CHALMERS
UNIVERSITY OF TECHNOLOGY

TRUST, PRIVACY AND TRANSPARENCY WITH BLOCK- CHAIN

TRUST, PRIVACY AND TRANSPARENCY WITH BLOCK-CHAIN TECHNOLOGY IN LOGISTICS

Research full-length paper

Track - Blockchain Applications: Issues, Challenges and Opportunities

Akram, Asif, Chalmers University of Technology, Gothenburg, Sweden
asif.akram@chalmers.se

Bross, Philipp, T-Systems International GmbH, Leinfelden-Echterdingen, Germany
philipp.bross@t-systems.com

Abstract

Since the introduction of blockchain over a decade ago, many industries and industrial sectors are exploring the potentials of the technology. In line with the trend, logistics sector is not an exception and is investigation various dynamics associated with the implementation of the technology. This study focuses on the linking between the capabilities of blockchain technology and trust, privacy and transparency. In order to explore dynamics of the linkage, the study used case study as a method for the inquiry. These have been common issues in logistics which the existing information solutions are unable in resolving to a greater extent.. The results shows that blockchain technology has the capability to build trust among unknown industry players while maintaining a sufficient level of privacy and transparency at the same time. Overall, the study presents useful insights by contributing to the major issues in logistics and supply chain when an innovative digital technology is put into action.

Keywords: Blockchain, Logistics, Trust, Privacy, Transparency, Dynamics

1 Introduction

Digital innovations changing the businesses horizons has been a well-established phenomenon over the last decade. Within these changing business horizons, the roles of organizations, relationships and other dynamics have all been transformed into evolving networks of interactions (Akram, 2016). In the recent digital era, blockchain technology is considered to be a revolutionary digital innovation having the potential of changing business landscapes. A decade ago blockchain was introduced within financial sector (i.e. technology underpinning bitcoin), and since then both researchers and practitioners are exploring ways to implement the technology in various sectors and industries. Banking sector (Crosby et al., 2016), social networks (Iansiti and Lakhani, 2017), shipping industry (Loklindt et al., 2018), supply chains (Baruffaldi and Sternberg, 2018) are examples of industries and sectors where blockchain is being implemented or explored to be implemented. However, the scope of the application of the technology is not limited to businesses, rather various public and social services such as land registration, energy saving, education, and free-speech right (Zheng et al., 2016), the management of intellectual property rights, sharing economy and enterprise collaboration (Tapscott and Tapscott, 2016) are using blockchain to address respective sectors' issues.

In its essence, blockchain is a distributed database where transactions' records are stored, shared among independent stakeholders using unique identifiers, and updated upon agreement of all stakeholders based on consensus protocol (Crosby et al., 2016, Avital et al., 2016). Traditionally, blockchains used in bitcoin consist of mutually mistrusting stakeholders to carry out financial transactions without the involvement of trusted third parties (i.e. banks). In return of transactions between mistrusting third parties,

blockchain offers transparent and integrity protected data storage (Nakamoto, 2008). Some of the unique characteristics of blockchain include decentralization, security and data integrity (Yli-Huumo et al., 2016). Other characteristics include public verifiability, transparency, privacy, redundancy, and trust anchor. Blockchains are divided into two categories as: permission-less blockchains and permissioned blockchains. In a permission-less blockchain, any peer can participate and leave the network as reader or writer at any time. In this category of blockchains, privacy of the information is ensured through cryptographic techniques. Bitcoin and Ethereum are two examples of permission-less blockchain (Sasson et al., 2014). On the contrary, permissioned blockchains involves a central entity who makes decision and give the rights to access to a limited set of readers and writers. Hyperledger Fabric and R3 Corda are two examples of permissioned blockchains (Brown et al., 2016).

Like other areas, researchers have shown an increasing interest in exploring the potentials of blockchain in supply chain management and logistics (Liang et al., 2016, Korpela et al., 2017). Since the deliveries in logistics are made on regular basis and multiple stakeholders are involved in the process where each using its separate operational data with little or no interest in sharing information – this makes the process opaque or non-transparent as well as asynchronous information (if shared) exist among stakeholders. Furthermore, reliance on a trusted third-party to carry out transactions pose another hurdle (Swan, 2015). The existing infrastructure of information systems within logistics are not designed for evolutionary technologies like blockchain resulting in organizational and technical adjustments. Therefore, the issues of ensuring trust, privacy and transparency at the same time are dominant within logistics sector. These industrial issues calls for some sort of revolutionary technologies that can address such issues in a more transparent manner without compromising privacy of the information. In this attempt, researchers have identified the blockchain technology as an enabler for digital supply chain integration (e.g. (Korpela et al., 2017)). Other researchers have attempted to explore various issues that lead to trust, privacy and transparency. For example, blockchain was used as a ledger to record complete ownership details of physical asset leading to transparency (Peters et al., 2015). Furthermore, devising an environment without traditional trust can impact business processes integration (Weber et al., 2016) as well as operational and business performances (Flynn et al., 2010). In addition to these, smart contracts can be used to ensure data security, in general, and confidence in data quality, in particular (Huckle et al., 2016). However, the blockchain adoption in logistics has been underrepresented in the recent literature, and therefore this study aims to contribute to the IS literature of Blockchain technology in logistics. Based on the aim of the study, we propose the following research question:

How can the capabilities of blockchain capabilities meet the needs of privacy, transparency and trust in logistics in order to improve the flow of information and goods? Driven by the research question, the purpose of this study is to explore the potentials and dynamics of the Blockchain technology for the logistics sector. In particular, the study will retain its focus around the capabilities of Blockchain technology in relation to the concepts of transparency, privacy and trust.

In the next section, review of literature is presented regarding blockchain technology as well as on the intermingling of privacy, trust and privacy in logistics. This section is followed by description of case study as a research methodology including data collection and analysis strategies. Then, results from the analysis of empirical material is presented. Finally, discussion on theoretical contribution followed by concluding remarks and future work concludes the study.

2 Blockchain Technology

Blockchain technology is commonly described as a public ledger, which stores information about all transactions made within a peer-to-peer network (Beck and Müller-Bloch, 2017, Kosba et al., 2016, Swanson, 2015, Pilkington, 2016). The term Blockchain already implies that blocks are linked together in some way. But what is a block in a Blockchain and how are blocks linked with each other? First, a block in a Blockchain contains information. This information can be categorized in metadata and in content. The content is usually information about a transaction. Metadata is stored in the header and

contains a hash value, which is calculated based on the content of the block and a reference to the previous created block (Pilkington, 2016). The reference to the previous block is the calculated hash value of the previous block (Crosby et al., 2016, Beck et al., 2016). This reference to the previous block and only to the previous block makes it a chain of blocks.

A fundamental concept of Blockchain technology is the consensus mechanism, which tackles the challenge to reach consensus about the correctness of transactions (Milutinovic et al., 2016, Crosby et al., 2016). The correctness of transactions is verified using cryptographic algorithms (Yli-Huumo et al., 2016, Pilkington, 2016). Due to the nature of a distributed system it is necessary to determine the order of the Blocks that are to be added to the Blockchain, this is also part of the consensus finding (Crosby et al., 2016). Blockchain technology emerged as the backbone of the Bitcoin network and the stated problems were solved with a consensus mechanism called "proof-of-work" (Nakamoto, 2008). It is called proof-of-work because a token in the form of hash code is generated by solving a mathematical problem to make sure that the creation of a Block required a certain amount of work (Becker et al., 2013, Crosby et al., 2016). This process is highly ineffective and relies on computational power, which is expensive and, in the end, wasted resources (Yli-Huumo et al., 2016). However, the reason why Blockchain technology is often referred to as tamper-proof lies in the consensus mechanism as well. If one would attempt to change or remove a block, the hash values of all Blocks that were created since needed to be calculated. This is nearly impossible by today's standards due to limitations of computational power (Nakamoto, 2008, Swanson, 2015).

Due to the mentioned drawbacks, alternative methods to reach consensus are being researched. Proof-of-Stake is a consensus mechanism without reliance on computational power (Bentov et al., 2016, King and Nadal, 2012). The power of decision making is distributed across stakeholders of the system and blocks the creation of new blocks is based on a deterministic approach, based on the stake of the users (Bentov et al., 2016, King and Nadal, 2012, Pilkington, 2016).

This approach leads to faster transactions and less energy consumption (Buterin, 2014). A potential attacker would have to hold a huge stake of the network but if the network is under attack the value of the stack decreases, which makes an attack less likely (Xu et al., 2016).

2.1 Transactions and Scalability

Transaction in the context of Blockchain technology as a distributed and decentralized database is a mix of two different concepts. First, it refers to a database transaction. Second it refers to a transaction record of data, such as money, goods, property or even votes (Beck and Müller-Bloch, 2017). Therefore, a transaction in a Blockchain is an entry of information into the distributed and decentralized database as content of a block.

The initial intention when the Blockchain was developed as the backbone of Bitcoin was the transaction of digital currency and the consensus mechanisms were developed for the sole purpose of monetary transactions. This has implications because the throughput is a major issue within the Bitcoin network and only a maximum throughput of 7 transactions per second (tps) (Nakamoto, 2008).

As comparison, the number of transaction that VISA handles is around 4000 tps/s (Beck et al., 2016, Yli-Huumo et al., 2016). The consensus mechanism proof-of-work also comes with high energy costs and according to Croman et al., (2016) that it costs between $1.4 and $6.9 to confirm a transaction on the Bitcoin network if the costs for hardware to carry out the proof-of-work, energy costs, storage and bandwidth are considered. As approach to reduce costs is the developing of alternatives to the commonly used consensus mechanism proof-of-work (Croman et al., 2016).

2.2 Smart contracts

Nick Szabo already introduced the concept of smart contracts in 1994 as *"a computerized transaction protocol that executes the terms of a contract"* ((Szabo, 1994), p.1). In other words, smart contracts translate clauses of a contract into code and embed them into either hardware or software (Szabo, 1997).

Blockchain technology is regarded as the first technology to make the implementation of smart contracts possible (Wright and De Filippi, 2015). A smart contract is embedded into a Blockchain and possesses a unique address (Christidis and Devetsikiotis, 2016, Luu et al., 2016). Based on the clauses of the respective contract, a transaction is triggered and sent to the defined address where the contract is executed. The Ethereum Blockchain is an open-source project and mainly designed for smart contracts (Wood, 2014). Furthermore, smart contracts are identified by Korpela et al. (2017) as similar to letters of credit in logistics operations. This makes it an interesting to automatically process single and multi-tranche transactions (Korpela et al., 2017).

2.3 Privacy, transparency and trust

Trust, privacy and transparency are concepts found in the research streams of Blockchain technology (Beck et al., 2016, Kosba et al., 2016, Lemieux, 2016) and logistics (Faltings et al., 2008, Léauté and Faltings, 2011, Klein and Rai, 2009).

Privacy, or more precise information privacy is defined as the control over one's personal information and the use of such information by others without one's consent (Bélanger and Crossler, 2011).

The definition of transparency is more ambiguous. A wider definition is provided by Ball (2009), who describes *"transparency as a public value embraced by society to counter corruption, transparency synonymous with open decision-making by governments and non-profits, and transparency as a complex tool of good governance in programs, policies, organisations, and nations."* (Ball, 2009, p. 293) The definition from Do Prado Leite and Cappelli (2010) that describes transparency from an IS angel regarding the disclosure of information (do Prado Leite and Cappelli, 2010).

Privacy and transparency in the context of Blockchain technology are intertwined because the basic idea behind Blockchain is an open one, where transactions are anonymous and visible to everyone. However, Blockchains are not open per-se and a distinction can be made between private and public Blockchains. In the literature the terms 'permissioned' and 'permissionless' are used as well (Pilkington, 2016, Lewis, 2015, Xu et al., 2016). In a public Blockchain there are no restrictions regarding participants in the network and all transactions are identifiable by their public hash value, which is used to validate the transaction (Christidis and Devetsikiotis, 2016). A private Blockchain on the other hand, involves the monitoring of read and write permissions as well to restrict the access to the network (Pilkington, 2016). Implications of the different approaches are that private Blockchains can not reach the same level of decentralisation as public Blockchains. Due to the described system of user rights management in private Blockchain, the degree of transparency can be controlled as users are known and not anonymous. The users and their transactions of public Blockchain remain anonymous and transactions visible (Xu et al., 2016). The degree of privacy and transparency in a Blockchain depend on the kind of Blockchain that is used as illustrated in Figure 1 below:

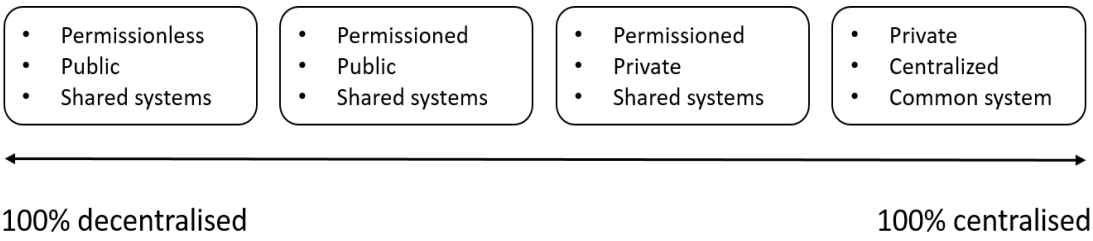

Figure 1. Degree of centralisation adapted from(Walport, 2016)

Logistics providers face the dilemma of which information they are willing to share when coordinating their operations with partners to keep costs low (Léauté and Faltings, 2011). Blockchain is regarded as

a potential technology to improve overarching communication between organisations but the lack of transactional privacy is an open issue (Kosba et al., 2016, Zhang et al., 2016). The balance between privacy and transparency in logistics processes in combination with the use of Blockchain technology has not been studied previously.

Blockchain technology is referred to as a technology that enables a "trust-free" economy based on a highly secure and transparent design (Becker et al., 2013, Beck et al., 2016). Trust in an organisational context is defined by Mayer, Davis & Schoorman (1995) 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. 751). This implicates the reliance on a third party that acts as a trustworthy instance. This instance ensures that records are secure of unauthorized access and altering. Without existing physical and geographical boundaries in digital context this is most crucial. Instances that act as third parties in today's economies are for example banks or civil registries that record births, deaths, marriages or land registrations (Lemieux, 2016). The approach to create trust with Blockchain technology is to assume that all participants are mutually untrusted, and trust is created by the consensus mechanism of the Blockchain (Milutinovic et al., 2016, Zyskind and Nathan, 2015). The potential of Blockchain technology to establish trust is recognized but the reliance of this way to establish trust between organisations needs further investigation (Lemieux, 2016).

In an earlier study, Klein and Rai (2009) examined trust in logistics and supply chain relationships in relation to strategic information sharing. They found out that there are financial benefits in the sharing of strategic information, but the opposite party must be trusted (Klein and Rai, 2009). If Blockchain technology provides the capabilities to create trust between the participants of a logistics process without the need of a trusted instance has not been part of previous studies.

3 Research Methodology

In order to explore the dynamics of blockchain adoption in terms of trust, privacy and transparency, this study used case study methodology. Case study is a preferred research method where: (i) "how" or "why" research questions; (ii) little control over events by the researcher; and (iii) focus is on contemporary phenomenon in real-life context (Yin, 2017). The case study methodology is commonly used within IS field, and have the ability to test, generate and develop theory about a real context phenomenon of interest. The description of the case is presented in the following paragraphs:

ABenterprise (Pseudonym) was first established in 1880s as a mechanical and electronic appliances manufacturer. The company operates in 150 countries and employ around 390,000 people. Within the innovation department of the company, blockchain technology has gained special attention and support from top management as the technology is viewed as a promising area for solving current logistic problems. This was set up in the form of a project called 'Block & Log'. The project is carried out between three departments of ABenterprise (called herein as AB 1, 2, 3), a logistic company (LogA) which specialises in time critical deliveries and an IT company (ITC) providing infrastructure and consultancy services. Th participant from ABenterprise include project manager from AB1, a product manager for IoT devices from AB2, and a business manager responsible for logistics innovation from AB3. The participants from LogA include business manager and the IT director.

Overall aim of the Block & Log project was to develop use cases to apply blockchain as a data source in combination with Internet of Things (IoT) devices within logistics. These IoT devices are manufactured by ABenterprise and were capable of measuring and recording various parameters including temperature, humidity, tilt and shock. The state of shipped goods were visualized via a mobile app. In this way, the project was pilot test to explore the capabilities when IoT devices are combined with blockchain technology in logistics. LogA transport time critical deliveries to overseas ABenterprise plants regularly. Their main purpose was to improve the tracking of shipped goods and to improve the information flow between them. One of main routes between Germany and China was chosen for this project. The shipped

goods are equipped with IoT devices to collect data about the goods and track their geographical locations. The blockchain platform and necessary infrastructure provided by an external service provider was based on a Hyperledger – an open-source implementation of distributed ledger framework. The platform served as the backbone for IoT devices and information flow among participants; and to implement smart contract for automating transactions between the participants.

3.1 Data Collection

During the case study, various kinds of data has been collected including semi-structured interviews, documents and meetings. The following Table 1 provides the summary of data collection activities:

Type	Activity (with numbers)	Participants
Semi-structured Interview	Aimed at gathering information about logistics industry & processes, IS in logistics, blockchain, privacy, trust and transparency of logistics and blockchain (9)	AB2 product manager; AB, LogA, &external business managers; LogA IT director; ICT IT manager, External researcher, blockchain consultant & GTD commercial manager
Documents	Summary of customer interviews (37); meeting notes (5); technical documentation (2); project presentation slides (3)	ABenterprise; Project partners
Meetings	Regular internal project meetings (10); meetings with project partner (5)	Includes ABenterprise, AB1 project manager & department; Project partners

Table 1. Summary of data collection

Semi-structured interviews were chosen as data collection since they provide the freedom to explore interesting aspects during the inquiry (Myers and Newman, 2007). In this project, the value of blockchain was obtained during the process of engagement in conversations to obtain in-depth understandings. In general, these interviews were designed with dual purposes: On the one hand, to obtain information about existing information systems used in logistics, and concept of privacy, transparency and trust as identified in the literature. On the other hand, the interviews explored the capabilities of blockchain within logistics. These interviews were conducted with top management as well as with the experts from the field to ask about their personal experiences regarding blockchain in logistics. These interviewee participants include product managers, business managers, IT manager, IT director, and researcher both internal to ABenterprise as well as externals. Furthermore, during the interviews both retrospective (i.e. what is) and prospective (i.e. what might be) reflections were used (Schultze and Avital, 2011). For each of the interview, suggestions by Schultze and Avital (2011) on conducting a semi-structured interview were used. In total, 9 interviews were conducted with various interviewees at different positions (see Table 1). Last but not the least, each of the interviews were recorded for transcriptions at the later stage.

Although interviews are considered as a rich source of information, many researchers (e.g. (Schultze and Avital, 2011, McNamara, 1999) suggest to couple them with other sources. Following the advice of these researchers, *documents* were used as another source of information. Different kinds of documents used in this study include protocols of previously conducted customers' interviews, meeting notes, technical documentation of infrastructure and project presentations on the Block & Log project. In total, 47 documents have been selected in this study.

In addition to semi-structured interviews and documents, *meetings* (15 in total), were also used as the part of data collection activities. Two kinds of meetings served the purpose in this regard: meetings with

project partners and internal project meetings. While the meetings with project partners were conducted on-demand, the internal project meetings were conducted on regular intervals. During the meetings, notes were taken for further analysis of data as described in the next stage.

3.2 Data Analysis

The collected data from semi-structured interviews, documents and meetings were analysed using thematic analysis. In general terms, a thematic analysis is used to identify, analyse and report different themes within data in situations where detailed theoretical and technical knowledge of approaches is limited (Braun et al., 2012). This is in rhyme with the blockchain in logistics – an area where a little research has been done. The analysis was conducted in six phases as: (i) familiarizing yourself with data – data transcription, reading and re-reading of data, notation of initial ideas; (ii) Generating initial codes – systematic coding of interesting feature of the data across the data set, collection and combination of data relevant to each code; (iii) searching for themes – translation of codes into potential themes and gathering data around those themes; (iv) review of themes – reviewing is done on two levels – level 1 is about reviewing the assigned codes and level 2 reviewing is related to entire data set and generation of thematic map; (v) defining and naming themes – includes refining different aspects for each theme with clear definitions and naming; and (vi) producing the report – involves finalizing the analysis such as final selection and analysis of codes, referring to the research question and literature, and generating a report. The following Table 2 shows these stages were implemented:

Stages	Description
Familiarizing with data	Transcribing and translating the interviews, reading of documents and meeting notes; re-reading the whole data set; illustrating initial thoughts in the comments
Generating initial codes	Assigning IDs to data each of the data sources; highlighting importance sentences and keywords; assigning codes to the highlighted text using spreadsheets; codes include both words and phrases
Searching for themes	Structuring the codes based on similarities resulting in 9 columns; each column was restricted to maximum 10 entries; initial thematic map was drawn from these structured information
Reviewing themes	Reviewing related to codes; comparing codes with the whole dataset; a second round of review was conducted with focus on guiding concepts of privacy, transparency and trust; a third-round of review was conducted to simplify the complexity of thematic map
Defining and naming themes	Clear definition of themes and naming was conducted based on second iteration of thematic map and emerged codes; outcome with final iteration of thematic map illustrating the linkage between privacy, transparency and trust with blockchain
Producing the report	Description of each identified theme was presented

Table 2. Summary of data analysis strategy

4 Finding

The analysis of the data echoed number of problems with existing information systems being used in logistics. First, the systems were described as outdated having the legacy of traditional standalone software from 90s. Although, external systems, that is, system for customers are a bit more advance, internal organizational systems are still quite old. This raised problem associated with compatibility, dependency on legacy hardware, and integration with recent technologies like telematics and IoT. Like many other interviewees, this has been expressed by product manager at AB2 in these words:

"They were developed in a time before the internet was invented".

The compatibility issue is further drowned by the use of different kinds of information systems, even reaching up to 15 in case of big companies. Last but not the least, management attitude towards IT investment is quite low as the industry is driven by cost, resulting in ending up with lagging behind and failure of IT-based projects. Furthermore, the general notion of *"it always worked in the past"* combined with the lack of skills and IT expertise added to the failure. Therefore, we can say that privacy or protection of intellectual property, organization overarching information exchange, and provenance of goods are the core requirements that various information systems (IS) fail to address.

In general, the analysis of the data collected reflects that blockchain technology can improve the logistics processes along the whole supply chain by serving as an information exchange platform. The improvement of processes also do not require heavy infrastructure investment by a single organization due the distributed nature of blockchain technology. This is because the distributed resources are still owned by different stakeholders in the supply chain resulting in sharing the overall cost of the infrastructure. In this way, blockchain connects various components of the existing infrastructure. The analysis of various data sources also shows that logistic companies have high concerns regarding the privacy of intellectual property. This is, however, countered by increasing demand on transparency from the customers and trust on the technology. A description of each of these concepts is presented in the following sub-sections.

4.1 Privacy

The analysis of data shows that the feedback on privacy in logistics has been the most uniform among all three. That is, the control over an information is decisive factor for providing efficient solutions and competition in the market, eventually. Almost all of the interviewees were in favour protecting the privacy of information within their respective domains. For example, LogA business manager showed his concerns about protecting data about products, value of products and the customers. This has been expressed as:

"The requests from the customers to have transparency about the transport processes is followed by operators within the industry."

Similarly, *LogA IT Director* was in favour of protecting the privacy of partners against the transparency request by the customers. He put forward his concerns in these words:

"Information about partners must be protected and transparency in that regard is absolutely not wanted".

Furthermore, the *GTD commercial manager* was in favour of privacy about logistics operations. He expressed his viewpoint as:

"Companies are so reliant on their supply chains that they don't want others to know how they do things".

The only disagreement related to privacy was reflected in the level of privacy and varies from one stakeholder to another one. For instance, the insurance of privacy is less important for an *inbound logistics manager* than a *transport logistics manager*.

Like traditional logistics business, privacy has been described as a major concern. This has been emphasized by the *Blockchain consultant* in terms of data security since the data over a public blockchain is prone to attacks. The analysis highlight that since the entries (of data) are irreversible and unchangeable, a thorough investigation should be made before publishing data. Moreover, smart contracts should be treated in the same way.

Logistics operators value the protection of intellectual property and the control over information to a great degree. It is seen as a crucial competitive advantage to manage the flow of information for larger companies. The analysis showed that the use of a public Blockchain is not appropriate for logistics operations. With the concept of private Blockchains the privacy requirements can be met due to

permission and user management. It was further identified that a hybrid approach of public and private Blockchains in combination is promising. This allows disclosing certain information to the public but keep others within the boundaries of the company. Privacy can be maintained but also provide transparency where it is necessary.

4.2 Transparency

The analysis of data collected during the interviewees with experts shows more diverse opinions about the transparency. In this regard, the degree of transparency plays an important role in the formation diverse opinions and is influenced by number of dependencies.

First, a distinction between time-critical or special transport and standard transport is necessary. Standard transport is characterized by low-profit margin with minimum requirements on transparency. This has been expressed by AB3 logistics manager as:

"…. I promised a specific delivery time but leave me alone during this period".

Further analysis probe into the reason behind lack of transparency is an attitude or unwillingness to be transparent about a logistic process, itself. This may include cost-optimization and replacement of damaged goods by transport service providers during transportation.

Second, the organization of a transport company influence the dependency on transparency. This has been expressed by product manager at AB2 as such:

"High level of transparency is expected in cases where a transport company is established under the umbrella of a manufacturing company".

On the contrary, the analysis of data reflected that the opaqueness of private data sharing increases with the involvement of third-party (according to *LogA & ABenterprise representatives*).

For some companies, the level of expected transparency is quite high due the demand of transparent transport from customers, according to *commercial manager at GTD*. However, privacy and transparency are not necessarily contesting (as is traditionally considered) as long as a certain degree of both can be maintained. Here, comes the role of blockchain technology where privacy can be ensured via anonymity of a blockchain and non-personal parts of private data can be released to ensure transparency, simultaneously. This has been explicitly mentioned by an external researcher as:

"The one means that it is publicly traceable and other one means that I have my private space".

The exchange of information over organisations' boundaries was identified as a core requirement in the analysis. There are several reasons why this is an important requirement for logistics operators. Standards in the industry are non-existing or not followed due to legacy systems with technical limitations and the wide range of different systems used. The outcomes are unclear processes and manual effort for all involved parties to route information. For customers the non-transparent processes are a problem but the analysis also revealed that logistics operators do not want their customers to know how they work in many cases. However, internally they have the desire to make their processes transparent. The privacy concerns described in the previous section correlate with the requirements regarding transparency. Blockchain technology provides the capabilities to create a certain level of transparency by enabling the organisation overarching exchange of information.

4.3 Trust

Like transparency, the analysis of data exhibit two levels of trust: trust in the ability to handle the transport itself; and trust in information exchange among partners in a supply chain and logistics. However, irrespective of the levels, the trust is very critical factor in case of high-value or time-critical transports. But achieving trust in not an easy task, as mentioned by LogA business manager:

"It is a bit harder in our segment to acquire new customers, new business because a lot depends on positive experiences and trust".

Furthermore, trust is not of that importance when sharing transport information with partners, but it becomes an important factor for sharing any kind of information other than regular transport one (IT Director LogA). The analysis also prescribed some solutions for building trust in logistics as illustrated by GTD commercial manager:

"Look at the no. of companies and the amount of value tied up in those companies, who exist to acta as trusted third party to supply chains and it's the preference of the market that they need to be there".

However, this traditional way of trust is time consuming and requires a lot of value in terms of efforts, incentives and so on. Blockchain here plays a crucial role as its logic is based on transactions between non-trusted partners. A statement by blockchain consultant support this point as:

"We don't have trust any longer because we have transparency".

Enabling trust has been identified as one of key concerns among the practitioners. The analysis of data suggested two distinct ways of enabling trust with the help of blockchain technology. For example, according to one of the Blockchain consultants:

"Trust can be enabled by smart contracts"

Enabling trust through smart contract implies a security or guarantee about the availability of funds. These smart contracts ensure (through implementing escrow function) that the business partner own the funds required for the transaction. However, smart contracts are not the only means of enabling trust. The ICT IT Architect pointed out another way of enabling trust as:

"Trust can be enabled through the publication of hash values of transactions. These hash values are reviewed and verified by all participants in a blockchain."

Within logistics, trust is normally associated with the provenance of goods (as shown in Table 3 below). This provenance of goods and trust association has two meanings. On one hand, it is the desire of customers to know about the origin of products. On other hand, it describes the tracing of goods throughout a supply chain from end to end. The association to trust is made in order to know the origin of a product. This knowing of goods origin helps to create trust between a company and their customers. When it comes to Blockchain technology, the customers do not establish traditional way of building trust, that is, trust on any organisation. This is due to the fact that the matter of trust is shifted towards the Blockchain technology who acts as an enabler for trust. Here, smart contracts act as an enabler for compliance matters to follow laws and regulation based on technology as well.

The detailed findings about themes and their relevant concerns about privacy, transparency and trust in relation to blockchain capabilities have been presented in the Table 3 below:

Requirements in IS	Capabilities of Blockchain Technology		
	Privacy	Transparency	Trust
Protection of intellectual property	User roles and permissions in private blockchains		
Organizing overarching systems to access information		Allows sharing and distribution of authentic information across multiple organizations	
Digital document transfer between organizations	Documents are not directly saved in a Blockchain but pointers to other databases should be used	Hash value of data is stored in a blockchain	
Integration of customs systems		Smart contract to follow regulations and call APIs of third party systems	

Control over data	Stack like approach of private and public blockchains		
Ensure data security		Data is distributed to all nodes, which means once the data is out, it can't be reverted	
Transparency towards customers to provide proof of provenance		Publications in a public Blockchain as a proof to the public	
Ability to trace goods through the whole supply chain		Allows sharing and distribution of authentic information to multiple organizations	Storage for transactions that can't be altered. This ensures correctness

Table 3: Summary of IS Requirements in logistics and Capabilities of Blockchain Technology

In short, blockchain technology blockchain technology can improve the flow of information by facilitating organisation overarching information exchange systems. This system, in turn, resolve the requirements associated with privacy, transparency and trust by allowing only fewer disruptions in the flow of information in logistics. The thematic map below summarizes the outcome of the analysis of the empirical data. The core requirements of Information systems in logistics and the core capabilities of Blockchain technology are brought in relation based on the identified themes and the concepts of privacy, transparency and trust. This overall reflection can be summarized in Figure 2 below.

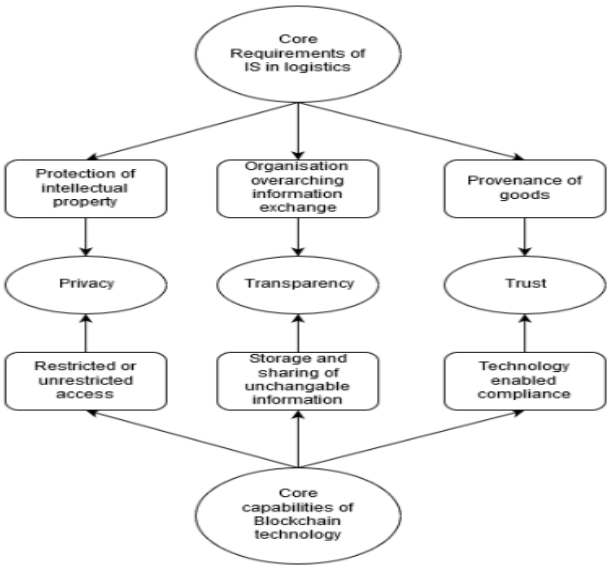

Figure 2. An overview of privacy, trust and transparency with blockchain

5 Discussion

This study aimed to explore the implementation of blockchain in logistics where privacy, transparency and trust have been identified among key concerns in the field. Based on the results from case study in Block & Log project, the links of privacy, transparency and trust with Blockchain in logistics have been presented in the result section. These results have number of implications for research as well as for practice and will be described in the following part of this section. In line with many other explorative

research, this study has been explorative in nature because of the limited amount of work related to blockchain in logistics.

First, traditional conceptualization regarding privacy and transparency argue for contradictory view. That is, privacy will be compromised at the cost of providing transparency and vice versa. However, the result in this study reflects that privacy and transparency are not essentially contradictory and a certain degree of privacy can be preserved while providing transparency to a greater extent, at the same time. But, maintaining such balance is not an easy task and come up with number of challenges. Along this line, this study reports an instance of such challenges. The challenge points out the complexity in the decision making about the level of transparency - that is, making the whole information or a part of it as public while protecting another information or part of the same information is a matter of great concern for the organizations. Nevertheless, this solution has implication for ensuring data security and abiding of existing regulations, on one hand, and protection of intellectual property, on the other hand.

Second, blockchains inherently exhibit a lack of transactional privacy (Kosba et al., 2016, Croman et al., 2016). This inherent lack of transactional privacy associated with blockchain technology is also reflected within logistics sector. Therefore, the findings in this study suggest that researchers should sustain the importance of transactional privacy within logistics, especially related to the information about networking with other stakeholders in the industry. This study also probed into the solution of transactional privacy. This inherent problem, to a greater extent, can be addressed by the use of private blockchains and permissioned approaches which involve recording data in the form of hash values. In this way, using additional control and access restrictions to specific group, private blockchains can still maintain transactional privacy.

Third, establishing trust between unknown parties has been identified as one the major potentials of blockchain technology (e.g. (Milutinovic et al., 2016, Zyskind and Nathan, 2015, Lemieux, 2016)). This study deviates a little bit in case of trust within logistics, that is, a trusted third party is still preferred by key players. However, the case may not hold true for all the stakeholders in logistics. For example, this study shows that the elimination of trusted third party can be valuable for some players such as logistic providers. In that case, trust can be enabled using transparency as well as using smart contract which enables compliance through blockchain technology. Furthermore, this study attest to earlier findings of trust in terms of information sharing (Klein and Rai, 2009) by illustrating that stakeholders in logistics prefer control over their private data, at least.

Finally, this study affirm that blockchain technology has great potentials for improving the flow of information between stakeholders, resulting in improvement of overall logistics operations. In this regard, sole proprietors and SMEs can play a vital role.

The implementation of Blockchain technology in logistics has not been fully explored yet. Therefore, exploring the use cases in various parts of supply chain and theorizing is, rightfully, the next step ahead which this study attempted to achieve. It is evident that a dominant logic of the logistics industry needs is hindering successful implementation of Blockchain technology for a number of organizations. Therefore, the existing dominant-logic within logistics needs to be re-addressed due to the fact that blockchain is not owned or controlled by a single entity or an organization. This, in turn, results for a change related to attitude of sharing information not only with other stakeholders but with customers, as well. The attitude also calls for more IT or technology based investments in order to create value from Blockchain technology. Furthermore, publishing sensitive and private data in public blockchain can lead to serious legal consequences for organizations especially after the introduction of GDPR. Additionally, stakeholder organizations need to think in terms of open-source strategies since the technology is built on this approach, especially when it comes to intellectual property rights. Last but not the least, Blockchain technology can be a catalyst for much-needed digitalization and digital innovation in logistics.

6 Concluding Remarks

The research on Blockchain technology, in general, is a highly relevant within information systems field. This study provides insights on privacy, transparency and trust from a single case study which has its limitations in terms of generalizability. Therefore, more case studies or other studies can help to generalize the results found in this study. However, the results provides useful insights regarding the better understanding of implementing blockchain in logistics and address some of the major concerns. Moreover, the study has been conducted within one organization in Germany. Moreover, various organizations have their own contexts and organizational cultures. Similarly, different countries have their own geographic and social dimensions. Therefore, future research, can probe the phenomenon in different organizational and geographic contexts. Finally, supply chain integration can further be explored for different sizes of organizations, that is, especially in cases where SMEs and sole proprietors can be part of blockchain based solution.

References

Akram, A. 2016. *Value Network Transformation–Digital Service Innovation in the Vehicle Industry*.

Avital, M., Beck, R., King, J., Rossi, M. & Teigland, R. 2016. Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future.

Baruffaldi, G. & Sternberg, H. 2018. Chains in Chains-Logic and Challenges of Blockchains in Supply Chains.

Beck, R., Czepluch, J. S., Lollike, N. & Malone, S. Blockchain-the Gateway to Trust-Free Cryptographic Transactions. ECIS, 2016. ResearchPaper153.

Beck, R. & Müller-Bloch, C. 2017. Blockchain as radical innovation: a framework for engaging with distributed ledgers as incumbent organization.

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. P. & Böhme, R. 2013. Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. *The Economics of Information Security and Privacy.* Springer.

Bélanger, F. & Crossler, R. E. 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly,* 35**,** 1017-1042.

Bentov, I., Gabizon, A. & Mizrahi, A. Cryptocurrencies without proof of work. International Conference on Financial Cryptography and Data Security, 2016. Springer, 142-157.

Braun, V., Clarke, V. & Terry, G. 2012. Thematic analysis. *APA handbook of research methods in psychology,* 2**,** 57-71.

Brown, R. G., Carlyle, J., Grigg, I. & Hearn, M. 2016. Corda: An Introduction. *R3 CEV, August*.

Buterin, V. 2014. Slasher: A punitive proof-of-stake algorithm. *Ethereum Blog URL: https://blog. ethereum. org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm*.

Christidis, K. & Devetsikiotis, M. 2016. Blockchains and smart contracts for the internet of things. *IEEE Access,* 4**,** 2292-2303.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E. & Sirer, E. G. On scaling decentralized blockchains. International Conference on Financial Cryptography and Data Security, 2016. Springer, 106-125.

Crosby, M., Pattanayak, P., Verma, S. & Kalyanaraman, V. 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation,* 2**,** 6-10.

do Prado Leite, J. C. S. & Cappelli, C. 2010. Software transparency. *Business & Information Systems Engineering,* 2**,** 127-139.

Faltings, B., Léauté, T. & Petcu, A. Privacy guarantees through distributed constraint satisfaction. Web Intelligence and Intelligent Agent Technology, 2008. WI-IAT'08. IEEE/WIC/ACM International Conference on, 2008. IEEE, 350-358.

Flynn, B. B., Huo, B. & Zhao, X. 2010. The impact of supply chain integration on performance: A contingency and configuration approach. *Journal of operations management,* 28**,** 58-71.

Huckle, S., Bhattacharya, R., White, M. & Beloff, N. 2016. Internet of things, blockchain and shared economy applications. *Procedia Computer Science,* 98**,** 461-466.

Iansiti, M. & Lakhani, K. R. 2017. The truth about blockchain. *Harvard Business Review,* 95**,** 118-127.

King, S. & Nadal, S. 2012. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August,* 19.

Klein, R. & Rai, A. 2009. Interfirm strategic information flows in logistics supply chain relationships. *Mis quarterly***,** 735-762.

Korpela, K., Hallikas, J. & Dahlberg, T. Digital supply chain transformation toward blockchain integration. proceedings of the 50th Hawaii international conference on system sciences, 2017.

Kosba, A., Miller, A., Shi, E., Wen, Z. & Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. Security and Privacy (SP), 2016 IEEE Symposium on, 2016. IEEE, 839-858.

Léauté, T. & Faltings, B. Coordinating logistics operations with privacy guarantees. IJCAI Proceedings-International Joint Conference on Artificial Intelligence, 2011. 2482.

Lemieux, V. L. 2016. Trusting records: is Blockchain technology the answer? *Records Management Journal,* 26**,** 110-139.

Lewis, A. 2015. A gentle introduction to blockchain technology. *BraveNewCoin, http://bit. ly/2jdE8iz*.

Liang, K.-Y., Van De Hoef, S., Terelius, H., Turri, V., Besselink, B., Mårtensson, J., Johansson, K. H., Reglerteknik, Skolan för elektro- och, s. & Kth 2016. Networked control challenges in collaborative road freight transport. *European Journal of Control,* 30**,** 2-14.

Loklindt, C., Moeller, M.-P. & Kinra, A. How Blockchain Could Be Implemented for Exchanging Documentation in the Shipping Industry. International Conference on Dynamics in Logistics, 2018. Springer, 194-198.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P. & Hobor, A. Making smart contracts smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016. ACM, 254-269.

Mayer, R. C., Davis, J. H. & Schoorman, F. D. 1995. An integrative model of organizational trust. *Academy of management review,* 20**,** 709-734.

McNamara, C. 1999. General guidelines for conducting interviews. Retrieved 13.01. 2017.

Milutinovic, M., He, W., Wu, H. & Kanwal, M. Proof of luck: an efficient blockchain consensus protocol. Proceedings of the 1st Workshop on System Software for Trusted Execution, 2016. ACM, 2.

Myers, M. D. & Newman, M. 2007. The qualitative interview in IS research: Examining the craft. *Information and organization,* 17**,** 2-26.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system.

Peters, G., Panayi, E. & Chapelle, A. 2015. Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective.

Pilkington, M. 2016. 11 Blockchain technology: principles and applications. *Research handbook on digital transformations***,** 225.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. & Virza, M. Zerocash: Decentralized anonymous payments from bitcoin. Security and Privacy (SP), 2014 IEEE Symposium on, 2014. IEEE, 459-474.

Schultze, U. & Avital, M. 2011. Designing interviews to generate rich data for information systems research. *Information and Organization,* 21**,** 1-16.

Swan, M. 2015. *Blockchain: Blueprint for a new economy*, " O'Reilly Media, Inc.".

Swanson, T. 2015. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. *Report, available online, Apr*.

Szabo, N. 1994. Smart contracts. *Unpublished manuscript*.

Szabo, N. 1997. Formalizing and securing relationships on public networks. *First Monday,* 2.

Tapscott, D. & Tapscott, A. 2016. The impact of the blockchain goes beyond financial services. *Harvard Business Review,* 10.

Walport, M. 2016. Distributed ledger technology: Beyond blockchain. *UK Government Office for Science*.

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A. & Mendling, J. Untrusted business process monitoring and execution using blockchain. International Conference on Business Process Management, 2016. Springer, 329-347.

Wood, G. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper,* 151**,** 1-32.

Wright, A. & De Filippi, P. 2015. Decentralized blockchain technology and the rise of lex cryptographia.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B. & Chen, S. The blockchain as a software connector. Software Architecture (WICSA), 2016 13th Working IEEE/IFIP Conference on, 2016. IEEE, 182-191.

Yin, R. K. 2017. *Case study research and applications: Design and methods*, Sage publications.

Yli-Huumo, J., Ko, D., Choi, S., Park, S. & Smolander, K. 2016. Where is current research on blockchain technology?—a systematic review. *PloS one,* 11**,** e0163477.

Zhang, F., Cecchetti, E., Croman, K., Juels, A. & Shi, E. Town crier: An authenticated data feed for smart contracts. Proceedings of the 2016 aCM sIGSAC conference on computer and communications security, 2016. ACM, 270-282.

Zheng, Z., Xie, S., Dai, H.-N. & Wang, H. 2016. Blockchain challenges and opportunities: A survey. *Work Pap.–2016*.

Zyskind, G. & Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. Security and Privacy Workshops (SPW), 2015 IEEE, 2015. IEEE, 180-184.