggests that people now trust technology rather than institutions or agencies (e.g., notary; solicitor) and that such institutions may be combined with or even replaced by Blockchain applications. These effects of distributed technology on business networks appear to be similar to dis-intermediation and cyber-mediation effects in e-commerce (Laudon and Traver, 2018). In the case of dis- and cyber-mediation, traditional intermediaries (e.g., notary; solicitor) are augmented by or even fully replaced by technology-based platforms. However, in some cases this may require new intermediaries, e.g., a software certifier. So, by analogy, Blockchain applications may have a variety of effects on business networks and business relations, including effects on trust and effects on the network structure.

In this paper we focus on how Blockchain applications may enhance trust in business relations, and under which conditions trust is or is not established. To analyze these trust aspects, we take two distinct perspectives. First, we analyze recent Blockchain cases in order to identify how trust requirements have been specified and how such specifications affect the design of the Blockchain

application (**Figure 1**, relation A). Second, we analyze how the design of a Blockchain application influences the levels and types of trust in the business network (**Figure 1**, relation B). In this paper we do not focus on how (existing) trust may affect (new) requirements for trust (relation C).

The aim of this paper is explorative: we define key concepts in chapter 2 (including types of trust, Blockchain Technology, and a conceptualization of Blockchain Applications) and we explore three cases to identify relations between "how do trust requirements influence the design of Blockchain Applications" and also between "how does the design of Blockchain Applications influence trust" (which is a design research question, related to A in **Figure 1**) (which is an effectiveness or behavioral research question, related to B).

The remainder of this paper is structured as follows. Section Theory on Blockchain Technology and Trust defines section Blockchain Technology, and provides conceptualizations of section Blockchain Applications, conceptualizations of trust in the e-commerce domain section Trust, and develops hypotheses for testing relations A and B in **Figure 1** section Relations between Blockchain Applications and Trust. Sections Method and Relations Between Trust and Blockchain in the Diamond Industry detail the method and the case studies. The paper ends with a discussion and suggestions for future research (section Discussion and Conclusions).

THEORY ON BLOCKCHAIN TECHNOLOGY AND TRUST

We first define section Blockchain Technology, then section Blockchain Applications, section Trust, and the framework to analyze section Relations Between Trust and blockchain Applications.

Blockchain Technology

Magazzeni et al. (2017) show that Blockchain in its widest sense combines three existing technologies: (1) distributed databases, (2) encryption and (3) consensus protocols. This combination of technologies makes it possible to build applications around a representation of a shared state. In accounting terms, this shared state is a ledger: a repository of data on transactions and the distribution of assets, recorded in accounts. The consensus protocol ensures that parties maintain an identical copy, without the need for a centralized administrator or data storage. So unlike previous automated communication protocols, Blockchain, and general ledger technology make it possible to maintain a so called "*stateful shared state*" of a series of transactions (Magazzeni et al., 2017). "*Shared*" refers to the fact that all participants maintain an identical copy, unlike current systems, in which parties have to rely on their own version of events. In terms of game theory, parties have common knowledge of the state (Fagin et al., 1995). Potentially, this means a huge step forward, as it removes the need for second-guessing misunderstanding and manipulation. "*Stateful*" refers to the fact that each state of the conversation is stored. The system remembers all steps that went on before, unlike stateless communication protocols that only remember the previous step. As the history is shared, the ledger of states becomes immutable and can only be changed in case of consensus.

For a comprehensive introduction to Blockchain technology, we refer to Swan (2015), Magazzeni et al. (2017), and Smits et al. (2020). In short, a Blockchain consists of "*blocks of data*" where each block codifies a set of transactions. A block of transactions is considered valid if the transactions adhere to formal rules that can be verified automatically. For example, a sales transaction is only valid if the seller actually owns the asset to be sold. To avoid the need for a central authority, a Blockchain operates using a consensus protocol. Parties called "*nodes*" verify the validity of the latest block to be added to the chain. To do so, the nodes have to solve a cryptographic puzzle. The solution is represented by a number, called "*nonce*". Essentially the nodes vote by submitting a nonce, and after a majority of nodes have voted a block to be valid, the block is added to the Blockchain, and proof of validity (the nonce) is included in the next block. To make sure that blocks cannot be manipulated without trace, blocks are hashed. Hashing generates for each block a unique number, also called *hash*. Changing a block will result in a different hash. To allow for comparison, the hash of a block is included in the next block. Nodes try to validate the latest block. To keep track of time, also a *timestamp* is added to the next block. In other words, all pieces of evidence needed to verify that blocks of transactions are valid and unchanged, are included on the Blockchain itself.

Blockchain technology can use different consensus protocols to prove validity. The Bitcoin blockchain uses the *proof of work* (POW) protocol. Nodes need to put quite a lot of computing power into solving the cryptographic puzzle. In return, they are rewarded in the currency that is associated with the Blockchain application. Demonstrating validity has value. However, a Blockchain platform based on proof of work consumes enormous amounts of energy. An alternative system is

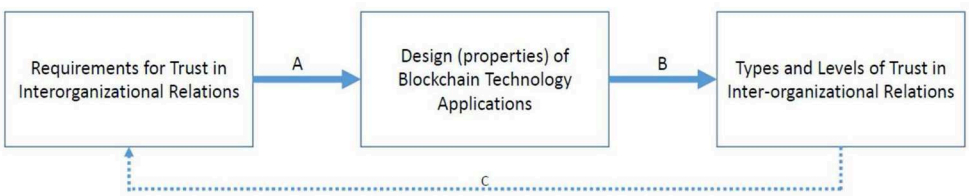

FIGURE 1 | Research model representing two complementary research questions (A,B) (see text).

based on *proof of stake* (POS). In POS, the nodes follow a voting procedure in which nodes that own more of the underlying assets, have a larger voting share. A third alternative is called *validator,* meaning that validity of a block is not determined by voting but by automated verification. A single authority or a selected group of nodes can play the role of validator. Note that such mechanisms re-introduce a form of party trust: the validators need to be trusted.

One can also distinguish *permission less* and *permissioned* Blockchains. The first are open to all actors, the second only to actors with specific permission. For example, if a multi-national firm wants to use a corporate Blockchain for swapping foreign currencies between its country offices, then it makes sense to use a closed (permissioned) Blockchain: only offices of the firm may join. On the other hand, the Bitcoin Blockchain must be open (permission less) to allow all actors worldwide access to the currency. Some authors group these two dimensions into three forms of blockchain: public (permission less, proof of work or proof of stake), consortium (permissioned, selected group of validators), and private (permissioned, single authority), see de Kruijff and Weigand (2017), based on Buterin[1]. See also section Blockchain applications under "Logic Layer."

Blockchain Applications

Blockchain technology can be applied in a business network or in other empirical settings in many different ways. Like all technologies, a Blockchain application must be understood as a sociotechnical system (Clegg, 2000). The sociotechnical system consists of the technological artifact (Blockchain, described in section Blockchain Technology) and the social environment in which the technology is applied, including the interactions between technology and social settings. To analyze the application of Blockchain technology in a specific business network (the socio-technical system), we summarize Smits et al. (2020) who specify three distinct levels at which Blockchain technology may impact a business network (see **Figure 2**).

The business network layers in **Figure 2** are based on e-commerce and business network theory (Van Heck and Vervest, 2007). The bottom layer is the *physical layer*, representing the logistics processes in and between firms (the actors), at specific locations in the network. The *information layer* represents the transactions between firms, and the transaction data stored in information systems (within firms) or in shared ledgers (shared between firms). These shared ledgers may include all data on all transactions, or—depending on the design decisions- only parts of these data. For example, only some crucial financial data or some product properties may be shared in the general ledger. Note that such design decisions may depend on trust requirements specified by actors in the network. The third layer is the *logic layer*. It specifies the business logic, like consensus protocols or validation rules, deployed to control Blockchain operations and automated transactions in other layers. We now specify the three layers in more detail, starting with the information layer (layer 2 in **Figure 2**).

[1]Buterin V. (2015). On Public and Private Blockchains, crypto renaissance salon, August 7, 2015.

The Information Layer

The information layer is where data on transactions are stored in either internal information systems of individual firms or in distributed ledgers shared between firms. Where transactions between organizations used to be stored by each organization internally (represented by separate data silo's in the information layer), transactions can also be stored now only once externally in a Blockchain ledger. Transaction data may include orders, order commitments, as well as payments and deliveries. Internal transactions within the company can be stored in a private (local) blockchain. When transactions are stored (internally or externally) in an irrevocable way in a Blockchain, this not only eliminates duplications (data redundancy), but also related inconsistencies. Another effect of the externalization of data into the shared ledger is mitigation of data heterogeneity. Data representation standards and ontologies will still be needed to enforce a shared definition of crucial concepts, but their reach and effect at the network level will be much stronger, as they are not only used for exchanging data but also for storing the data.

The Physical Layer

The physical layer represents the firms (including intermediaries) and logistics operations involved in the business network. From an organizational perspective, Blockchain-enabled transactions will affect the position of the intermediaries in the physical layer. In particular, *intermediaries supporting information exchange or trust* will be threatened, but this may depend on the type of service offered by the intermediary (e.g., Giaglis et al., 2002). *Search intermediaries* may not be affected. *Trust intermediaries* may be affected if the basis for trust shift to Blockchain security. *Information exchange intermediaries* may be affected because Blockchain aims for single point of storage.

Business transactions are usually related to the movements of goods represented in the physical layer. However, as has been argued in the service science literature, there is an evolution from a goods-dominant logic to a service-dominant logic ("*servicification of goods*"). This not only means that the service sector grows in economic significance, but also a shift from the emphasis on control (ownership) of resources toward use of resources (access right). For example, there is, for instance, less need to own a car if you can have a car or a taxi service, when you need it.

These developments reinforce and are reinforced by Blockchain technology: Blockchain based transactions can be used to transfer money (Bitcoin), but also to transfer access keys for digital products (software and e-books). In the same vein, it can be used to transfer ownership rights on registry goods like houses and ships, and trace consecutive owners along a supply chain.

It is still unclear to what extent transfers of ownership can be turned into valuable services and data. Perhaps Blockchain transactions cannot govern all exchanges at the logistics, physical level. Still, it is expected that Blockchain based transactions will not only record but also govern a large amount of economic exchanges. This may affect operational efficiency (less human effort in the loop) and control efficiency (external control by IT replacing internal control). Together with the savings (and

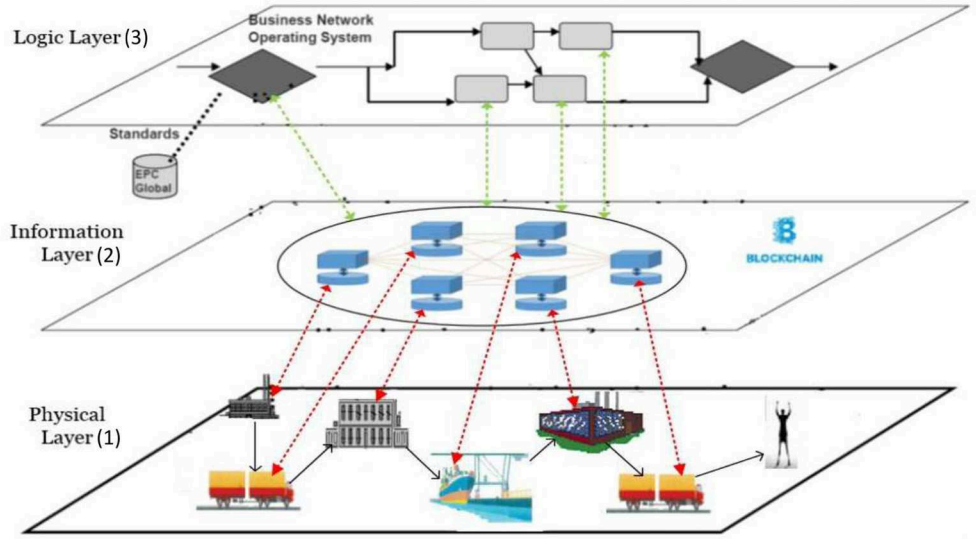

FIGURE 2 | Blockchain applications relate to three business network layers (based on Van Heck and Vervest, 2007; Smits et al., 2020).

costs) at the information layer, this may cause significant savings in transaction costs that in turn may also affect the business network structure.

The Logic Layer

The logic layer is the third business network layer and can become rather complex because it may contain logic and smart contracts that (automatically) do tasks like (i) allowing access to business actors in the network, (ii) executing transactions, (iii) managing risks and rewards, and (iv) assigning roles and responsibilities to business actors (Van Heck and Vervest, 2007). Blockchain transactions can be embedded in smart contracts that are executed automatically. At this moment, smart contracts are still in their infancy, but in principle, there is no computational limit to their scope and smart contracts could take on automated coordination of the other two layers.

We use the 4 × 4 model (Birch et al., 2016) to analyze the logic layer in a blockchain-enabled Smart Business Network. The 4 × 4 model distinguishes four types of logic:

Communication logic: This is the logic for communication between participants in the network. Communication logic includes logic for providing and getting "access to read" and "access to write" for various actors in the Blockchain application (Brennan and Lunn, 2016). Brennan and Lunn (2016) state that in a permission less public Blockchains anyone can read and write on the Blockchain, as long as they meet certain criteria and follow the specified rules. This type of Blockchain is entirely distributed, is a single source of truth and has entirely trustless integrity. A well-known example is the Bitcoin Blockchain. Second, in a permissioned public Blockchain, only permissioned entities may write the ledger, but anyone may view the content. This results in greater accountability and transparency. This form shows great potential in the financial services sector. Third, permissioned private Blockchain, only permissioned entities can read and write on the Blockchain. This form is mostly used in experimental settings where R&D is the main purpose of its existence. A well-known example is the R3CEV consortium (www.R3.com/about).

Content logic: This type of logic is related to the type of goods and services in the business network and the types of assets that are distributed over the network. On a blockchain, many types of assets can be transferred, like cryptocurrencies, letters of credit, or stock bonds. The token value can be simply information, representative of extrinsic value or have intrinsic value. It may also be possible to configure multiple kinds of assets on a single Blockchain.

Consensus logic: To ensure that only legitimate transactions are added to the blockchain, the participating nodes in the network use voting to confirm that new transactions are valid (see above). A new block of data will be added to the Blockchain only if miners in the network reach consensus as to the validity of the transaction. Consensus can be achieved through many different voting mechanisms. The most common is Proof of Work, which depends on probability through the amount of processing power donated to the network (Wright and De Filippi, 2015).

Contract logic: Also defined as the automation logic; the way that transactions are animated to trigger events. Using Blockchain technology, parties have the possibility to confirm that an event or condition has in fact occurred without the need for a third party. A well-known application is a "Smart Contract": a computable contract where the determination of performance and enforcement of contractual conditions occur automatically, without the need for human intervention (Wright and De Filippi, 2015).

Each of the four types of logic can be modified (designed) to optimize the logic layer and to achieve different business objectives (Birch et al., 2016).

Analyzing the Design of a Blockchain Application

To analyze the design of a Blockchain application in a business network setting, we use the three layer model defined above and the nine questions given in **Table 1** (Smits et al., 2020). These questions identify the relevant aspects of the current situation ("As Is") of the Blockchain application in the three layers.

Trust

Trust has been studied in various disciplines. Here we use economic literature (Gambetta, 1988), where trust is related to transactions between buyer and seller. In a (simple) transaction, the buyer needs to trust the seller to deliver the goods or services; and the seller needs to trust the buyer to pay. There are two possible perspectives: trustor (needs reasons to trust the trustee) and trustee (needs to be seen as trustworthy by the trustor). Most literature focuses on the trustor's perspective. Trust is a crucial factor in business relations where there is uncertainty, interdependence, and fear of opportunism, as is the case in online markets (Pavlou and Gefen, 2004). Trust is the foundation of e-commerce (Keen, 1999). Trust between actors has been defined as a "*belief* that the seller will behave in accordance with the consumer's confident *expectations* by showing ability, integrity, and benevolence" (see e.g., Pavlou and Gefen, 2004). Trust is also characterized as "the *willingness* of a party *to be vulnerable* to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al., 1995, p. 712). So usually, trust refers to a relationship between parties.

TABLE 1 | Questions to assess the three layered design of a Blockchain application.

Physical layer (1)	1. Which firm starts (or started) the Blockchain application, and seeds the first block?
	2. Is the Blockchain application provided by an existing actor in the network or a new entrant (cyber-, dis-intermediation, or re-intermediation)?
	3. Which other firms participate in the Blockchain application?
	4. Is the Blockchain application closed (private blockchain) or open to other firms (public or hybrid blockchain)?
Information layer (2)	5. Which transaction data are stored in the Blockchain (and which data not)?
	6. How is the Blockchain application linked to other (internal and inter-organizational) information systems in the business network?
Logic layer (3)	7. Who (in the network?) decide(s) on the logic applied in the blockchain?
	8. Who may read or write in the blockchain and which control mechanisms are applied?
	9. Which consensus and contract logic is used?

Note that changes in the logic layer may affect the information layer (e.g., which data are shared and stored in the ledger) and the physical layer (e.g., how many organizations will participate; how many transactions will take place).

Parties can trust another, based on reputation or previous contacts (*party or person-based trust*). In modern society, trust relations have often been replaced by formal controls, embedded in institutions (Zucker, 1986). That suggests a category of *institution-based trust*, partly based on reputation and partly based on control mechanisms. We can also trust technology (*technology-based trust*), in the sense that we rely on a mechanism to behave as expected (Vermaas et al., 2010). This depends on a mental model of how the mechanism is supposed to work, and some trust in the party offering the technology, to properly install and maintain it.

Consider the example of a coffee vending machine: we trust the machine to provide coffee when we insert a coin, and not to explode. Is that real trust or merely a metaphor? Upon analysis, it seems that *technology trust* is based on understanding how a system works and on the strength of the prediction of the machine behavior. Note that usually, technology trust also involves party trust and institutional trust. The coffee machine's vendor is trusted to have properly installed and maintained the machine. We may even base our trust on a regulator, to oversee safety of all coffee machines. So even for such a simple case, there is a governance model, involving actors with various roles. By itself, technology cannot be trusted.

In the context of strategic alliances between firms, and in the context of e-commerce, trust has been explored extensively (Das and Teng, 2001; Gefen, 2002; Tan and Thoen, 2002; Perks and Halliday, 2003; Pavlou and Gefen, 2004). Crucial is that e-commerce platforms (like Blockchain applications described above) may enhance trust by adding control mechanisms to the functionality of their platforms, such as an Escrow service, or a reputation rating mechanism. These mechanisms are added to the design of a system to increase trust in other users and reduce possible risks through technological means. Pavlou and Gefen (2004) have shown that in the case of online platforms, trust can be partly based on control mechanisms, such as reputation rating, escrow services, and reviews. Moreover, in the case of e-commerce control mechanisms like reputation rating or reviews, the effectiveness of the (technology based) control mechanism depends on a community of fellow users. The application facilitates and makes use of a social system that provides meaning to it. In a sense, such mechanisms exhibit what has been called socio-materiality: the "social and material aspects of the technology are constitutively entangled" (Orlikowski, 2010). We expect the same to be true for Blockchain applications: effectiveness of a "*stateful shared state*" to generate trust will crucially depend on how the community will accept Blockchain guarantees.

In a series of papers Tan and Thoen explore the notion of *transaction trust*, defined as: "the mental state of the trustor that determines whether he has sufficient trust *to engage in a transaction*" (Tan and Thoen, 2000a,b, 2002). They define transaction trust as the combination of party-based trust and control-based trust. These trust types are defined as follows:

- Party based trust is the belief that the other party (that can be a person or an institution) will behave as expected. This definition fits the definitions above for person based and institution-based trust.
- Control based trust is the belief that the procedures and protocols that monitor and control the successful performance of a transaction, will function properly. Control-based trust also includes the belief that transaction details remain transparent and can be checked. This definition fits the above definition of technology-based trust.

Following decision theory, Tan and Thoen add that the ultimate decision to engage in a transaction for the trustor, depends on a trade-off between "potential gains" of the transaction, and the "transaction risks." The way the trade-off is made, depends on the "transaction trust" as outlined above, but also on the actor's "attitude toward risk" (risk averse, risk seeking). The transaction trust model is depicted in **Figure 3**.

Relations Between Blockchain Applications and Trust

We now use the trust model in **Figure 3** to explore the relations between a Blockchain application (as defined in section Blockchain Applications) and trust (section Trust). Following the definitions of trust, a Blockchain application may affect the decision to engage in a transaction and enter a blockchain based network in four ways:

1. The actor believes the *institution(s)* offering the blockchain based platform to have properly implemented the blockchain, and for each transaction, to faithfully represent the agreement on the blockchain (party-based trust).
2. The actor *believes* the blockchain based network can be *monitored*, and subsequently, that the Blockchain application helps to *reduce* transaction risks (control-based trust).
3. The actor sees *potential gains* because of the Blockchain application in the business network. More potential gains enhance engaging in business network transactions.
4. The actor sees *transaction risks* in the original business network, and believes that a Blockchain application may reduce those risks, through Blockchain based controls.

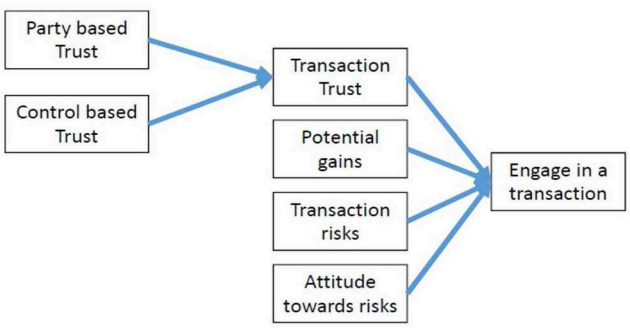

FIGURE 3 | Factors influencing the degree of transaction trust and the decision of an actor to engage in a transaction (adapted from Tan and Thoen, 2000a,b, 2002).

The fifth factor, the actor's *risk attitude* is usually seen as a stable characteristic, and is not likely to be affected by the availability of a Blockchain application.

METHOD

We aim to explore the relations between the design of an artifact, trust in the artifact, and the impact of both design and trust on use of the artifact in a business network. Our research focuses on two related questions, as shown in **Figure 1.** (A) How do the trust requirements in particular application domain influence the design of Blockchain Applications? (B) How does the design of a Blockchain Applications influence the types of trust and trust levels found? Case based research is an appropriate research strategy when it is difficult to separate a phenomenon (blockchain technology effects) from its context (business collaboration, networks, trust, and innovation) (Yin, 2003). In addition, we use observations in case studies to try and develop theory (Eisenhardt, 1989). Specifically, we are interested in design theory for building the artifact (question A), but also in behavioral theory about effectiveness (question B) (Hevner and Chatterjee, 2010).

Cases From Public Sources

As with all emerging technologies, real and mature applications of Blockchain technology are rare. Many organizations have started initiatives to explore the possibilities of Blockchain technologies, but there are few cases in which blockchain is actually deployed in business networks. We have chosen to start by studying publicly known cases, using material from websites, press releases and other public sources, such as news items and technology blogs.

Naturally, this will lead to a bias in the selection of cases. Not many cases of actual implementations of blockchain technologies are known, and even less that have successfully developed in beyond a pilot stage. Moreover, those applications that have been published are likely to be successful ones, or ones that want to be transparent. In addition, there can be bias in the case material itself, because self-published statements are often meant to present a positive image of a project or initiative. Nevertheless, even with this bias toward successful cases and a positive message, the cases provide insight in the aims and choices of a Blockchain application, as we do not use the cases to evaluate success factors, but to search for relations between Blockchain application and trust.

Case Selection

We investigate relations between Blockchain applications and trust in a particular application domain: the diamond industry. We select the diamond industry because trust mechanisms are crucial in this domain. The primary case is Everledger. Everledger offers a Blockchain application focusing on ensuring trust in the *provenance* of diamonds. The term provenance originates from the art and antiques world. It describes means to "relate the value of an object to its origin." The term provenance is also used as a technical term for tracing sources of data in scientific research, and is common in the Semantic Web community where it refers

to the meta-data needed for tracing origin, sources and reliability of data (Simmhan et al., 2004; Janowicz et al., 2015). Observe that the value of objects such as antiques or diamonds depends on the provenance of these objects, the quality and type, the previous owner, and whether the object was lawfully acquired. Such properties can be validated and recorded by Blockchain technology. This characteristic appears to be generic: what is crucial for Everledger, is likely to be crucial for other application scenarios that involve trading objects of value.

When analyzing the Everledger Blockchain in 2018, we found two competing Blockchain initiatives in the same industry: Tracr and Richline. We have included these alternative cases in the analysis, because the three Blockchains provide similar services, but have made different design choices, and induce different types of trust.

We collected the data for all three cases from public sources by doing desk and web research in 2018. We used the official websites[2], as well as additional sources (papers, reports) and blogs. Using the snowball method, we collected 13 documents (65 pages in total) covering the three cases and the diamond industry. We used 18 pages on the diamond industry in general, 17 pages on Tracr, 13 pages on Everledger, and 17 pages on Richline. From these documents, we collected and cross-checked (triangulation) the statements on trust, Blockchain design, and business objectives.

In terms of the research problem (**Figure 1**) we study relationship (A) between requirements for trust in a domain and design choices in Blockchain applications. In the document analysis, these requirements follow from the demands and characteristics of the industry, in this case the diamond industry, and from the type of problem to be solved, in this case trust in provenance of valuable objects. The specific design choices may depend on the context and dependencies of the individual companies and surrounding business networks involved. We also study relationship (B) between the design choices, and the actual types and levels of trust found. This relationship depends on the specific Blockchain application design. As we use public sources, relationships A and B can only be explored to formulate propositions or hypotheses. In depth analysis and hypotheses testing is not possible on the basis of such sources, and needs additional research.

RELATIONS BETWEEN TRUST AND BLOCKCHAIN IN THE DIAMOND INDUSTRY

We present the cases by first describing the industry, including an overview of the key players and business processes. Then we analyze the Blockchain application by using the nine questions (**Table 1**). Subsequently, we explore the relations between the Blockchain application and trust, using **Figure 3** and section Relations Between Blockchain Applications and Trust.

[2]https://www.everledger.io, https://www.tracr.com, https://richlinegroup.com

The Diamond Industry

The diamond industry consists of many small and some large organizations distributed across the supply network illustrated in **Figure 4**. The diamond supply network covers the following five main activities, ranging from mining rough diamonds to selling polished diamonds:

- Mining: Diamond mining takes place in Russia (28% of the total production in 2017), Canada (15%), Botswana (15%), Congo (13%), Australia (11%), and some 20 other countries. Miners sell the rough diamonds to wholesalers. In 2017, 150 million carats of rough diamonds (which equals about 30.000 kilo) were mined for a total value of 15 billion US$.
- Sorting: Wholesalers buy, clean and sort the rough diamonds into "industrial (low) quality" and "gem (high) quality" stones. After that the gem-quality stones are classified in thousands of categories based on size, shape, quality, and color. Wholesalers assign a value to each gem stone. These data are attached to a certificate (under the Kimberly Process Certification Scheme; see below).
- Cutting and polishing: In this phase, the rough diamonds are split and processed into polished diamonds by highly specialized diamond cutting centers (in for instance Amsterdam, Johannesburg, and New York). Polished diamonds are then ready to be sold as gems or to be mounted in jewelry. Diamond cutting centers again classify each diamond, but now on the "four Cs" of the diamond piece: Cut, Color, Clarity, and Carat.
- Diamond Exchanges: Diamonds are sold via registered diamond exchanges. Worldwide, there are about such 25 bourses, all registered by the World Federation of Diamond Bourses (WFDB), which is again supervised by the World Diamond Council (WDC).
- Jewelry Manufacturing and Retail: Jewelers and jewelry manufactures sell the diamonds to end consumers. The total sales value of polished diamonds is about 50 billion US$ per year (www.diamondfacts.org, 2017).

Important actors in the industry are the supervisory authorities KPCS, WFDB, and several large firms. De Beers Group is a large international corporation specialized in diamond exploration, diamond mining, diamond retail, diamond trading as well as in industrial diamond manufacturing (www.debeers.com). Over 70% of the diamond industry is controlled by De Beers via production and purchase agreements with most of the diamond producing countries (Gottlieb, 2006). De Beers provides about one-third of the global supply of diamonds by value (www.tracr.com). Other manufacturers include Alrosa (Bates, 2018) and Diacore, Diarough, KgK group, Rosey Blue, Venus Jewel (Reuters, May 10, 2018).

Two Key Issues in the Diamond Industry

Two key issues in the diamond industry are (i) avoiding trade of so called "conflict diamonds" and (ii) providing trust in provenance ("assuring the origin") of valuable and polished diamonds.

The first issue relates to the trade in rough diamonds. This trade is strictly regulated under the supervision of the

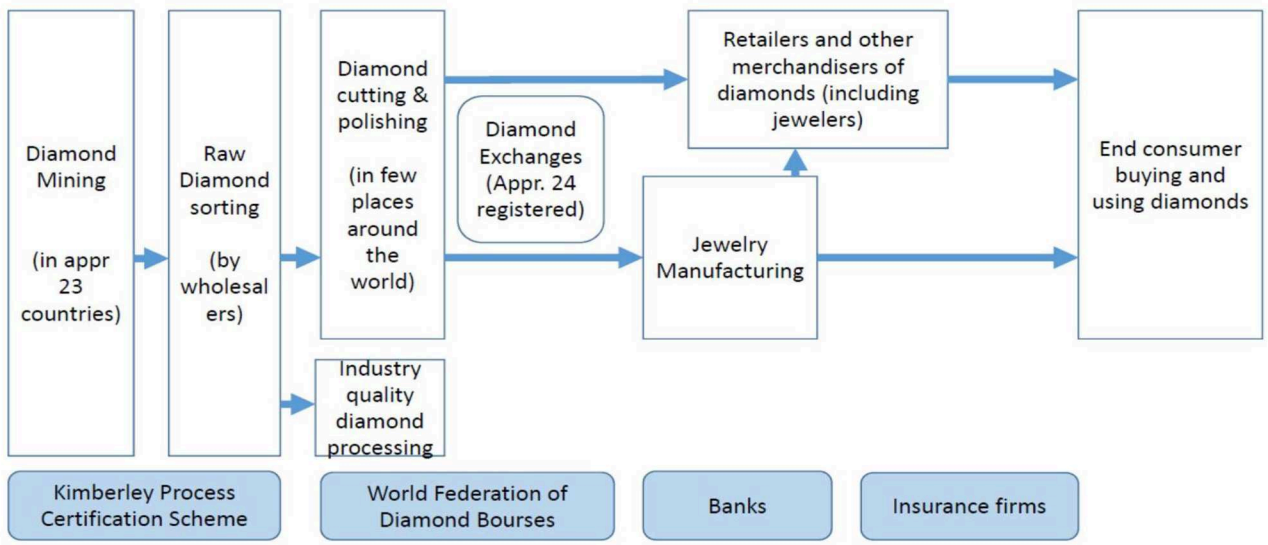

FIGURE 4 | The diamond supply network, including the key actors.

Kimberley Process Certification Scheme (KPCS), which aims to fully eliminate "conflict diamonds." Conflict diamonds are "rough diamonds used by rebel movements … to finance conflict aimed at undermining government." KPCS relies on the financial contributions of participants, supported by industry and civil society observers. The Kimberley Process is, strictly speaking, not an international organization: it has no permanent offices or permanent staff. Neither can the Kimberley Process be considered as an international agreement from a legal perspective, as it is implemented through the national legislations of its participants (www.kimberleyprocess/com; November 2018). KP participants are the states and regional economic integration organizations that are eligible to trade in rough diamonds. As of November 2013, there are 54 KP participants representing 81 countries (including the EU, counting as one participant). KP participants include all major rough diamond producing, exporting, and importing countries. The diamond industry, through the World Diamond Council, and civil society groups are also part of the Kimberley process. These organizations have been involved since the start of KPCS and continue to contribute to its growth and monitoring. As much as 81 governments have enshrined the KPCS into national law. For example, the US adopted the Clean Diamond Trade Act in 2003 (Executive Order 13312). The act requires that all diamonds imported to and exported from the United States have a certificate of origin, according to the Kimberley process, adopted by the UN. In 2018, 99.8% of the world's diamonds are said to come from conflict-free sources. Governments, NGOs and the UN continue to strengthen the Kimberley Process and its system of warranties (www.kimberleyprocess/com; November 2018).

To execute and enforce the KPCS, *rough diamonds receive a unique serial number* that makes it possible to store essential data about a diamond and link the data to the KP certificate. Strong physical control measures exist in the mining and testing process to ensure that data stored for each diamond (type, cut, color, weight, origin, quality) corresponds with the real diamond. In all subsequent processing, the system ensures that the data and the actual diamond remain aligned. For instance, diamonds may be packaged in tamper-proof containers, sealed with an identification code. After that, the transaction history is traced, making it possible to establish legal ownership. In 2017, 70.000 KPCS certificates were issued for a total production of 150 million carat, implying that one KPCS certificate includes -on average- 2.000 carats (about 0.4 kilo) of rough diamonds (if all rough diamonds are certified).

The second issue relates to provenance of polished diamonds. Diamond supply chains are complex and fragmented, resulting in a lack of transparency and trust amongst stakeholders, despite KPCS certificates. The lack of trust, the high value of the assets, and the need to prove that diamonds are legitimately obtained, mean that actors continuously need to *prove provenance of diamonds*. Provenance refers to "the place of origin or earliest known history of something." As stated above, the term originates in the art world, where it means "a record of ownership of a work of art or an antique, used as a guide to authenticity or quality" (online dictionary). The analogy is clear. Buyers of antiques or diamonds usually do not have the expertise to recognize authenticity and quality of the object; they have to rely on evidence from experts. For example, if a retailer wants to sell a valuable diamond, proof is needed on who has cut and polished the diamond and where the original raw diamond came from. Currently, this proof (as far as it exists) is based on linking the KPCS certificate to data provided by the Diamond Exchanges and other actors in the network. However, as the supply network is fragmented, and there are no standards for packaging, identifying or tracing diamonds, it remains hard to establish a full trace

of origin. This explains the huge difference in value between certified and non-certified diamonds.

Three Blockchain Applications to Enhance Trust

In 2018, at least three Blockchain applications aim to solve the issues above: the blockchain applications of Everledger, Tracr, and Richline, a USA based jewelry producer and retailer. We compare the Everledger, Tracr, and Richline blockchain applications and the relation with trust.

Everledger is a rapidly growing business and IT service provider, based in London, and founded in April 2015 (www.everledger.io). In 2018, Everledger had 70 employees across 6 countries. In March 2018, Everledger raised 10 million US$ to expand its global business. Everledger presents itself as an "independent, emerging technology-based enterprise focused on addressing real-world challenges through breakthrough solutions [. . .] to industries where transparency, trust and provenance matter most." This phrase confirms a focus on generation of trust as the main purpose, and a focus on provenance and real-world problems and solutions.

The core issue that Everledger claims to address is "provenance of valuable objects." In 2018, Everledger offers services in six business domains: diamonds, gemstones, minerals, wines, luxury goods, and art (www.everledger.io). Everledger provides services via six different platforms: each domain has its own designed blockchain-based services. To design and provide the services, Everledger collaborates with local experts in mining countries or wine growing areas, or with art experts and artists in the art world. The value proposition of Everledger is based on combining traditional domain knowledge and modern technologies to record, trace and certify transactions and to store evidence on immutable general ledgers. Everledger claims that the Everledger Blockchain application has created an ecosystem of trust within the diamond industry by means of digital provenance tracking and certification.

Everledger makes use of the *IBM Blockchain Platform*, also called *Hyperledger*, for building its blockchain application[3] Everledger is a permissioned system: it is open only for a community of users, who are known in advance and are therefore identifiable and traceable. Nevertheless, the Blockchain application is distributed, avoiding a single point of failure and increasing transparency. The consensus protocol is specifically used to ensure immutability and non-repudiation of transaction records. How validation is done in practice, is not disclosed. Everledger uses expertise of its local partners (as a single authority), in establishing authenticity of a diamond or other valuables. After that, tracking and tracing of the transactions can be done by a regular distributed ledger, i.e., without centralized authority.

Summarizing, the Everledger Blockchain application aims to ensure the following properties:

- *Identification and authentication of diamonds*: diamonds are identified and authenticated, based on a unique number, description of type and origin, and evidence like photographs.
- *Identification and authentication of KPCS certificates*: certificates are uniquely identifiable and traceable, and linked to the diamonds they are about. These properties, if recognized in the market, make it hard to sell two separate diamonds under the same certificate. Note the similarity to the double-spending problem, for which blockchain was originally designed.
- *Data integrity*: no manipulation or deletion of records, after initial recording.
- *Non-repudiation*: once recorded, it is impossible to deny a transaction in which a specific diamond occurs. These two properties makes it possible to trace ownership in a reliable way. If enough traders demand verification of ownership before a transaction, this will make it harder to sell stolen diamonds.

Figure 5 illustrates how the Everledger blockchain application provides services (A–G) to the various actors involved. Note that the Everledger application (like all multi-sided platforms and electronic markets) needs to design and develop customized interfaces and services for each actor type. For instance, service A enables mining experts to add and check information on a certain set of raw diamonds. Service G allows regulators like KPCS to add KP certificates to raw diamonds. Note that Everledger aims to convince each actor (group) to use the platform by offering a specific value proposition for that group, based on customized interfaces.

Tracr is another Blockchain application in the diamond industry. Tracr was conceived by De Beers in 2017 as a mine-to-customer traceability solution. In a pilot project in 2018, Tracr reports that it has identified and tracked 200 diamonds from rough diamond until sales. Tracr claims to have solved the key problem "to determine the characteristics that uniquely identify a rough diamond," "to determine the characteristics that uniquely identify a polished diamond," and "to match the polished with the rough piece" (Bates, 2018).

Tracr is dominated by the mining side of the supply network (actors to the left). Given the large market share of De Beers, it is likely that involvement of De Beers will help to reach a critical mass for diamond certificates. On the other hand, De Beers also represents the "vested interests" in the industry. Blockchain initiatives like Everledger compete with reputation-based trust in provenance. It could be possible that the initiative was started in order not to lose market share.

Richline is a US based company specialized in manufacturing, distribution, marketing and retail of jewelry and luxury goods. The company was founded in 1982 and is based in Florida (USA). Richline has a strong position in lab-grown diamonds. These artificial diamonds are claimed to be chemically, physically, and optically identical to mined diamonds. Diamonds from a lab are guaranteed to be conflict-free and naturally comply with the Kimberley process. In 2018, Richline started a blockchain application, called TrustChain, to ensure provenance of diamonds used in rings and other jewelry (https://www.

[3]https://www.ibm.com/blogs/think/2018/05/everledger/

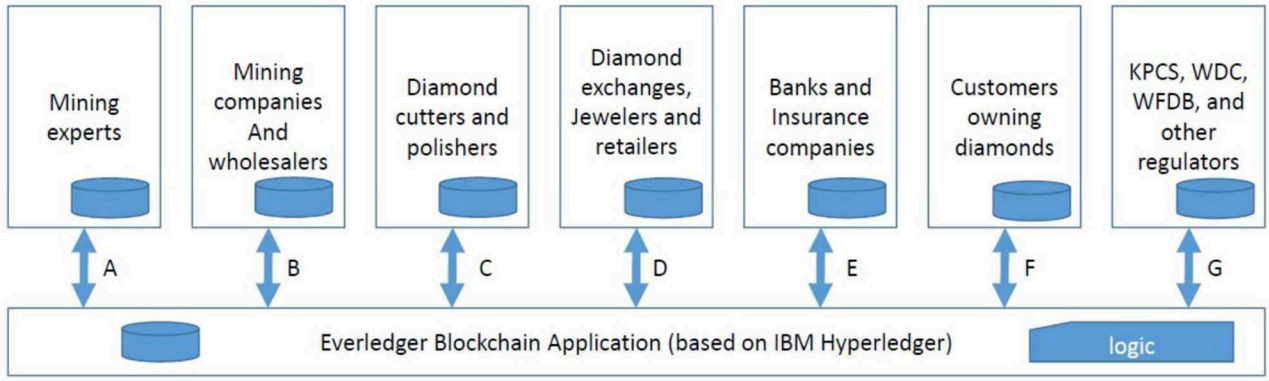

FIGURE 5 | Overview of the Everledger Blockchain application in the diamond industry.

trustchainjewelry.com). The aim is to track and trace diamonds and precious metals from mining (or growing) through to refining, polishing, manufacturing, and delivery. Trustchain is a collaboration between IBM (technology provider), Richline (jewelry manufacturing and distribution), Rio Tinto (diamond supplier for the proof-of-concept), Leach Garner (precious metals supplier), Asahi Refinery (precious metal refinery), and Helzberg (US jewelry retailer). Together these actors cover the entire supply chain. In 2018, they are in the development phase, with the purpose of establishing a proof-of-concept. After that, a full trial will be held with a wider set of industry parties (expected 2019; no further details).

Comparing the Three Blockchain Applications

Before analyzing relations between trust and Blockchain design, we first compare and analyze the designs of the three Blockchain initiatives in the diamond industry using the nine questions on the three application layers in **Table 1**.

The Physical Layer

1. *Which firm started the blockchain application and seeded the first block?* The three cases have different initiators: Everledger is initiated by a London based newcomer in the industry. By contrast, Tracr is initiated by a large, well-known worldwide producer and retailer in the industry (De Beers), and Richline is initiated by a large retailer in the USA, and also a trader in artificial diamonds, who will benefit from increased demand for diamonds with known origin. All three initiatives are in the start-up phase. Developments in party-based trust (does the industry accept the actors?) and control-based trust (does the application provide the right services?) will determine further growth of the initiatives.
2. *Is the blockchain application provided by an existing actor in the network or by a new entrant (cyber-, dis-intermediation, or re-intermediation)?* The Everledger application is an example of a new technology-based intermediary entering the industry. All three initiatives are in principle examples of cyber-mediation: an IT-based intermediary is taking a position in the diamond supply chain. Ultimately, the cybermediary may take over the position of (some) diamond bourses or exchanges, or may lead to bankruptcies of testing agencies (disintermediation). It is also possible that Tracr and Richline involve window-dressing of incumbents in order to retain or regain market share (re-intermediation).
3. *Which other firms participate in the blockchain application?* All three initiatives are in the start-up phase and only a limited number of actors participate in 2018. Note that Everledger provides an infrastructure that allows other actors to enter into the industry, in particular insurance companies ("providing insurance services to diamond owners") and banks ("providing financial services to diamond owners"). This move may be a potential disruptor since banks and insurance providers may require strict certification of diamonds, thereby potentially reducing the power of incumbent firms like De Beers.
4. *Is the blockchain application closed (private blockchain) or open to other firms (public or hybrid blockchain)?* All three blockchain applications are permissioned, but are open to known actors in the diamond industry and also to "all customers that own diamonds" and some to "providers of banking or insurance services." All Blockchain applications require participants to be identified and authenticated. No anonymous users are allowed.

The Information Layer

5. *Which transaction data are stored on the Blockchain, and which data are not?* The initiatives cover data on rough as well as polished diamonds and aim to provide provenance proof by tracking origin, type, quality, and ownership. The material we studied does not provide details on the exact data elements stored in the distributed ledgers. The data architecture of the applications and the uptake of standards for identification and authentication, and representation formats for crucial properties, will affect the further development of services, thereby influencing the potential gains and transaction risks for actors to engage in the blockchain application.

6. *How is the Blockchain application linked to other (internal and inter-organizational) information systems in the business network?* All three applications provide interfaces to information systems maintained by the various actors in the industry (e.g., for recording KP certificates), suggesting functionalities for linking the blockchain application to (some) internal systems. No information is provided on, for instance, the automatic or manual linking process to KP certificates.

The Logic Layer

7. *Who (in the network?) decide(s) on the logic applied in the blockchain?* The initiators of the three applications decide on the logic. The logic is embedded in the application services for different stakeholders (A–G in **Figure 5**), but is based on common properties (physical provenance, identification and authentication, traceability, integrity, non-repudiation). Transparency of the logic, and impact of this transparency on control- based trust remain unclear. Some actors must remain secret (as indicated by De Beers) and therefore the logic must allow for partial disclosures. Successful development of each initiative will depend on how the initiator (focal actor of the network), handles this sensitive issue and how this development will affect party based and control-based trust.
8. *Who may read or write on the Blockchain and which control mechanisms are applied?* The Blockchain access control logic in each initiative determines who exactly will be permitted to enter, and which data may be read or written by which actors. Details on identification and authentication of actors are not provided. Also, no details are provided on how the Blockchain validators verify the certification of the physical diamond mining processes.
9. *Which consensus and which contract logic is used?* It is likely, that all three initiatives work with a validator consensus logic, although the records themselves are distributed. The differences between Tracr and Everledger, illustrate how different perspectives of the focal actors are influencing the decision rights embedded in the blockchain logic. Everledger appears to be a cooperative, whereas Tracr has a clear dominant player. The development of decision rights will further influence the actors' perception of gains and risks, and the subsequent decision to engage in the network.

We now use the observations in the three cases to analyze relations between trust and the design of the Blockchain applications.

Analyzing Relations Between Trust Requirements and Blockchain Applications

Using the trust definitions of **Figure 3**, we analyze (A) the influence of trust requirements on Blockchain application design, and (B) the influence of Blockchain application design on trust. We present our findings in **Table 2** where columns one to three illustrate six observations (A1–A6) on relation A and four observations (B1–B4) on relation B. Our observations in the three cases provide support for the impact of four trust requirements (T1–T4) on six Blockchain design aspects (BC1–BC6). We identify 15 examples (1–15 in the right column) of the impact of (four) Blockchain design choices on trust, gains and risks.

Our observations in the three cases and **Table 1** lead to the following propositions. Specifically, observations A1–A6 appear to support P1, and observations B1–B4 appear to support P2. This provides reason for these propositions to be further developed and tested in additional research.

P1: Trust requirements influence the design choices for the physical, information and logic layers of the Blockchain application.

P2: Blockchain design properties influence party based trust, control based trust, expected gains, and expected risks of using the Blockchain application.

Our observations in the three cases were only made in 2018, which is the year that the three initiatives started offering their services in the diamond industry. More follow-up research is needed to evaluate the combined impact of design choices and trust on Blockchain application and business network success.

DISCUSSION AND CONCLUSIONS

The aim of this paper was to explore the relations between trust and the design of Blockchain applications. We first defined a *Blockchain application* as an application of Blockchain technology in a sociotechnical setting, also known as a business network. To analyze the design of a Blockchain application, we use the three layer model (**Figure 2**) consisting of the (i) physical layer specifying the firms and logistics in the business network, (ii) the information layer specifying the data architecture of transactions and shared ledgers, and (iii) the logic layer specifying four types of logic (communication, content, consensus, and contract logic). Second, we define *trust* using an (adapted) model of Tan and Thoen, which analyzes transaction trust in terms of party-based trust, control-based trust, potential gains, transaction risks, and risk attitude.

We analyzed three Blockchain applications in the diamond industry. The diamond industry is characterized by assets, whose value depends on ensured provenance. This need for provenance is strengthened by regulatory compliance (Kimberly Certification Process). Hence, trust mechanisms are crucial in this domain. The three Blockchain applications differ in their design choices on each of the three layers. In the physical layer, we observe different numbers and types of actors who participate in the Blockchain applications; in the information layer, we observe different types of data shared; in the logic layer, we find different types of business logic.

One key question is about how trust requirements in a business setting affect the design of a Blockchain application. In the three cases we find six examples of the impact of trust requirements on design. The other key question is about the effect of Blockchain application design on types and levels of trust. In the three cases we find 15 examples of the impact of design on party trust, control trust, expected gains, and risk. We formulate two propositions to be developed in future research.

We conclude from our observations that trust requirements do indeed influence the design of a Blockchain application and also, vice versa, that the design of a Blockchain application

TABLE 2 | Six observations (A1–A6) on how trust requirements affect Blockchain application design and four observations (B1–B4) on how application design affects trust.

Trust requirements	A	Blockchain application design	B	Party trust/control trust/gains/risks
T1. Needs to track provenance of valuable goods	A1	BC1. Link IDs to rough and polished diamonds (identification and authentication in the logic layer)	B1	1. Belief in mechanisms for identification and authentication of rough and polished diamonds (control trust) 2. Belief in mining and cutting experts from Everledger partners, De Beers or Richline participants to execute these mechanisms (party trust) 3. Expected gains: reduced costs of testing downstream 4. Expected risks: increased dependency on limited number of certifiers for trading
	A2	BC2. Identification of pieces (in physical, information, and logic layer)		
	A3	BC3. Single source of truth on origin, quality, and ownership of objects (shared data in the information layer)	B2	5. Belief in mechanisms for tracking and tracing objects (control trust) 6. Belief in blockchain immutable records of ownership (control trust) 7. Belief in Blockchain platform providers to execute these mechanisms properly (party trust) 8. Expected gains: increased certainty of origin, quality and ownership, reduced costs of insurance 9. Expected risks: increased dependency on limited number of certifiers for trading
T2. Needs for valid data entry; and compliance with audit criteria (KPCS)	A4	BC4. Permissioned blockchain with validation protocol in the logic layer	B3	10. Belief in mechanisms for data entry and KPCS compliance (control-based trust) 11. Belief in Blockchain platform providers to execute these mechanisms properly (party-based trust) 12. Expected gains: reduced transaction risks, reduced compliance risks 13. Expected risks: increased bureaucracy and administrative burden
T3. User needs to control their data	A5	BC5. Contract logic and communication logic		
T4. User needs to check with other users	A6	BC6 Ability to tell and share stories using the Blockchain application (information and logic layer)	B4	14. Platform based belief in Blockchain data and provenance of the diamonds (party trust) 15. Expected risks: reduced risks because of shared risks and protection by the community

influences the trust induced. These vice versa relations suggest dynamic interactions between application design choices and trust over time (**Figure 1**). For example, if a new-comer offers a Blockchain application in a network, the design may enhance trust for those organizations that decide to start using the application. After some time, those trust levels may have become "de facto" mandatory for all actors in the network. This may trigger other actors, such as incumbents, to formulate different or stronger (trust) requirements that will force the original new-comer to adjust the information, physical, or logic-layers of the design. If the subsequent design is taken on, and effective, this will again lead to changes in trust and perceptions of trustworthiness.

The possibility of such a trust dynamic shows that the current discourse of Blockchain replacing trust by means of technology, is too simplistic. At best it will replace some forms of trust by other forms of trust. In particular, party trust in traditional institutions is replaced in technology-based control trust combined with some residual party trust, namely in those parties who execute the control mechanisms.

These dynamic relations between trust, Blockchain application design, and further business developments make it hard to predict which Blockchain application design will be most commonly adopted. Prediction is even more difficult when multiple Blockchain applications are competing for dominance. We advise to follow the developments of the three Blockchain applications in the diamond industry to evaluate interactions between trust, design, and adoption.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: www.jckonline.com/editorial-article/tracr-de-beers-blockchain-platform/, footnote 2 in other web sources see article.

AUTHOR CONTRIBUTIONS

MS and JH made substantial contributions to the conception and design of the work, revising the work critically, approved for publication of the content and agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work were appropriately investigated and resolved.

REFERENCES

Bates, R. (2018): *Inside TRacr, the De Beers developed Blockchain platform. In Luxury*. Available online at: www.jckonline.com/editorial-article/tracr-de-beers-blockchain-platform/ (accessed November 2, 2019).

Birch, D., Brown, R., and Parulava, S. (2016). Towards ambient accountability in financial services: shared ledgers, translucent transactions and the technological legacy of the great financial crisis. *J. Payments Strategy Syst.* 10, 118–131.

Brennan, C., and Lunn, W. (2016). *Blockchain: The Trust Disruptor*. Report Credit Suisse.

Clegg, C. W. (2000). Sociotechnical principles for system design. *Appl. Ergono.* 31, 463–477. doi: 10.1016/S0003-6870(00)00009-0

Das, T. K., and Teng, B.-S. (2001). Trust, control and risk in strategic alliances: an integrated framework *Organ. Stud.* 22, 251–283. doi: 10.1177/0170840601222004

de Kruijff, J., and Weigand, H. (2017). "Towards a blockchain ontology," in *Advanced Information Systems Engineering (CAiSE 2017),* eds E. Dubois and K. Pohl (Berlin: Springer), 29–43.

Eisenhardt, K. M. (1989). Building theories from case study research. *Acad. Manage. Rev.* 14, 532–550. doi: 10.5465/amr.1989.4308385

Fagin, R., Halpern, J. Y., Moses, Y., and Vardi, M. (1995). *Reasoning About Knowledge*. Cambridge, MA: MIT Press.

Gambetta, D. G. (1988). "Can we trust?" in *Trust,* ed D. G. Gambetta (New York, NY: Basil Blackwell), 213–237.

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM Sigmis Database* 33, 38–53. doi: 10.1145/569905.569910

Giaglis, G., Klein, S., and O'Keefe, R. M. (2002). The role of intermediaries in electronic marketplaces. *Inform. Syst. J.* 12, 231–246. doi: 10.1046/j.1365-2575.2002.00123.x

Gottlieb, M. S. (2006). *Jewelry Retail: An Industry Study, MSG Accountants, Consultants and Business Valuators.*

Hevner, A., Chatterjee, S. (2010): *Design Research in Information Systems: Theory and Practice*. Berlin: Springer. doi: 10.1007/978-1-4419-5653-8

Janowicz, K., van Harmelen, F., Hendler, J. A., and Hitzler, P. (2015). Why the data train needs semantic rails. *AI Mag.* 36, 5–14. doi: 10.1609/aimag.v36i1.2560

Keen, P. G. W. (ed.). (1999). *Electronic Commerce Relationships: Trust by Design.* Englewood Cliffs, NJ: Prentice-Hall.

Laudon, K. C., and Traver, C. G. (2018). *E-commerce, 13 Edn*. London: Pearson education.

Magazzeni, D., McBurney, P., and Nash, W. (2017). Validation and verification of smart contracts: a research agenda. *Computer* 50, 50–57. doi: 10.1109/MC.2017.3571045

Mayer, R. C., Davis, J. H., and Schoorman, F. D. (1995). An integrative model of organizational trust. *Acad. Manage. Rev.* 20, 709–734. doi: 10.5465/amr.1995.9508080335

Meijer, D., and Ubacht, J. (2018). "The governance of blockchain systems from an institutional perspective, a matter of trust or control?" in *Proceedings of the 19th Annual International Conference on Digital Government Research (DG.O 2018),* eds M. Janssen, S. A. Chun, and V. Weerakkody (Delft: ACM), 90:91–90:99.

Orlikowski, W. J. (2010). The sociomateriality of organisational life: considering technology in management research. *Camb. J. Econo.* 34, 125–141. doi: 10.1093/cje/bep058

Pavlou, P. A., and Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Inform. Syst. Res.* 15, 37–59. doi: 10.1287/isre.1040.0015

Perks, H., and Halliday, S. V. (2003). Sources, signs and signalling for fast trust creation in organisational relationships. *Eur. Manage. J.* 21, 338–350. doi: 10.1016/S0263-2373(03)00049-5

Simmhan, Y. L., Plale, B., and Gannon, D. (2004). A survey of data provenance in e-science. *ACM Sigmod* 34, 31–36. doi: 10.1145/1084805.1084812

Smits, M. T., Weigand, H., and Kruijff, J. D. (2020). "How blockchain technology affects performance of financial services," in *Digital Transformation*, eds B. van Gils and E. Proper (Berlin: Springer Verlag).

Swan, M. (2015). *Blockchain: Blue Print for a New Economy*. Boston, MA: O' Reilly

Tan, Y.-H., and Thoen, W. (2000a). An outline of a trust model for electronic commerce. *Appl. Artifi. Intell.* 14, 849–862. doi: 10.1080/08839510050127588

Tan, Y.-H., and Thoen, W. (2000b). Towards a generic model of trust for electronic commerce. *Int. J. Electro. Commer.* 5, 61–74. doi: 10.1080/10864415.2000.11044201

Tan, Y.-H., and Thoen, W. (2002). Formal aspects of a generic model of trust for electronic commerce. *Decis. Sup. Syst.* 33, 233–246. doi: 10.1016/S0167-9236(02)00014-3

Van Heck, E., and Vervest, P. H. M. (2007). Smart business networks: how the network wins. *Commun. ACM* 50, 28–37. doi: 10.1145/1247001.1247002

Vermaas, P. E., Tan, Y.-H., van den Hoven, J., Burgemeestre, B., and Hulstijn, J. (2010). Designing for trust: a case of value-sensitive design. *Knowl. Technol. Policy* 23, 491–505. doi: 10.1007/s12130-010-9130-8

Wright, A., and De Filippi, P. (2015). Decentralized blockchain technology and the rise of Lex Cryptographia. *SSRN*. doi: 10.2139/ssrn.2580664

Yin, R. K. (2003). *Case Study Research: Design and Methods*. Newbury, CA: Sage Publications

Zucker, L. G. (1986). "Production of trust: institutional sources of economic structure, 1840-1920," in *Research in Organizational Behavior,* eds B. M. Staw and L. Cummings (Greenwich: JAI Press), 53–111.

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.