LU Engineering Logistics

Master Thesis

Spring 2018

Unraveling the hype

A literature review and Delphi study of the potential of public and permission-less blockchains in the supply chain

Petter Mårtensson, Oscar Stenman

Industrial Engineering and Management, Lund University

Supervisor Engineering Logistics: Andreas Norrman

Abstract

Title	Unraveling the hype - A literature review and Delphi study of the potential of public permission-less blockchains in supply chain
Authors	Petter Mårtensson and Oscar Stenman
Supervisor	Andreas Norrman, Professor Engineering Logistics, Faculty of Engineering (LTH) at Lund University
Background	Blockchain technology has during the last years become a hot topic for supply chain management. Solutions are being developed and sold, but exactly what blockchain technology can bring to the supply chain is unclear. The technology can be divided into two main varieties, public and private. The public version sparked the initial interest in the technology but has not been as heavily promoted in a supply chain management context as its private counterpart.
Purpose	The purpose of this thesis is to evaluate the potential of public permission-less blockchain technology to solve supply chain issues.
Research Questions	RQ1: What are supply chain issues that public permission-less blockchain technology can solve? RQ2: How can public permission-less blockchain technology be applied to solve these issues? RQ3: What are challenges for successful implementation and use of public and permission-less blockchain technology in the supply chain?
Method	The thesis is based on a literature review and a Delphi study. Scientific articles and whitepapers describing use cases of public permission-less blockchain were reviewed and the findings from the literature review were used as a foundation for the Delphi study. The Delphi study involved 31 experts divided into three panels, representing experts on supply chain management, blockchain technology and academic experts with knowledge of the two previous fields.
Conclusions	Public and permission-less blockchain technology was found to have potential in solving issues related to paperwork and to increase transparency and traceability of products. Further it can be used to automate transactions and to create marketplaces without trusted middlemen.
Keywords	Public, permission-less, blockchain, supply chain

Acknowledgements

We would first like to thank our supervisor at LTH, Professor Andreas Norrman for valuable and thorough feedback in every stage of our thesis.

We would also like to express our gratitude to Blockchainlab, and especially Simona Macellari, for letting us stay in their office and immerse us in the discussions and current topics of the Bitcoin community in Milan. The company Eternity Wall also proved helpful and we are thankful for all the questions they have answered for us.

Finally we would like to express our profound gratefulness to all the experts who took part in our Delphi study. Without all these people the study would not be possible and we appreciate that so many of them managed to fit our three questionnaires into their tight schedules.

Lund, May 2018

Petter Mårtensson Oscar Stenman

Glossary

Abbreviation	Full name of term
BCT	Blockchain technology
B2B	Business-to-business
C2M	Consumer-to-machine
Dapp	Decentralized application
DLT	Distribute ledger technology
DPoS	Delegated Proof-of-Stake
ICO	Initial coin offering
IQR	Interquartile range
M2M	Machine-to-machine
P2P	Peer-to-peer
PBFT	Practical Byzantine Fault Tolerance
Pub-PL	Public and permission-less (blockchain)
PoW	Proof-of-Work
SCF	Supply Chain Finance
SCM	Supply Chain Management

Blockchain concepts

Atomic swap - Atomic swaps are the exchange of cryptocurrency from two different chains without the need for a trusted third party. It is based on a concept called hash time-locked contracts that ensure that both parties are fulfilling their part of the deal. Additionally it requires certain functions to be implemented on each blockchain involved which currently is just beginning to be used, hence it has not been used in a practical way yet. (Madeira, 2018)

Bitcoin - Bitcoin is a cryptocurrency for sending funds without any third party involved presented in 2008 (Nakamoto, 2008).

Block - A number of transactions (on the Bitcoin blockchain) or other data grouped together (Sikorski et al., 2017).

Blockchain technology - A trust-less distributed data structure storing data in blocks and linking each block to the previous block, using the hash of the previous block (Xu et al., 2017).

Consensus - Since the blockchain and its calculations are distributed some method to reach consensus about results is needed. Two common ways to reach consensus on whether to add blocks to the blockchain or not are Proof-of-Work and Proof-of-Stake. (Sikorski et al., 2017)

Cryptocurrency - A digital currency operating independently of any central bank, which uses cryptography to regulate creation of new units of the currency and to verify the transfer of funds (Sikorski et al., 2017).

Decentralized application - There is no exact definition because of the novelty of the area but it can be said to be an application without any single point of failure, run on many different nodes (Raval, 2016, pp. 3-7).

Distributed ledger - A distributed ledger (DLT) is a shared database that is updated by consensus and records timestamped data with unique cryptographic signatures leading to a secure auditable history of transactions (Swan, 2017).

Delegated Proof-of-Stake - Delegated Proof-of-Stake (DPoS) is a consensus algorithm. The difference between DPoS and Proof-of-Stake (PoS) could be described like that between direct democracy and representative democracy. In DPoS users decide on nodes to vote for them in the consensus process. (Zheng et al., 2017)

Ethereum - Ethereum is a blockchain specifically designed to be a platform for smart contracts (Ethereum Community, 2016).

Hard fork - A hard fork is a change of rules of the blockchain protocol leading to that blocks created according to these new rules will be seen as invalid by validators running the old protocol (Castor, 2017).

Hash - A hash is an output of a hashing function of fixed length based on an input of any size. (Narayanan et al., 2016, pp. 23-24). In blockchains the hash points to the previous block (Zheng et al., 2017).

Hyperledger - The Hyperledger project is an open source initiative to create blockchains for business use and the Linux Foundation launched it in 2016 together with 30 founding corporate members. Currently there are nine different blockchains being developed by the project. The focus is not to have specific chains, which are to be used by the members, but to collaboratively develop code bases and frameworks that can be implemented by those who are interested. (The Linux Foundation, 2018)

Initial coin offering – An initial coin offering (ICO) is similar to an initial public offering in that it is used to raise capital for companies in the blockchain sphere. If the company offers a blockchain service that has a native cryptocurrency it can raise capital through selling this cryptocurrency, where investors hope that the coin will gain value as the service increases in popularity. (Jaffe, 2018)

Interplanetary file system – The interplanetary file system (IPFS) is a distributed file system storing files using techniques similar to the ones used in blockchains, such as hashing. It lets information be stored in the system while securely storing a link to the data on the blockchain. (Protocol Labs, 2018)

Lightning Network - The Lightning Network allows two users to set up a payment channel containing a fixed amount of Bitcoin. The users can then transact using this payment channel. Only the opening and closing of a channel generates a transaction on the Bitcoin blockchain, reducing the amount of transactions on the chain. If user A and user B have opened a channel, and user B and user C have opened a channel, user A can transact with user C through channeling money through both channels. (Torpey, 2017)

Merkle tree - A Merkle tree is a data structure. In its leaf nodes it has data that is hashed, concatenated in pairs and hashed again. The hashes are paired and hashed again which goes on until only one block remains, the root of the Merkle tree. Storing data this way makes it impossible to change the data without changing the Merkle root, effectively making it impossible to change. (Narayanan et al., 2016, pp. 34-37)

Mining - Mining simply means carrying out the consensus algorithm that allows for the creation and addition of new blocks to the blockchain. A node carrying out the mining is called a miner. The exact process varies between chains but basically includes verifying transactions and publishing blocks. See Proof-of-Work and Proof-of-Stake for further details. (Sikorski et al., 2017)

Node - A node is a computer running a blockchain protocol (Morabito, 2017) and holding a copy of the blockchain (Narayanan et al., 2016, p. 54).

Nonce - A nonce is an arbitrary string that can be changed in order to satisfy the rules for adding blocks in Proof-of-Work (Zheng et al., 2017).

Oracle - An oracle provides information from the outside world to the smart contracts on the blockchain (Buck, 2017).

Practical Byzantine Fault Tolerance - Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm. It is not applicable for public permission-less blockchains since every other node has to be known. (Zheng et al., 2017)

Proof-of-Stake – Proof-of-Stake (PoS) is a consensus algorithm that uses ownership of the blockchain's currency as a scarce resource to ensure security and integrity of the blockchain. This is also in limited supply and for an actor to be able to make changes not following the rules of the chain they would need to own more than half of the coins on the chain. (Morabito, 2017, p. 11)

Proof-of-Work – Proof-of-Work (PoW) is a consensus algorithm that uses work as scarce resource. In the case of Bitcoin this means computational power and the proof is in the form of solving a hash puzzle. The nodes compete in solving this puzzle by finding a specific number, the nonce, so that when you concatenate the block header and use the hash function on it, the value of the hash falls within a certain range. (Narayanan et al., 2016, pp. 64-65)

Public/Private-key cryptography – The method by which a public identity is created with an associated private one. In blockchains this is used for creating public addresses for sending currency to and to verify signatures made by the private key. To make a transaction you have to use the private key. (Swan, 2015, pp. 98-99)

Smart contract - A smart contract is a snippet of code on the blockchain, using logical IF/ELSE statements to stipulate conditions. They are executed without any person or middleman involved. Often they are used to transfer funds from one place to another if some criteria are fulfilled. (Morabito, 2017, pp. 101-105)

Soft fork - A soft fork is a change of rules of the blockchain protocol that is backward compatible and makes blocks created according to the new rules valid also according to the old rules (Castor, 2017).

Timestamp - By timestamping a file through the blockchain it is possible to prove that the file existed at a certain point in time. A hash of the file is included in the block as a transaction and when somebody at a later stage want to prove the existence of this file at the time of the block's creation they simply regenerate the hash. (Swan, 2015, pp. 37-38)

Token - Tokens are created through smart contracts and represent an asset on the blockchain (Chen, Forthcoming 2018).

Transaction - Exactly what transactions are differs between blockchains, but generally they are data packages that store parameters. In Bitcoin they record monetary parameters but in other blockchains it can also be results of smart contracts. (La Rosa et al., 2016)

Wallet - A wallet in terms of cryptocurrencies is software that stores public and private keys and interacts with blockchains. It is used for storing, sending and receiving cryptocurrencies (Max, 2017). Tokens can be stored in some wallets as well (Ledger, 2018).

According to our own definitions, see chapter 2.1.1 for further details:

Permission-less blockchain - A blockchain that anyone can read, send transactions to, have their transactions included if valid and anyone can take part of the consensus process to add new blocks.

Permissioned blockchain - A blockchain that only certain parties can read, send transactions to, have their transactions included if valid and anyone can take part of the consensus process to add new blocks. Someone or something has the power to give permission.

Public blockchain - A blockchain that anyone can read.

Private blockchain - A blockchain controlled by someone or something such as a company.

Table of Contents

1. Introduction

This chapter gives a background to the subject matter of this thesis. It introduces blockchain technology and its implementations in supply chain management. It goes on to offer a problem description, stating the need for this study, and presents the purpose and research questions. Finally, it outlines the focus and delimitations of this study.

1.1 Background

The blockchain technology[1] (BCT) has gained fame in recent years as the technology behind cryptocurrencies such as Bitcoin[2]. The Bitcoin blockchain was originally proposed by Satoshi Nakamoto in 2008 (Nakamoto, 2008) and has since been the focus of much attention. This technology has spawned many other more or less similar digital currencies, and currently there are close to 1500 different currencies (CoinMarketCap, 2018).

However, more recently the technology itself has risen to fame. Schatsky and Muraskin (2015) stated already in 2015, in a report written for Deloitte, that millions of dollars in venture capital was flowing into blockchain-related start-ups, that banks were joining consortia for building blockchain solutions, and that blockchain concepts, prototypes and investments were emerging in all major industries. According to Gratzke et al. (2017) the situation has all but calmed down since 2015. More consortia have been started and their focus has broadened from the mostly financial focus of the past. There are now blockchain consortia focused on logistics as well as health care.

Shapira and Leinz (2017) state that there is a great hype surrounding BCT and it is many times used as a buzzword, with unclear connection to actual business, and as a promotion tool. One typical example is the case of the Long Island Ice Tea corporation changing its name to Long Blockchain, and its stock price subsequently rising with as much as 289 %. However, as suggested by Banker (2017) the actual capabilities of the technology remain unclear to many. It is often referred to as an immature technology where actors do not properly explore what value it can create for their business. It is a foundational technology to build applications on but it is currently advertised as having value in itself.

There are however signs that the hype is now slightly fading as it becomes clear that many companies using the word do not actually fully understand the technology's impact on, and capabilities for, their business (Stafford and Murphy, 2016). Gartner places BCT after the peak of expectations in their hype cycle of emerging technologies (see Figure 1.1), meaning that the hype is slowing down and

[1] A trust-less distributed data structure storing data in blocks and linking each block to the
[2] Bitcoin is a cryptocurrency for sending funds without any third party involved presented in 2008 (Nakamoto, 2008).

disillusionment is taking over (Panetta, 2017). They further estimate that the plateau of productivity, i.e. when the BCT has matured, is in five to 10 years. When Gartner produced the Hype Cycle for Supply Chain Strategy (see Figure 1.1), blockchain in supply chain was instead placed in the stage of innovation trigger (van der Meulen and Pettey, 2017). This stage is characterized by early proof-of-concepts generating public interest while there is still a lack of usable products and proof of commercial viability (Gartner, 2018).

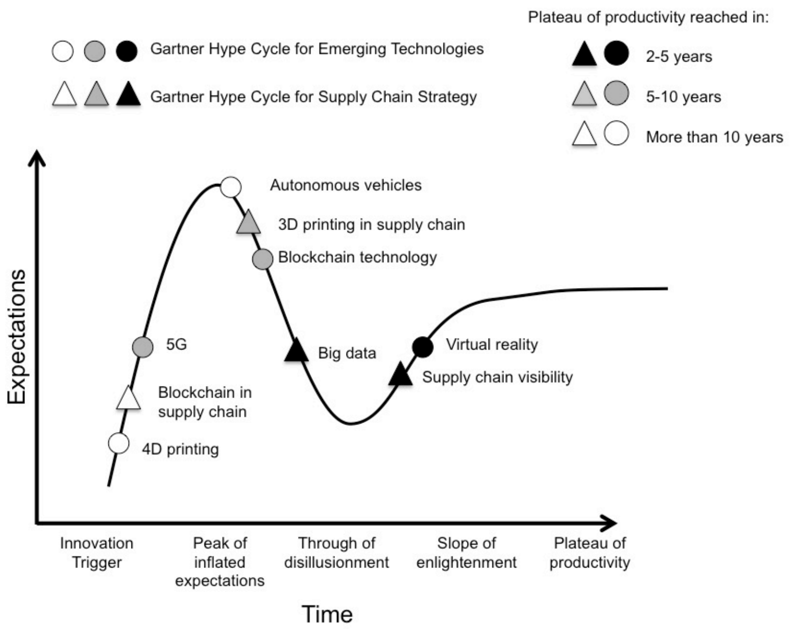

Figure 1.1: Combination of the Gartner Hype Cycle for Emerging Technologies and The Gartner Hype Cycle for Supply Chain strategy. Adapted from Panetta (2017) and van der Meulen and Pettey (2017).

A famous example of blockchain in the supply chain is the pilot project launched by IBM and Maersk based on a Hyperledger[3] blockchain, which aimed at reducing the complexity of the administration and to provide visibility in the supply chain (Groenfeldt, 2018; White, 2018). In the beginning of 2018 the two companies announced that they intend to launch a joint venture to further develop and bring their blockchain-based solution to the market (White, 2018). IBM (2017) also champion BCT as a technology to ensure food safety and enable recalls of contaminated products in a reasonable way. A number of initiatives have been launched, in cooperation with companies such as Walmart, Nestlé and Unilever. According to Deloitte (2017) blockchain can help to record information such as price, date, certifications and many other types of information. Obviously, this information is already recorded in any organized supply chain but what makes the situation different in the case of blockchain is the specific characteristics of the technology which

[3] The Hyperledger project is an open source initiative to create blockchains for business use and it was lauched by the Linux Foundation in 2016 together with 30 founding corporate members. Currently there are nine different blockchains being developed by the project. The focus is not to have specific chains which aret o be used by the members but to collaboratively develop code bases and frameworks that can be implemented by those who are interested. (The Linux Foundation, 2018)

implies that the information stored on the blockchain can be trusted. Deloitte further claims that having this information available on the blockchain can increase traceability, reduce counterfeit losses, improve visibility and compliance, and reduce paperwork. According to Deloitte (2017), the increased traceability follows from the creation of digital identities for goods and the subsequent recording of any events and information throughout the lifecycle of the goods. It also gives examples of why the suggested improvements are important. According to them up to 30 % of medicine sold in developing countries are counterfeits and inability to control processes at manufacturers can lead to bad publicity should irregularities be uncovered. In extension to the tangible improvements the technology provides more abstract effects that could also be realized. Having a system providing transparency can strengthen company reputation, improve credibility and public trust of the company, reduce risk concerning public relations due to supply chain malpractice and engage stakeholders (Deloitte, 2017).

Another example of blockchain being used in supply chain management (SCM) is a project by Microsoft (2018), which aims to integrate the use of blockchain into their cloud service Azure. BCT is advertised as a transformational technology enabling users of Azure to integrate with suppliers and have the security of a distributed database rather than trusting a single entity.

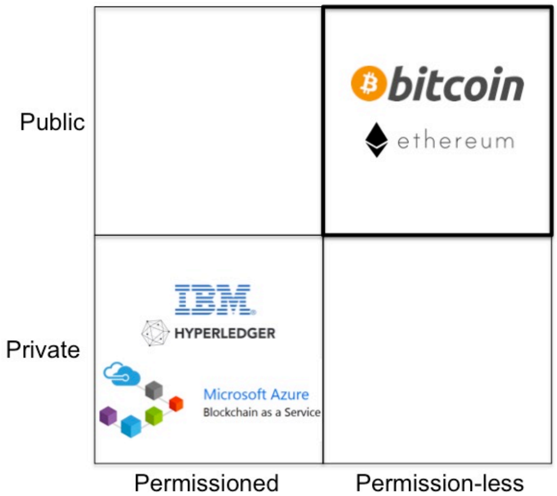

Figure 1.2: Visualization of the public-private and permissioned-permission-less spectrum. The focus of the thesis is marked with thicker lines in the upper right corner.

The previous examples are based on permissioned blockchains, meaning that only selected and trusted actors with permission can participate in the blockchain. In contrast Bitcoin is a public and permission-less blockchain (Pub-PL), i.e. any interested member of the public can participate (Nakamoto, 2009). The more exact meaning of permission and permission-less as well as the dimension private-public will be further explained in chapter 2.1, but a simple visualization can be seen in Figure 1.2. It can shortly be said that permission refers to what actions actors are allowed to take with permission-less meaning that all actors have the same rights while in a permissioned blockchain users have different rights. The private to public spectrum refers to who can access the blockchain at all, a public is visible and possible to interact with for anyone while access to a private one is limited to actors decided by its owner. Besides Bitcoin, there are also other Pub-PL blockchains. A very popular Pub-PL blockchain is the Ethereum chain (Popper, 2017a). Compared to Bitcoin it does not focus on being a currency but rather to work as a "global computing network" (Popper, 2017b). This enables users to program decentralized apps, i.e. essentially running programs on all the computers in the network simultaneously as if they together constituted one computer (Popper, 2017a).

The distinction between different types of blockchains is important since it has fundamental effects on the characteristics (Buterin, 2015). This thesis will focus on Pub-PL blockchains and what value their specific characteristics can have in supply chains. The investigated system can be seen in Figure 1.3 as a basic visualization, it will be given more detail in chapter 3. The blockchain is an information technology that lets users record data in a specific way, which in the case of Pub-PL blockchains then can be access by any stakeholder or member of the supply chain. This connects the technology to the information flow in a supply chain, as it is envisioned as a new way of recording, storing and sharing information in the supply chain. Some blockchains execute smart contracts[4] which might be used to transfer funds or assets (Morabito, 2017, pp. 101-105), constituting a connection to the financial flow. The physical flow is not directly interacting with the blockchain and can only be said to be affected indirectly through the information flow.

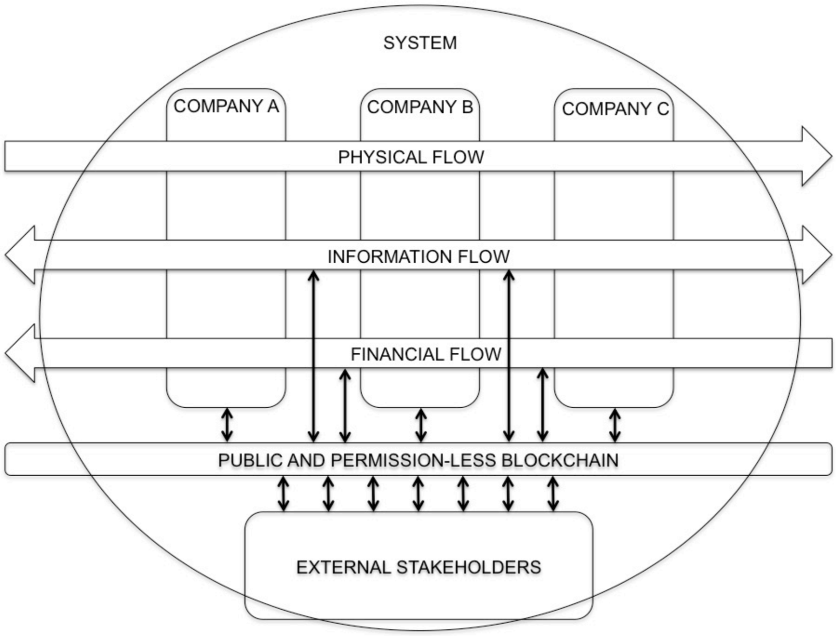

Figure 1.3: The system studied in the thesis.

Academic research has been slow to react to this new technology. A literature review by Yli-Huumo et al. (2016) only found 41 papers, of which only 1 was published in a peer-reviewed journal. They further found that 80 % of the reviewed papers focused

[4] A smart contract is a snippet of code on the blockchain, using logical IF/ELSE Statements to stipulate conditions. They are executed without any person or middleman involved. Often they are used to transfer funds from one place to another if some criteria are fulfilled. (Morabito, 2017, pp. 101-105)

on Bitcoin and only 20 % on the broader, underlying technology of blockchain. Even though the publication rate has increased since this literature review, the combination of industry hype and the lack of scientific attention make this phenomenon interesting to study from an academic perspective.

1.2 Problem description

This thesis focuses on the potential of Pub-PL blockchains in supply chains. According to Buterin (2015), most companies to date are considering implementing private blockchains as they appear easier to handle and implement. This is because the use of those resembles current structures, but bring some additional benefits. Advantages compared to Pub-PL blockchains include the possibility to change the rules of the blockchain, revert transactions, control access to information, and cheaper transactions. However, Pub-PL blockchains has characteristics that set them apart from permissioned ones. In short, Pub-PL blockchains lets anyone interact with the data stored on it while on a private blockchain only certain actors have permission to do certain actions. Cryptographically permission-less blockchains with certain “consensus mechanisms”, i.e. the way new data is added to the chain, can be considered more secure than their permissioned counterparts in that no one party can reverse transactions. This obviously has both advantages and disadvantages depending on your needs. The characteristics of Pub-PL blockchains given by Natarajan et al. (2017) are similar: It is easier for new actors to join the network since no central authority has to give their confirmation first and there needs to be no trust in a central authority nor in the actors transactions are taking place between.

Iansiti and Lakhani (2017) compare the situation in BCT today with that of the early days of Internet, when many companies started their own intranets. Nowadays intranets are scarce but at one point in time they were a step towards reaping the benefits of the then new technology of Internet. The development around BCT mirrors this development. In the 1970's the TCP/IP protocol was launched and saw *single-use* as the basis for sending email within the organization, pioneering the technology. In the next step of development the technology saw *localized use* as private networks, i.e. intranets, when new building blocks using the technology became available. The technology reached the public through the World Wide Web in the mid-1990s. Companies providing the infrastructure and tools around the TCP/IP protocol emerged at a large scale. With all this available the services using the Internet started *substituting* existing businesses, such as Amazon. In the last stage, the way in which businesses create value was *transformed* by, for example, Google and EBay.

The similarities are striking: Iansiti and Lakhani (2017) states that Bitcoin is used as a mean of sending money between two parties just as emails are used to send messages between people. They further explain that what is happening now is that organizations create their own private blockchains similarly to the creation of intranets. Blockchain could for example change the financial system the way the Internet changed the media industry and it is not just a technology for sending money, it is a protocol to build applications on (Ito et al., 2017). If the analogy holds the Pub-PL blockchains are the ones that will create the real change and where the long-term effects will be seen. Hence, in the long term these types of blockchains are the most interesting ones. Ametrano (2016) also supports the idea that the real paradigm shift will follow the permission-less blockchains, while the private blockchains are merely and incremental innovation of databases. Hence, it is clear that Pub-PL blockchains are interesting in a longer-term perspective. However, being a new technology, its use in supply chain should be evaluated.

1.3 Purpose

The purpose of this thesis is to evaluate the potential of public and permission-less blockchain technology to solve supply chain issues.

1.4 Research questions

RQ1: What are supply chain issues that public and permission-less blockchain technology can solve?

RQ2: How can public and permission-less blockchain technology be applied to solve these issues?

RQ3: What are challenges for successful implementation and use of public and permission-less blockchain technology in the supply chain?

The research questions are the vehicles for evaluating the suitability of the technology and combined they can fulfill the purpose. RQ1 identifies what supply chain issues that are relevant in the context. RQ2 has its base in the answer to RQ1 but goes on to concretize how applying BCT can solve the supply chain issues. This ensures that the applications arrived at really solves an actual issue and that issues suggested to be solved by Pub-PL BCT truly can be by providing concrete examples, in some way proving that the issue really can be solved. RQ3 puts the applications into a context of what challenges there could be in their implementation and use.

1.5 Focus and delimitations

Instead of looking at BCT as a whole, the thesis focuses on Pub-PL blockchains. This delimitation was made for three reasons; the authors personal interest, the perceived lack of distinction between public and private blockchains when discussing the technology and finally that the authors had the opportunity to stay for a prolonged period of time at the offices of Blockchainlab Srl in Milano. Blockchainlab Srl develops blockchain solutions, consult companies on the technology and incubate blockchain start-ups. The company focuses on Pub-PL blockchains in general, and specifically the Bitcoin blockchain. This opportunity gave the authors the possibility to acquire more technical knowledge regarding the Pub-PL BCT. However, the thesis does not go deep into the technology but rather examines the use of this technology, based on the specific attributes the blockchain gets from being public. Within the realm of Pub-PL blockchains, the study aims at being blockchain agnostic in the sense that no specific chain, such as Bitcoin or Ethereum, is considered as the one and only solution. The scope in terms of the supply chain is the entire supply chain, from source to consumer with all flows of products, services, finances and information between actors. The thesis is purely theoretical as the proposed solutions to supply chain issues will not be implemented and tested but will remain as concepts. Since this study is carried out as part of a master thesis, with a limited timeframe of 20 weeks, this will affect the choice of method. One of the methods used, called a Delphi study, is an iterative process in rounds supposed to go on until certain stop requirements are met. The conditions around this thesis required the number of rounds to be fixed to three.

1.6 Audience of the report

This report aims to make a scientific contribution an unexplored and rapidly developing field. One of the main audiences of this report is therefore the academic community, who can evaluate and build upon the research described in this report. An extension of the purpose would therefore be to formulate propositions for future research. As the technology also seems to be attracting a lot of interest within the supply chain community, another main audience would be supply chain practitioners who want to increase their knowledge about the technology and begin to investigate where the technology can be used in their specific supply chain.

1.7 Structure/outline of the report

The thesis consists of seven chapters, including this first introductory one. The next chapter gives a frame of reference of blockchain technology, a definition of supply chain management and an introduction to the SCOR framework for describing supply chains. It explains important terms and concepts related to these areas and provides a base on which to build. The third chapter presents the research view applied in this thesis and introduces the methods used. Next the result of the literature study is presented followed by a chapter with the results of the Delphi study. The results of these are analyzed and discussed in the sixth chapter, and the thesis ends with a concluding chapter that summarizes the findings and outlines the path for future research within the field.

2. Frame of reference

This chapter gives a background to blockchain technology, together with high-level descriptions of how it works, what advantages it comes with and what drawbacks it suffers from. A definition of supply chain management is also given, together with a brief introduction to the SCOR framework, which will be used in this study to describe a supply chain.

2.1 Blockchain technology

The original blockchain is the Bitcoin blockchain launched by the unknown person or entity called Satoshi Nakamoto in 2009 (The Economist, 2015). It was intended to be a decentralized peer-to-peer payment system that prevented double spending (Nakamoto, 2009). The concepts were published in a whitepaper outlining the functions and concepts the year before (Nakamoto, 2008). However, the concept of a chain of blocks secured through cryptography was proposed already in 1991 by Haber and Stornetta (1991).

There is often some confusion regarding concepts related to blockchains. Swan (2015, p. 1) uses Bitcoin as an example. The term Bitcoin can mean any of three parts: The underlying BCT platform, the protocol that runs over the blockchain, or the digital currency. The first layer, the underlying BCT platform, is the transparent ledger. This ledger can be compared to a database and every node has a copy of it. It is also this layer that is maintained by miners and controlled by all nodes. The middle layer consists of the programs that perform the transactions. On top is the actual cryptocurrency[5] Bitcoin.

Xu et al. (2017) explains that as a technology, blockchain is a trust-less distributed data structure. It is an ordered list of blocks that contains a list of only transactions[6] in the most basic cases or transactions with auxiliary data in more advanced cases. Every block is linked to the previous one by a hash[7], a pointer referencing the previous block. The hash is determined by the content of the previous block. This means that changing a block would invalidate the chain of hashes. It is a form of data storage that is append-only and replicated by peers. For an illustration of the hashing process, see Figure 2.1. Copies of the blockchain are distributed in the network and there is no

[5] A digital currency operating independently of any central bank, which uses cryptography to regulate creation of new units of the currency and to verify the transfer of funds. (Sikorski et al., 2017)
[6] Exactly what transactions are differs between blockchains. Generally they are data packages that store parameters. In Bitcoin they record monetary parameters but in other blockchains it can also be results of called smart contracts. (La Rosa et al., 2016)
[7] A hash is an output of a hashing function of fixed length based on an input of any size (Narayanan et al., 2016, pp. 23-24). In blockchains the hash points to the previous block (Zheng et al., 2017).

centralized database. Every node[8] stores a copy of the blockchain. This means that there is no need for a trusted middleman in order to confirm the transaction or changes on the blockchain. New blocks are added according to certain rules, which can differ between different chains. Xu et al. (2017) finally states that since the blockchain is distributed there has to be a method for reaching consensus among nodes about what is the latest block in the chain.

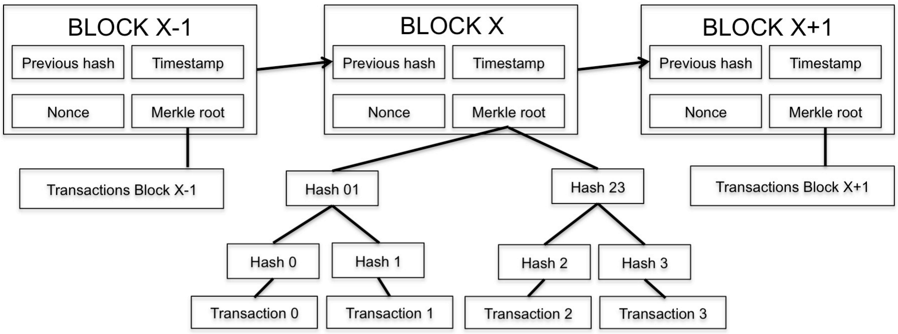

Figure 2.1: Illustration of the hashing process in the Bitcoin blockchain. Adapted from Rosic (2017).

Often BCT and distributed ledger technology (DLT) are used interchangeably, however, a distinction can be made according to Swan (2017). DLT is the more general term implying a shared database that is updated by consensus and records timestamped data with unique cryptographic signatures leading to a secure auditable history of transactions. Blockchain implements a distributed ledger with the additional technical feature of doing so by updating the database through blocks of data secured cryptographically with hashes which links the blocks together.

Further, Swan (2015, p. ix) makes a useful distinction of blockchains and their use into three levels. Bitcoin would be considered to be blockchain 1.0 since it is mainly concerned with cryptocurrency and applications related to cash. Blockchain 2.0 takes the economic uses one step further with the use of smart contracts, a concept we will expand on later, and more complicated applications than just cash transactions. The last level goes beyond economics and markets and concerns uses in areas such as government, healthcare and science.

2.1.1 Permission

The Bitcoin blockchain is a public blockchain where anyone can participate (Xu et al., 2017). However, this is not the only version of the BCT. It is possible to retain some of the main characteristics of blockchains using other set-ups where only selected parties can participate. Buterin (2015) explains three separate types of blockchains that are often identified:

[8] A node is a computer running a blockchain protocol (Morabito, 2017, pp. 6-7) and holding a copy of the blockchain (Narayanan et al., 2016, p. 54).

Public blockchains: A public blockchains is one that anyone can read, send transactions to, have their transactions included on, if valid, and where anyone can take part of the consensus process to add new blocks.

Consortium blockchains: A consortium blockchain is a blockchain controlled by a consortium of organizations or entities. The right to read and to send transactions, have their transactions included if valid and taking part of the consensus process to add new blocks can be restrict

Fully private blockchains: A fully private blockchain is similar to a traditional database but with the setup of a blockchain. Everything is controlled by one entity.

While Buterin (2015) used the terms public and private Xu et al. (2017) uses the terms permission and permission-less. In this paper the terms will be used as follows. Permission will mean what an actor is allowed to do on the blockchain. A public, or open, blockchain will mean one that is accessible to all and the opposite is then a private blockchain that only certain actor can use. Different setups have different characteristics and this thesis focuses on the permission-less blockchain.

Figure 2.2 shows the combinations of public-private and permissioned-permission-less according to the definitions. Bitcoin and Ethereum can be accessed by anyone and everyone has the same permissions (Xu et al., 2017). Ripple is a permissioned blockchain with a public ledger visible to anyone (Ripple, 2018) and Container Streams is based on a public ledger maintained by permissioned nodes (Jabbar and MacDonald, 2016). As mentioned before the IBM implementation of the Hyperledger Fabric blockchain is a private permissioned blockchain (IBM, 2018). The Swedish Lantmäteriet, the national land registry, is currently implementing a private permissioned blockchain for property sales (Anand, 2018). In the bottom right corner in Figure 2.2 it can be seen that there are no examples. It follows from the definition that it is impossible for a blockchain to be completely private and at the same time permission-less, letting anyone verify transactions.

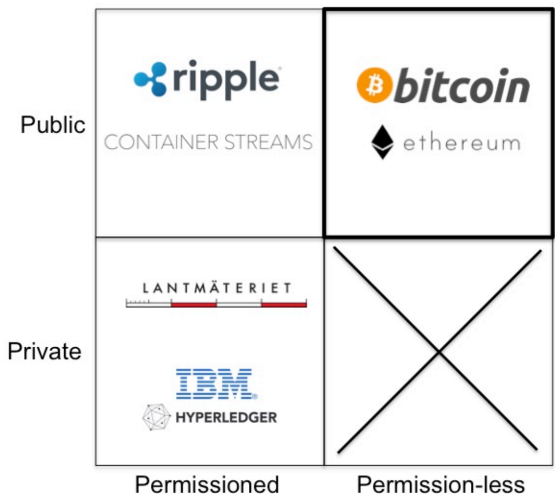

Figure 2.2: Examples of different types of blockchain, according to the classification used in this study.

2.1.2 Key attributes

The exact attributes of a blockchain depend on how it is configured in terms of, for example, permission and technology. Morabito (2017, pp. 22-23) gives the following as the most important attributes of blockchains:

Decentralization: Participants in the blockchain are linked together with each other and able to make transactions and transfer value without any central coordinating party. Hence you do not have to involve any third party in the transaction.

Trust and Provenance: BCT guarantees that data about a transaction existed at a certain point in time. Since every block contains information about the previous block in the chain, the history and ownership of the assets on the chain are automatically authenticated and unalterable. From this follows that no trust is needed to conduct transactions and it is possible to trace assets origins and everything that happened to them on the chain.

Resilience and Irreversibility: Every node stores one copy of the blockchain. This means that should some nodes fail, the system is stable enough to keep going. If the server in a traditional server system, without backup, fails, the data would instead be lost. Once a transaction is verified and approved it is unlikely that data will be changed.

The exact wording and focus of key attributes given in sources differs but overall the main ideas are the same. As a reference, Xu et al. (2017) give the fundamental properties of the blockchain as immutability, non-repudiation of data, integrity, transparency and equal rights.

2.1.3 Challenges for the technology

While delivering the attributes above, the technology is certainly not perfect and has certain drawbacks compared to traditional technologies. The main issues presented here are adapted from Swan (2015, pp. 81-83). Note the difference between throughput and latency; throughput is handled transactions per second and latency is when you can be certain that a transaction has been carried out.

Throughput: The rate to which a blockchain can process transactions is generally considerably lower than comparable technologies solving similar problems. Bitcoin has a throughput of seven transactions per second while VISA can handle 10000 transactions per second at its peaks.

Latency: In the Bitcoin blockchain it takes 10 minutes to create a new block, meaning that it can take at least 10 minutes for a transaction to be confirmed. However, for security reasons more blocks should be confirmed before it can be considered certain that the transaction is confirmed since the network chooses the longest chain if many alternatives should be available. In comparison, VISA only takes seconds to confirm a transaction. The reason it takes 10 minutes to add a block lies in the code of the Bitcoin protocol. The system self-adjusts to 10 minutes so that the resources going into the process will always be scarce (Narayanan et al., 2016, pp. 65-68).

Size and bandwidth: To be able to run a node validating the blockchain it has to be downloaded. With growing chains this might take time and it can be hard to keep up with the growth of it depending on the Internet connection available. While the size is still small compared to other data in areas such as research the difference is that it cannot be compressed since it has to always be readily available for security and availability reasons.

Security: The structure of the blockchain makes it secure, as could be seen in the beginning of this chapter, but there are still risks. The one most commonly heard about is perhaps the 51 % attack in the Bitcoin network. Should any entity get more than half the power in the chain they could potentially send previously transacted coins to its own wallet. Another potential risk is Sybil attacks in which an adversary creates many nodes in order to make itself seen as many different participants in order to isolate honest nodes from the network (Narayanan et al., 2016, p. 56).

Wasted resources: Certain processes for determining whether to add a new block to the blockchain requires huge amounts of energy. This is particularly a problem for blockchains such as the Bitcoin blockchain which uses Proof-of-Work as the consensus process for adding new blocks (Narayanan et al., 2016, p. 146). A lot of energy is used just to compete in adding new blocks to the blockchain and not for anything else. The annual energy consumption of the Bitcoin blockchain was estimated to be 69 TWh on the 28th of May 2018, which is similar to the annual energy consumption of the Czech Republic (Digiconomist, 2018). This is a more than five-fold increase when compared to the same time last year (Digiconomist, 2018).

Usability: The user friendliness for working with the blockchains is not always good.

Versioning, hard forks, multiple chains: The issue with having many different blockchains is that many of them are likely to be small and hence more vulnerable to attacks. Forking[9] chains, i.e. splitting them, gives rise to issue with interoperability.

2.1.4 Concepts and technology

In Figure 2.3 we can see the block header as explained by Rosic (2017). It contains data such as the hash of the previous block, a timestamp, a nonce[10] and a Merkle root. It would be inefficient to store all data as a series in the block and instead a Merkle

[9] A fork is a change of rules of the blockchain protocol and can be either hard or soft. A hard fork is a change of rules of the blockchain protocol leading to blocks created according to these new rules will be seen as invalid by validators running the old protocol (Castor, 2017). A soft fork is a change of rules of the blockchain protocol that is backward compatible and makes blocks created according to the new rules valid also according to the old rules (Castor, 2017).

[10] A nonce is an arbitrary string that can be changed in order to satisfy the rules for adding blocks in PoW (Zheng et al., 2017).

tree[11] is used. This makes it possible to find out if a transaction is part of a block or not much faster.

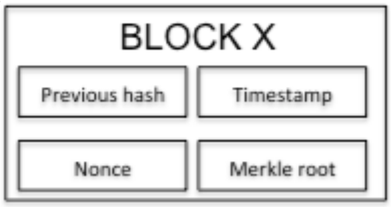

Figure 2.3: The header of a block. As earlier seen in Figure 2.1.

Only the Merkle root of the Merkle tree is in the header (Rosic, 2017). Just as the blocks are linked hash structures Merkle trees are internal hash structures to each block (Narayanan et al., 2016, p. 88). Swan (2015, pp. 37-38) states that the timestamp in the blockheader makes it possible to verify that the data in the block existed at a certain point in time and this can be used together with the hash to prove that files existed at a certain point in time. This is accomplished as any changes to the data in the block would generate a different hash and can therefore be spotted. This is referred to as timestamping the file.

The way it is decided whether a block should be added to the chain or not differs between blockchains, according to Narayanan et al. (2016, p. 64). In a distributed system such as a blockchain someone has to be chosen to record a transaction. It would be easiest to choose a node randomly, but true randomization is not possible and hence it is approximated. Nodes are chosen in proportion to a scarce resource that hopefully no one can monopolize, which is obviously not true randomization but close enough for this system. This makes attacks on the blockchain more costly and can work as a deterrent (Narayanan et al., 2016, p. 64). Commonly used algorithms to decide whether to add a block or not are Proof-of-Work (PoW) consensus[12] and Proof-of-Stake (PoS) consensus[13] (Zheng et al., 2017). Bitcoin uses a PoW algorithm

[11] A Merkle tree is a data structure. In it leaf nodes it has data that is hashed, concatenated in pairs and hashed again. The hashes are paired and hashed again which goes on until only one block remains, the root of the Merkle tree. Storing data this way makes it impossible to change the data without changing the Merkle root, effectively making it impossible to change. (Narayanan et al., 2016, pp. 34-37)

[12] PoW uses work as scarce resource. In the case of Bitcoin this means computational power and the proof is in the form of solving a hash puzzle. The nodes compete in solving this puzzle by finding a specific number, the nonce, so that when you concatenate the block header and use the hash function on it, the value of the hash falls within a certain range. (Narayanan et al., 2016, pp. 64-65)

[13] PoW is very energy intensive and PoS is an alternative requiring considerably less energy. Instead of using computing power as a scarce resource it uses ownership of the chain's currency. This is also in limited supply and for an actor to be able to make changes not following the rules of the chain they would need to own more than half of the coins on the chain. (Morabito, 2017, p. 11)

(Nakamoto, 2008) and the process of adding blocks is referred to as mining[14] (Zheng et al., 2017). The Ethereum protocol Casper is a PoS consensus mechanism but has not yet been implemented (Zamfir, 2015). Many more consensus algorithms exist, with two of them being Practical Byzantine Fault Tolerance (PBFT)[15], and Delegated Proof of Stake (DPoS)[16] (Zheng et al., 2017).

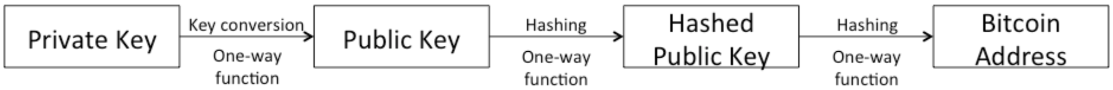

Figure 2.4: The connection between private and public keys, as well as the Bitcoin address. Adapted from Shirriff (2014).

As mentioned before, transactions are grouped together in blocks to be validated by some of the above-mentioned processes. Swan (2015, pp. 97-99) outlines the process of creating a transaction. To make transactions you have to have two linked keys, a private and a public one[17], Figure 2.4 gives a simplified view of how these are related on the Bitcoin network. The public one is transformed into an address known to everyone on the network and is used to verify your digital signature, and your private is used to sign your transactions. The private key is known only to you and it is not possible to find the private key from the public one. To send funds to someone else you need their address and the private key to the wallet that keeps your funds.

In Figure 2.5 the process of sending a transaction on the Bitcoin network can be seen, based on an example by Apodaca (2017). In this example there are two persons; Alice and Bob. Alice is sending the transaction to Bob and before doing so she creates a signature based on the transaction and her private key by using this as input to a signature function. The signature that is the output of the function is then sent together with the transaction to Bob. Bob can, with Alice's public key, the signature and the transaction verify through the signature function that the transaction submitted by Alice is authentic. In fact, the transaction is sent to Bob as you might imagine a letter being sent to someone's home address; it is sent to his Bitcoin address. This transaction is, as mentioned, authenticated and included in a block in the blockchain if the signature function outputs a confirmation.

[14] Mining simply means carrying out the consensus algorithm which allows for the creation and addition of new blocks to the blockchain (Morabito, 2017, p. 70). It is commonly carrying out the PoW algorithm that is called mining but it can be used to refer to other consensus algorithms too. Nodes calculating the hash values are called miners (Zheng et al., 2017). By adding blocks to the blockchain a node is awarded the currency of the chain, this is an incentive to carry out the process (Narayanan et al., 2016, p. 62).

[15] PBFT is not applicable for Pub-PL blockchains since every other node has to be known. It involves a voting process where a node queries other nodes for their vote in a series of rounds where every round output a new block. (Zheng et al., 2017)

[16] The difference between DPoS and PoS could be described like that between direct democracy and representative democracy. In DPoS users decide on nodes to vote for them in the consensus process.

[17] This is called Public/Private-Key Cryptography. Bitcoin uses the scheme Elliptic Curve Digital Signature Algorithm to create private and public keys. (Swan, 2015, pp. 98-99)

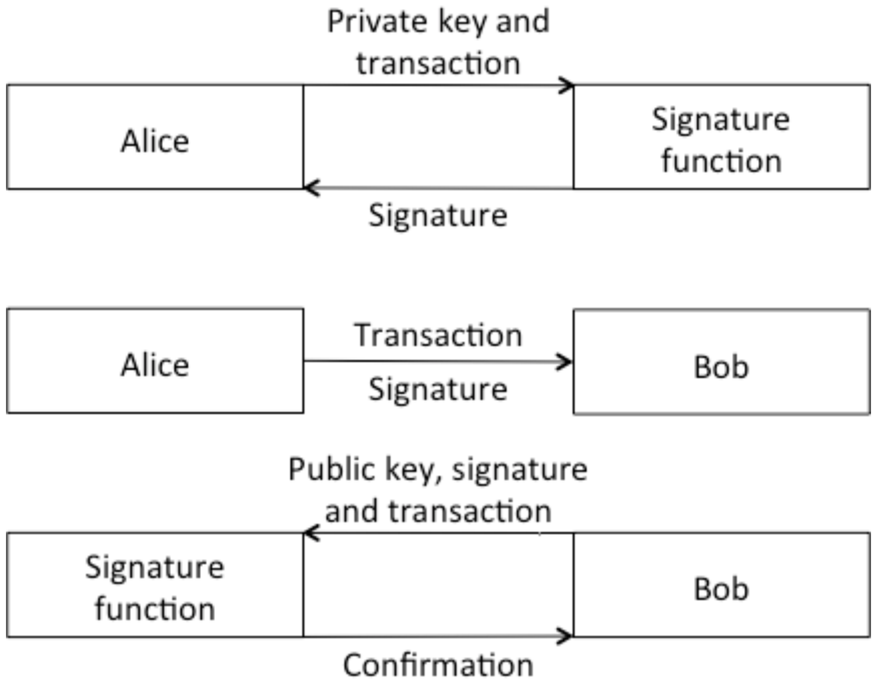

Figure 2.5: A transaction sent from Alice to Bob, using Public/Private-Key Cryptography. In the last step Bob verifies that the transaction is authentic and receives a confirmation. Adapted from Apodaca (2017).

Perhaps one of the currently most hyped concepts is smart contracts. Smart contracts are explained by Morabito (2017, pp. 101-105) as being snippets of code on the blockchain, using logical IF/ELSE statements to stipulate conditions. They are executed without any person or middleman involved. Often they are used to transfer funds from one place to another if some criteria are fulfilled. Smart contracts were initially described by Szabo (1996), who at the same time foresaw certain aspects of the BCT such as the use in digital currency and the use of public and private keys for cryptography. Trüeb (2018) describes smart contracts as being to blockchain what fish are to the sea. When BCT arrived, smart contracts found an infrastructure in which to swim in. However, smart contracts are not flawless. This was demonstrated by the DAO incident in 2016. The DAO (Decentralized Autonomous Organization) was a smart contract run on the Ethereum blockchain. Its purpose was to operate a decentralized venture capital fund, removing the middlemen and allowing owners to directly vote on funding of companies (The Economist, 2016). The smart contract of the DAO was implemented so that it would not release funding to a company unless a majority of the investors signed off, agreeing to the transfer (The Economist, 2016). A bug in the code of the smart contract was exploited in June 2016 and hackers managed to steal US$ 60M from the contract (Robertson, 2018). This lead to a hard fork of the Ethereum blockchain, with a majority of miners voting to revert the chain to its state before the attack (Coppola, 2016).

Chen (Forthcoming 2018) tells us that smart contracts can also be used to create tokens on top of the blockchain, which allows for tokenization of an asset. The token represents the asset on the blockchain and the price of the token is set by the market based on the underlying asset. It is further explained that in contrast, a cryptocurrency[18] is native to the blockchain. It is not based on a smart contract and is recorded straight on the blockchain. Both tokens and cryptocurrencies are kept in wallets[19].

Raval (2016, pp. 3-7) presents another use for smart contracts, decentralized applications (Dapps) that can also implement a token. No exact definition is given because of the novelty of the area but it can be said to be an application without any single point of failure run on many different nodes. Buck (2017) addresses the issue that smart contracts are coded to be executed when certain conditions are met but cannot access information not on the blockchain. Often input from the real world is needed and it is explained that oracles provide this service by providing information from the outside world to the smart contracts on the blockchain.

The Ethereum Community (2016) explains that Ethereum is a blockchain specifically designed to be a platform for smart contracts. However, even with this specific focus it costs a lot to store data on the blockchain and they suggest users to minimize the amount of data they store on the blockchain. Solutions for only storing certain parts of the data on the chain and the rest in other ways, such as the Interplanetary File System (IPFS)[20] are listed as alternatives.

2.2 Supply chain management & SCOR

2.2.1 Definition of supply chain and supply chain management

Although commonly used, the term "supply chain management" might not be that easy to properly define. Mentzer et al. (2001) defines the supply chain as "a set of three or more entities (organizations or individuals) directly involved in the upstream and downstream flows of products, services, finances, and/or information from a source to a customer". This is a basic definition many researchers agree on. The case for supply chain *management* is not as simple, even though the term has been around for many years (Ellram and Cooper, 2014). Mentzer et al. (2001) defines it as "the systemic, strategic coordination of the traditional business functions and the tactics across these business functions within a particular company and across businesses within the supply chain, for the purposes of improving the long-term performance of the individual companies and the supply chain as a whole." LeMay et al. (2017)

[18] A digital currency operating independently of any central bank, which uses cryptography to regulate creation own new units of the currency and to verify the transfer of funds (Sikorski et al., 2017).

[19] A wallet in terms of cryptocurrencies is software that stores public and private keys and interacts with blockchains. It is used for storing, sending and receiving cryptocurrencies (Max, 2017). Tokens can be stored in some wallets as well (Ledger, 2018).

[20] IPFS is a distributed file system storing files using techniques similar to the ones used in blockchains, such as hashing. It lets information be stored in the system while securely storing a link to the data on the blockchain. (Protocol Labs, 2018)

collected many definitions from a literature study and arrived at their own definition: "Supply chain management is the design and coordination of a network through which organizations and individuals get, use, deliver, and dispose of material goods; acquire and distribute services; and make their offerings available to markets, customers, and clients." The last definition is chosen as it highlights the activities and tasks to be carried out in a supply chain. This definition connects to the Supply Chain Operations Reference model, published by APICS.

2.2.2 SCOR

The Supply Chain Operations Reference (SCOR) model was first released in 1996 by the Supply Chain Council, which has since merged with another supply chain management association called APICS. The SCOR model can be used to describe, measure and evaluate a supply chain. Focus in this study will be on the descriptive part, although linkages to evaluating the supply chain can be explored to assess the potential impact of BCT.

Processes

The model defines SCM as six integrated processes: Plan, Enable, Source, Make, Deliver and Return (APICS, 2017). Using this model, a supply chain can be seen as a chain of organizations performing these processes (see Figure 2.6). The SCOR model can be considered abstract and trivial when viewing a supply chain in low resolution. Therefore, the model can be viewed on successively more detailed levels. Level one defines the processes, level two adds sub-processes that allow for configuration to describe a specific supply chain and level three describes key processes to successfully compete using the selected supply chain configuration (Rosenbaum and Bolstorff, 2003, p. 4).

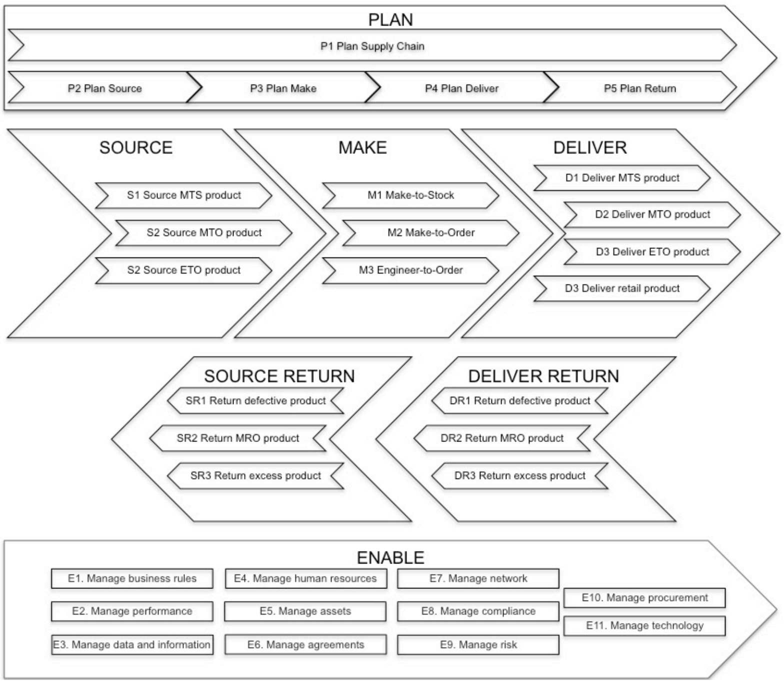

Figure 2.6: Overview of the SCOR processes. Adapted from Rosenbaum and Bolstorff (2003).

For readers who are not familiar with SCOR framework and wish more detailed descriptions of the different processes, this can be found in Appendix A.

Other aspects of the SCOR model

The processes form the foundation of the SCOR model. They facilitate the detailed description of specific supply chain configurations as a supply chain can be characterized as a combination of the processes. APICS (2017) provides three other puzzle pieces to the SCOR 12.0 model: performance, practices and people.

Performance describes measurements for evaluating supply chain execution. There are five different performance attributes: reliability, responsiveness and agility, which are considered customer-focused, and cost and asset management efficiency, which are considered internally focused. Performance metrics are also categorized in a hierarchical structure of three levels. Level three metrics help identify performance gaps in level two metrics who, in turn, diagnose level one metrics. The performance metrics can be linked to the processes of the SCOR 12.0 model.

The SCOR list of practices helps identify practices that could improve supply chain performance. It contains valuable practices, divided into the categories of emerging practices, best practices and standard practices. Each practice is also connected to processes and performance metrics. As an example, BCT is listed as an emerging practice, connected to the enabling processes of managing business rules, managing information and managing assets. Blockchain is also connected to the level one performance metric Total Supply Chain Cost.

The final aspect of the SCOR 12.0 model, people, reflects the need for staffing the supply chain with the right talent. It is a list of skills, which processes they are required for and which experiences and trainings are necessary. Five competence levels ranging from novice to expert describe the level of knowledge.

2.2.3 Use of SCOR in this study

Samuel et al. (2004) argued already in 2004 that the SCOR framework was on its way to becoming an industry standard. Connecting the study to a well-known framework facilitates the use of the results by supply chain practitioners. Samuel et al. (2004) further noted that the SCOR framework could be used to evaluate supply chain software applications, a purpose that mimics the purpose of this study.

The reference model spans all customer and market interactions as well as product transactions, just as intended when examining the supply chain, but excludes areas such as marketing, which are related to supply chains but would make the scope too wide (Rosenbaum and Bolstorff, 2003, p. 6). This study links processes listed in SCOR 12.0 to capabilities of BCT. This gives a framework to ensure that relevant areas are covered and structures the results of the study. It also provides a common language for readers and participants of the study and in doing so reduces the risk of misunderstandings.

3. Research approach and method

This chapter begins by introducing the general research view applied in this study. It then goes on to describe the two main research methods employed in this study: the literature review and the Delphi study. The chapter concludes with a discussion on research quality and how the quality of this study has been guaranteed.

3.1 Research view

Arbnor and Bjerke (2009) propose a view of scientific research where a connection between presumptions, methodology and the area to be studied is made. The presumptions of the researcher, regarding the conception of reality and how knowledge is created, influence the methodological view. The procedures and methods that arise from this view influence the research in the study area. Three contrasting views are presented: the analytical view, the systems view and the actors view.

3.1.1 The analytical view

According to Arbnor and Bjerke (2009) the underlying assumption of the analytical view of science is that the world around us is filled with facts that are considered as true. The aim is to discover those facts that are invariant to environment and individual perceptions. It is assumed that variables can be studied independently from each other. The research is often quantitative in its nature and therefore aims to produce precise measurements of variables and their relationships.

3.1.2 The systems view

Arbnor and Bjerke (2009) also introduce the systems view. A system is constructed by a number of interrelated components. The fact that individual components of a system are related means that studying them separately, as proposed in the analytical view, is impossible. Instead they must be contextualized as part of a system, and given its context they can be studied. In the systems view, relations between variables are therefore important and the aim is to discover and explain these relations. According Gammelgaard (2004) , the primary purpose of the systems view is to improve the performance of a system. This leads to a more pragmatic view of science and objective truths.

3.1.3 The actors view

Arbnor and Bjerke (2009) present the actors view where reality is a social construct that is impossible to separate from us. This means that all phenomena need to be interpreted in relation to the actors they concern. It also means that researchers are influenced by their relation to the phenomena, and this influences the created knowledge.

3.1.4 View in this study

The authors of this study view the supply chain as a system of subcomponents, e.g. companies, activities and processes. This view is shared by Mentzer et al. (2001) who state that SCM is characterized by its systems approach to viewing the supply chain as a whole. In this study, the BCT is viewed as a component that in interacting with the supply chain system is integrated into it. The study aims to describe the relations between BCT and subsystems and components of the supply chain. For these reasons, a systems view has been adopted in this study and has influenced the choice of method.

The system to be studied in this thesis has been influenced by the view of Jaradat et al. (2017). They base their view of the supply chain on Porter's Value Chain, a commonly used tool to describe the organization of a firm to transform inputs to outputs, adding value to consumers. As the SCOR framework is used as the overarching supply chain framework in this study, the description of Jaradat et al. (2017) has been adapted to include this.

Figure 3.1 presents our view of the system to be studied in this thesis. It is an illustration of how companies in a supply chain interact (described through connections between SCOR-processes) and how BCT interacts with these companies. External stakeholders in this system could be end-consumers, regulators and financial institution. This is a more detailed systems view than the initial view presented in Figure 1.3, increasing the level of detail on the internal processes of the companies and how flows and processes are connected.

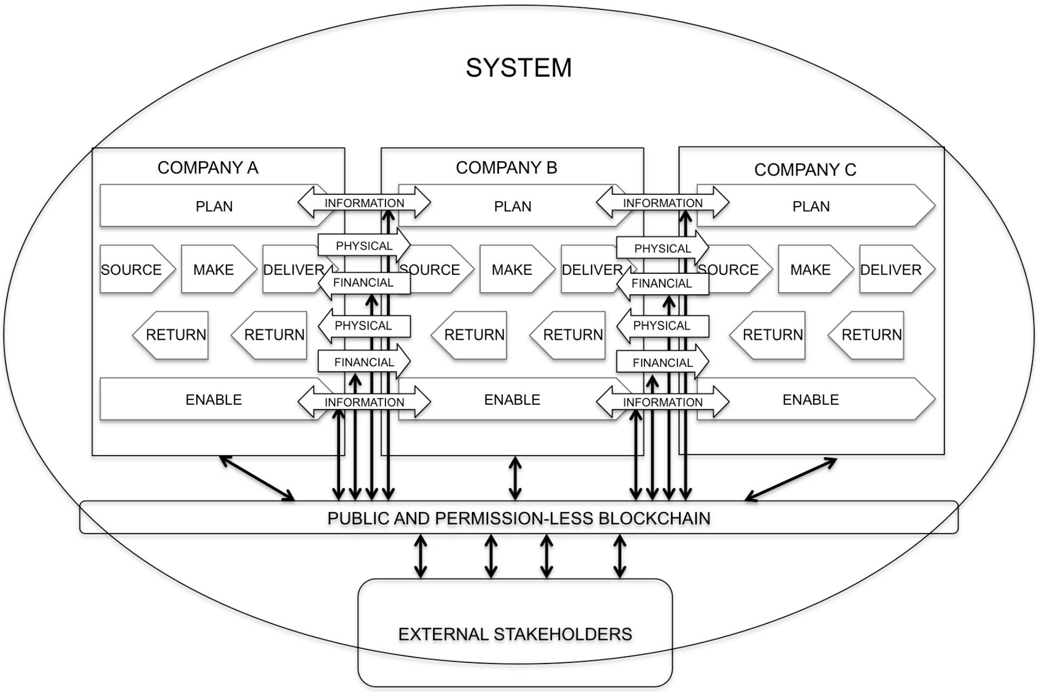

Figure 3.1: The system investigated in the thesis. The main purpose of this system illustration is to show how Pub-PL blockchains can interact with flows between supply chain partners.

3.2 Research approach

The research carried out in this thesis began by conducting a literature review to identify what had already been written on the topic of BCT in supply chains. This literature review generated a list of supply chain issues that Pub-PL BCT has been suggested to solve and a list applications of Pub-PL BCT that have been suggested for use in the supply chain. These lists were used as input into a three-round Delphi study. The specifics of the Delphi method will be explained later in this chapter, but it can be said to be an iterative research method that uses the knowledge and opinions of experts within the field. Each round was analysed and the results were used as inputs into the following round. The final result of the Delphi study was a rated list of supply chain issues that Pub-PL BCT could potentially solve and a rated list of applications of Pub-PL BCT that are suitable for the supply chain, answering research question 1 and research question 2. As a final step of the analysis, the results of the Delphi study were compared to and contrasted with the reviewed literature. Comments provided by the experts in the Delphi study were also analyzed and grouped into themes, from which challenges of the implementation of Pub-PL BCT in supply chains could be deduced. This analysis answered research question 3. The general approach of this thesis has been summarized in figure 3.2.

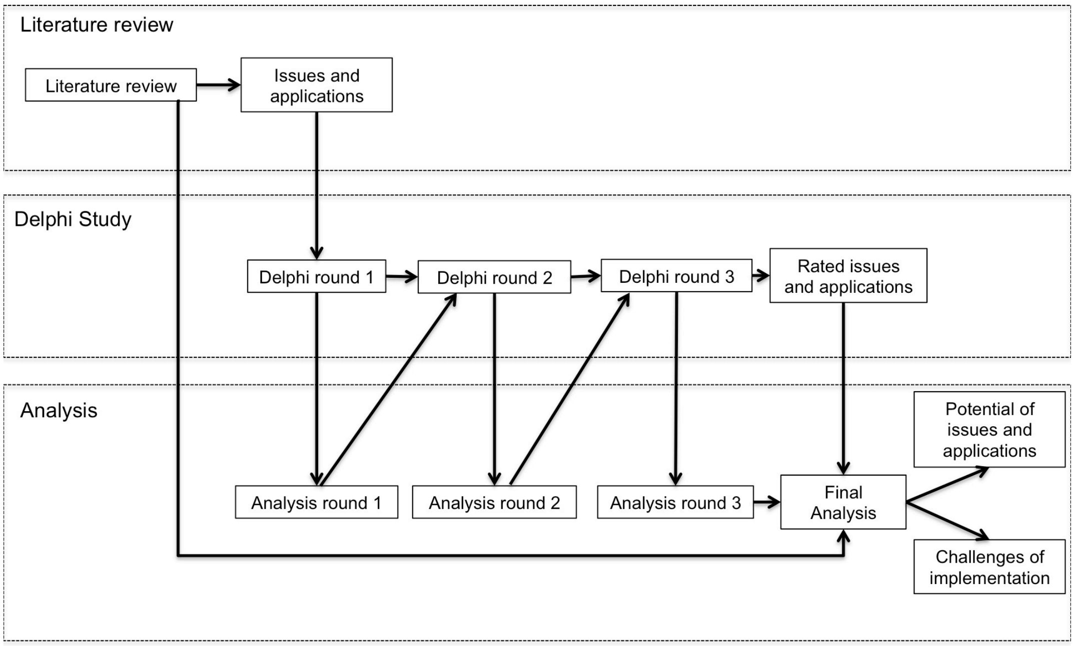

Figure 3.2: The general approach of this study.

3.3 Quantitative and qualitative research

Two labels are usually placed on scientific methods, to distinguish two forms of thinking: quantitative and qualitative. Quantitative thinking "relies heavily on linear attributes, measurements, and statistical analysis" (Stake, 2010, p.11) while qualitative thinking "relies primarily on human perception and understanding" (Stake, 2010, p.11).

Stake (2010) lists a few characteristics of a qualitative study, e.g.: it is interpretive, it is empirical and it is situational. According to Morse (1991), qualitative studies are useful for emerging subjects, exploring a phenomenon, developing theory and when possibilities to quantitatively measure the phenomenon are limited. The aim of this study is to explore an emerging field of study: BCT in SCM. As few projects have been implemented at a larger scale and the potential relationships between components in the system are unknown, it would be difficult to produce quantitative measurements. The study will also be highly situational, focusing on the intersection between technology and the supply chain at this moment in time. The study will therefore mainly rely on qualitative thinking and qualitative research methods. Quantitative measurements will however also be incorporated into the Delphi study.

3.4 Literature review

This study used a literature review to construct the first-round questionnaire in the modified Delphi method; the review therefore played a vital role. Rowley and Slack (2004) propose six other reasons for which conducting a literature review can play an important role. These reasons, and their corresponding role in this study, can be seen in Table 3.1.

Table 3.1: Different reasons for conducting a literature review according to Rowley and Slack (2004). For each reason, a reflection on the connection to this study is given.

Reason to conduct a review	*Role in this study*
Support identification of research topic.	Validates that this is an area of interest within the scientific community.
Identifying literature to which the study will make a contribution.	Identifies the frontier that the study aims to extend from.
Understanding terminology and concepts.	Allows for a more informed literature review and incorporation of these terminologies and concepts in the study will make it accessible to the research community.
Building a bibliography.	Increases validity of the study as it is founded on previous research.
Suggesting research methods.	An initial literature review of methodology allows for an informed choice of methods.
Analyzing and interpreting results.	Empirical results can be contrasted with literature review to strengthen earlier research or identify areas of conflict.

Tranfield et al. (2003) observe that literature reviews in management research have been criticized for being biased and lacking a critical view, with researchers selecting literature for the review based on personal bias. The systematic literature review attempts to structure the process of conducting a literature review adding properties of transparency and replicability.

This study used the approach of Tranfield et al. (2003) for conducting a systematic literature review, also taking suggestions by Durach et al. (2017) into account. Tranfield et al. (2003) build on the strong tradition of conducting systematic literature reviews in the medical field and add adaptions that apply to the idiosyncrasies of management research. In turn, Durach et al. (2017) add their view on the peculiarities of SCM research to further adapt the method.

Tranfield et al. (2003) propose a three-stage process for conducting a literature review: planning the review, conducting the review and reporting the review. Each phase includes a set of activities to be carried out.

3.4.1 Planning the review

This phase includes performing a scoping study to initially assess the existing literature and theory in the field of interest (Tranfield et al., 2003). For the field of SCM, given its broad nature and lack of universal definitions, a theoretical framework in which to study the phenomenon has to be decided upon at this stage (Durach et al., 2017). This is also where the research question for the literature review is defined.

Booth et al. (2016) suggest asking three questions to determine what the scope of the study should be: Who are being studied? What is being studied? What is the impact that is being studied?

The initial scoping study of this review revealed that very few articles on the subject of blockchain in supply chain had been published in peer-reviewed journals.

The research questions of the literature review mimicked the research questions of the master thesis:

1. What are supply chain issues that public blockchain technology can solve?

2. How can public blockchain technology be applied to solve these issues?

The research questions incorporate two of the three questions proposed by Booth et al. (2016): "What is being studied?" and "What impact is being studied?". "Who is being studied?" could be applied through singling out certain industries or types of organizations, but with regards to the low number of publications it was decided to not narrow down the study in this regard.

The reason for having the research questions of the literature review consider all public blockchains and not the more narrow case of Pub-PL blockchains were because it would have ruled out many articles treating public and permissioned blockchains that presents ideas quite easily adaptable to permission-less blockchains. For scientific articles, certain private or hybrid blockchain applications were included in the literature review when it was deemed that they could be adapted to a Pub-PL solution. This poses no threat to the final result of the thesis in terms of mixing the characteristics of the two types of technology since the experts in the Delphi study will review what has been identified in the literature review. Instead it might improve the results as certain applications that have so far only been considered using private blockchains could be implemented with Pub-PL blockchains.

The criteria for including or excluding identified literature from the final review should also be developed at this stage (Tranfield et al., 2003). The research question will influence the inclusion criteria as it specifies the scope of the research to be studied (Booth et al., 2016). Inclusion criteria could also specify when the study has been published, where a study was published and the methodology that has been used. In SCM studies, both analytical and empirical studies can provide useful input to the review and the inclusion criteria should not exclude one of these (Durach et al., 2017). The pre-defined theoretical framework should be taken into account when developing inclusion criteria, e.g. with regards to unit of study, contexts and the definitions used (Durach et al., 2017).

Two sets of inclusion criteria were developed, one to be used for scientific articles and one to be used for grey literature. The grey literature used in this study were whitepapers, a publication type we will describe more in detail later. For scientific articles, the inclusion criteria in Table 3.2 were used.

Table 3.2: Inclusion criteria for scientific articles, with corresponding motivations.

Inclusion criteria	*Motivation*
Is the paper published in a scientific journal?	Publications in scientific journals guarantee a certain level of quality.
Is the paper written in English?	English articles are easier to critically assess for interested readers of this thesis.
Is the paper written between 2008 and now?	The first application of BCT, Bitcoin, was launched in 2008. Any articles pre-dating that could reference another concept of the same name.
Does the paper treat the interaction between blockchain technology and the supply chain?	The paper should treat the phenomenon that is studied in this thesis.

The inclusion criteria for whitepapers can be found in Table 3.3.

Table 3.3: Inclusion criteria for whitepapers, with corresponding motivations.

Inclusion criteria	*Motivation*
Is the paper written in English?	English articles are easier to critically assess for interested readers of this thesis.
Does the paper describe an application built on public or permission-less blockchain technology?	This thesis studies public, permission-less blockchains.
Does the application have a clear connection to supply chain?	The application should be connected to the phenomenon that is studied in this thesis.
Does the application extend beyond using cryptocurrency or tokens as means of raising funds?	Many start-ups are using initial coin offerings as a way of raising capital. If no other connection to BCT exists, it is not deemed as an interesting application for this study.

It can be noted that the inclusion criteria for whitepapers specify that the application should be based on a public or permission-less blockchain, while no such inclusion criteria is applied to scientific articles. After the initial scoping study, it was concluded that there is a lack of scientific publications on the subject and that many publications do not make the distinction between public and private or permissioned and permission-less blockchains. There is, however, not a lack of whitepapers for blockchain applications, allowing for more specific selection criteria in terms of technological implementation.

As per the recommendation by Tranfield et al. (2003) a review protocol summarizing the research questions for the literature review, which databases to search in and the inclusion and exclusion criteria was prepared. The review protocol can be found in Appendix B.

3.4.2 Conducting the review

This phase can be broken down into four key activities; searching for articles, selecting articles for inclusion, extracting data and analysis.

Tranfield et al. (2003) suggest a wide search including published journals, databases, unpublished studies, conference proceedings, industry trials and the Internet. This literature review was conducted using both peer-reviewed articles published in academic journals and what is referred to as grey literature. Grey literature, as opposed to white literature, is a term referring to literature not published in a journal and not subject to peer-review. The reasons for including grey literature in a systematic literature review could be to adapt the research to non-academic end-users, to fill gaps in academic literature to be able to catch very recent developments in the field or to capture contextual information that is not adequately captured by a review of white literature only (Adams et al., 2017).

This review relied on peer-reviewed articles and grey literature in the form of whitepapers. The decision to include whitepapers was made as blockchain is a rapidly developing technology and whitepapers could reflect recent developments in a better way. A whitepaper could also fill gaps in academic literature, providing a different perspective on the technology. A whitepaper usually specifies the problem that a certain application of the technology aims to resolve and the means by which it will resolve it. A whitepaper is often, but not always, published by a company as a way of demonstrating their solution. Adams et al. (2017) highlighted two main challenges of incorporating grey literature into a literature review. The first one is to use scientifically sound search techniques. If no relevant databases exist, search engines, such as Google, could be used. This requires different search criteria; there are examples where the first five pages of Google results or the 500 first results have been used as delimitation. The second challenge is to ensure the quality of included literature.

The scoping study was used to construct initial search words and search terms (Tranfield et al., 2003). Many different search strategies exist, of which a few are presented below:

Briefsearch

A briefsearch is a quick way to retrieve a small number of relevant documents; it can be used to retrieve a certain publication known to be important in the field or to get an initial view of the research present in the field (Rowley and Hartley, 2008, p. 115).

Citation pearl growing

Citation pearl growing uses one, or a few, central documents as a starting point and look for terms to be used to extend the search. It is useful if the terminology of the subject is unknown to the researcher (Rowley and Hartley, 2008, p. 115).

Building blocks

The building block strategy represents key concepts of the field through synonyms or related terms and uses the Boolean OR and Boolean AND functions to construct and iteratively refine the search (Rowley and Hartley, 2008, p. 115).

Successive fractions

Successive fractions are used to continuously narrow down search results by adding more specific terms to the search string (Rowley and Slack, 2004).

Search strategy in this study

The scoping study of this review was carried out using the briefsearch strategy. No central documents were identified, and the use of citation pearl growing was therefore discarded. Instead the building blocks strategy was used, and complemented by successive fractions when searching in databases that gave a large number of results. Terms, concepts and subjects were identified through the brief search and in the SCOR framework and combined to create relevant search strings.

The initial databases used for retrieving peer-reviewed articles were Web of Science Core Collection and Business Source Complete (EBSCOhost). As initial searches yielded few results, the search was extended using Emerald, ScienceDirect (Elsevier) and Google Scholar. For all databases except Google Scholar, all search results were retrieved and considered for inclusion. For searches on Google Scholar, the first 50 results were considered when using the building blocks strategy and the first 20 results were considered for consequent searches using successive fractions.

The search engine Google was used to search for whitepapers. The same strategy as when searching for scientific articles on Google Scholar was used, considering the first 50 results when using the building blocks strategy and the first 20 results for subsequent searches. The search strings used can be found in Table 3.4 and Table 3.5.

Table 3.4: Search strings used in the literature review for white literature.

<table>
<tr><td>Database</td><td>Basic string</td><td>AND</td><td>AND</td><td>AND</td></tr>
<tr><td rowspan="2">Web of Science
Business Source Complete
Emerald
ScienceDirect (Elsevier)</td><td rowspan="6">(blockchain OR “distributed ledger”)</td><td>(supply chain OR logistics)</td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>procurement</td></tr>
<tr><td rowspan="4">Google Scholar</td><td rowspan="4">(supply chain OR logistics)</td><td>(procurement OR sourcing)
(production OR manufacture*)</td><td rowspan="4">journal
-
conference
-book</td></tr>
<tr><td>(distribution OR deliver)</td></tr>
<tr><td>transport*</td></tr>
<tr><td>plan*</td></tr>
</table>

Table 3.5: Search strings used in the literature review for whitepapers.

<table>
<tr><td>Database</td><td>Basic string</td><td>AND</td><td>AND</td><td>AND</td><td>AND</td></tr>
<tr><td rowspan="7">Google</td><td rowspan="7">blockchain OR “distributed ledger”</td><td rowspan="7">whitepaper OR "white paper"</td><td rowspan="7">permission-less OR public</td><td rowspan="6">supply chain</td><td></td></tr>
<tr><td>plan</td></tr>
<tr><td>source</td></tr>
<tr><td>make</td></tr>
<tr><td>deliver</td></tr>
<tr><td>return</td></tr>
<tr><td>procurement</td><td></td></tr>
</table>

After the initial retrieval, the predefined inclusion criteria should be applied to the retrieved documents and the publications to be included in the review are selected (Tranfield et al., 2003). Reasons for exclusion should be documented clearly (Booth et al., 2016). After literature from these databases had been retrieved, a scan of the reference lists of each peer-reviewed article was made to find relevant articles that had not yet emerged in the literature review.

Data should be extracted using data extraction forms including details of the information source (title, authors, journal, publication details) and details on the study such as context, methodology, links to concepts and emergent themes (Tranfield et al., 2003). Two different extraction forms were used in this literature review, one for peer-reviewed articles and one for whitepapers. Both placed emphasis on identified applications of BCT and their connections with SCM. The complete data extraction forms are found in Appendix C.

The quality of selected studies is usually evaluated, though it is rarely employed as an inclusion or exclusion criteria. Forming a view of the quality of the selected studies and being transparent in this assessment is nonetheless necessary to judge the individual contribution of each included study (Booth et al., 2016). Evaluating the quality of quantitative studies is usually straight-forward as controlled trials lend themselves well to a statistical approach for testing significance (Tranfield et al., 2003). Popay et al. (1998) state that evaluating qualitative studies is generally more difficult but suggest some criteria that can be used in an evaluation (see Table 3.6).

Table 3.6: Criteria to evaluate quality of qualitative studies, and the related key question to answer. Adapted from Popay et al. (1998).

Criteria	*Key question*
Responsiveness to social context and flexibility of design	Has the research design been adapted to the real-life settings encountered?
Theoretical or purposeful sampling	Is the sample adequate for producing knowledge?
Adequate description	Is the description detailed enough to allow the reader to make own interpretations of context, methods and meaning?
Data quality	Are different sources compared and contrasted?
Theoretical and conceptual adequacy	Does the research move from data to analysis and interpretation in a transparent and coherent manner?
Potential to assess typicality	Are claims for generalizability supported by valid argumentation?

The evaluation criteria of Popay et al. (1998) were incorporated in the data extraction sheet for peer-reviewed articles. The quality of peer-reviewed articles was also assessed through looking at the publication, using the impact factor as a signal for quality. As one of the purposes of the grey literature review was to identify proposed applications of BCT, the quality of whitepapers was assessed through the level of detail in which the application is described. Quality was also assessed based on the clarity the whitepapers managed to describe the issues they intended to solve and how well the text was written in general, taking into account language and if the there was a clear line of argument throughout the text.

The analysis in a literature review can be performed using different approaches. In the medical field, where the tradition of systematic literature reviews is strong, meta-analysis is a common approach. Meta-analysis includes pooling results from different studies and using statistical tools to prove relations between variables (Tranfield et al., 2003).

Meta-analysis is difficult to attempt in the management field. Tranfield et al. (2003) cite the heterogeneity of the field as an issue while Durach et al. (2017) note that much research in the field of SCM seeks out new knowledge instead of attempting to validate earlier findings.

Denyer and Tranfield (2006) concludes that a lack of research studies posing the same questions, adhering to the same definitions and using the same methods leads to difficulties in pooling studies for statistical analysis. Instead, a narrative approach is usually taken. Narrative analysis groups different studies, studying different aspects of the same phenomenon, and tries to create a narrative and a bigger picture of the phenomenon. According to Rumrill and Fitzgerald (2001), a narrative analysis is useful for explanations of emerging issues and theory and model building but it has been criticized for its subjectivity. They go on to state that it is not unheard of that two systematic literature reviews on the same issue can present different results when using this technique.

As the use of BCT in SCM is an emerging field and few studies, to perform meta-analysis on, exist, narrative analysis was used to synthesize the findings of the literature review.

3.4.3 Reporting the review

The third stage, reporting, can be divided into reporting the descriptive and the thematic analysis. Tranfield et al. (2003) state that a descriptive analysis of the field can include age profile of articles, geographical spread of research and different sectors of research while a thematic analysis focuses on identifying themes and patterns in the research. In this study, themes will be related to supply chain issues that BCT is suggested to solve and proposed applications of BCT in the supply chain.

The results of the literature review have been reported from both a descriptive and a thematic point of view. The study followed the suggestions of Adams et al. (2017) in, to a certain extent, separating grey and white literature when reporting the review, so that readers clearly can see which sources the information stems from.

3.5 The Delphi method

The Delphi method was developed in the 1950's to extract consensus on a specific issue from a group of experts (Vernon, 2009). This is achieved by a series of questionnaires and controlled feedback (Dalkey and Helmer, 1963). Originally developed by the RAND (Research and Development) corporation to estimate the number of nuclear bombs the Soviets would use in the case of war (Dalkey and Helmer, 1963), it has since seen use in various areas such as planning and technological forecasting (Delbecq et al., 1975, p. 84) and medicine (Vernon, 2009). It can also be used as a decision tool, and even as a tool for learning among the participants (Gupta and Clarke, 1996).

The method has four special characteristics setting it apart from others: Anonymity, Iteration, Controlled feedback and Statistical group response. The list below is adapted from Rowe et al. (1991):

1. Anonymity: All experts are anonymous to each other by the use of questionnaires rather than physical meetings. By being anonymous the social pressure possibly felt in a group can be removed and the ideas considered can be evaluated on its merits. There is no risk of losing face.
2. Iteration: Several questionnaires are used; this allows members to revise their position.
3. Controlled: Between each round the opinions expressed by the expert each round are shared with every expert. It could be actual arguments but most often it is some statistical measure of the opinions of the group.
4. Statistical group response: In the end more than just a consensual judgment is available through the use of median value of the experts opinions and measures indicating their spreads.

Vernon (2009) combines point 2 and 3 but adds “Expert panel” as a characteristic. It is indeed central to the Delphi method; the data extracted is based on judgments made by experts.

The method was chosen because knowledge from different areas of expertise, i.e. both blockchain and supply chain, has to be combined. According to Cotton (2014, p. 81) the Delphi method is suitable for this purpose. A panel would give a better answer than a single individual and it allows both soliciting opinions from experts as well as having them rank them (Okoli and Pawlowski, 2004).

3.5.1 Advantages and disadvantages

According to Gupta and Clarke (1996) the Delphi method has the advantage of being able to use the expertise and authority of experts but avoiding some common weaknesses of face-to-face interaction like conflict within the group and the dominance of certain individuals. It lets the expert revise his or her position and react to inputs from the rest of the group without publicly admitting it, meaning that they can use their knowledge in a better way without losing face. The Delphi method embraces the idea that the whole is greater than the sum of its parts, the influence the feedback constitutes lets the participants learn from each other. Hence the result from the Delphi will be better than if all participants would answer questionnaires in a more traditional way. Gupta and Clarke (1996) state that the method works well with open-ended questions and when there is scarce historical data, which is the case for BCT in SCM.

Okoli and Pawlowski (2004) list certain advantages of Delphi studies when compared specifically to traditional survey studies. They are often used to study questions of high uncertainty and speculation meaning that a representative sample of the population could not satisfactorily answer the question and a group of experts might be more suitable. Further, it is claimed that expert judgments in groups are superior to individual answers and provide richer data through response revision through iterations and the possibility to make follow-up interviews.

There are certain aspects that could make an expert willing to participate in a Delphi study where they would not want to be a part of other studies. According to Okoli and Pawlowski (2004) : “(1) being chosen in a diverse but selective group; (2) the opportunity to learn from the consensus building; and (3) increasing their own visibility in their organization and outside.”. Furthermore, the experts can be situated in diverse locations as the Delphi method does not require them to travel (Vernon, 2009).

Gupta and Clarke (1996) also list disadvantages of the Delphi method compared to other scientific methods. There is a risk for sloppy execution, badly designed questionnaires, poor choice of experts, unreliable analysis of results, limited value of consensus and feedback and instability of results from consecutive Delphi rounds. There is also a weakness that the participants can, by giving certain answers, affect the result in ways that might favor them. It is a challenge to determine who is an expert and what separates an expert from a layman. There is also the issue that the feedback and anonymity can result in compromise rather than genuine consensus.

3.5.2 Rigor

According to Hasson and Keeney (2011) the Delphi method is often subject to criticism about its rigor and while this is acknowledged by many of its employers it is seldom addressed but rather just referred to as a weakness. They go on to explain that two key examples of challenges in establishing rigor are selecting the appropriate measurement and the continuing modification of the method. There are mixed opinions in the literature to whether the Delphi method should be considered, and hence evaluated, as a qualitative or quantitative method. Testing the rigor of the method has proven difficult because of the great variety within what is called the Delphi method. It is recommended to apply measures of rigor for both qualitative and quantitative methods on Delphi and the final result can be verified using other research methods to enhance confidence. It should be understood that the Delphi does not offer indisputable facts but a picture of a specific situation (Hasson and Keeney, 2011). Given a systems view approach this does not constitute a limitation. The Delphi method can specifically provide a systems approach through combining different areas of knowledge and different time frames (Ludlow, 1970).

An issue brought up early is the one of who to consider as an expert. There are many different criteria that could be used to try to judge a person’s expertise in an area, e.g. years of professional experience, self-appraisal or amount of relevant information the person can access (Brown, 1968). The general definition of an expert is “A person who is very knowledgeable about or skillful in a particular area” (Oxford Dictionaries, 2018). Different types of Delphi have aimed at using different persons as experts but all aim at using people knowledgeable in the area (Hasson and Keeney, 2011). There exists processes to ensure the best available experts are chosen, such as listing and contacting experts in order of expertise (Okoli and Pawlowski, 2004).

3.5.3 General method

As mentioned before, the Delphi method has seen use in many diverse areas and the method has seen many variations in order to better fit the area currently under investigation (Okoli and Pawlowski, 2004). Its use has shifted from the initial use by the RAND corporation to being a method that can combine knowledge and abilities of disparate groups in cases where there is much uncertainty (Stewart, 1987) and little previous research (Vernon, 2009). This goes well with the topic of the potential of blockchains in the supply chain because of the many uncertainties around it and as it is a new technology and situation.

According to Keeney et al. (2001) several types of Delphi methods exist and researchers often alter the method to fit; few researchers now use the exact same method and this is something the method is often criticized for. Keeney et al. (2001) list four common forms of Delphi often mentioned in the literature, but not further expanded on here, the "classic Delphi", "modified Delphi", the "policy Delphi" and the "real-time" Delphi. However, there are many more, all with differences in aim, type of experts, administration, number of rounds and design of round one. Even within a certain type there might be variations (Hasson and Keeney, 2011).

Delbecq et al. (1975, pp. 86-106) outline the general Delphi method. It can be described as an iterative process in which a group of experts' total knowledge is used to investigate a question. Essentially the Delphi method is a series of questionnaires the experts individually respond to and between every round the researchers aggregate and analyze the answers. The processed answers are used as a base for the next questionnaire. Usually the first questionnaire contains open-ended questions to map the initial opinions of the experts. In the next round the findings in round one is to be validated by the participants. In round three the experts get information of the answers of the rest of the group, often with some additional information, and asked to rank the opinions in some order. More rounds can be performed until consensus has been reached or has been deemed impossible to reach. According to Brockhoff (1975, p. 311) the best results of a Delphi study are as rule found after three rounds.

A common way to understand the extremes better is to ask the upper and lower quartile to not only give the rank as a number but to ask them why their response, and not the majority opinion, is correct (Rowe et al., 1991). Below, in Figure 6, the general outline of the Delphi process can be seen together with the outcomes from the different stages.

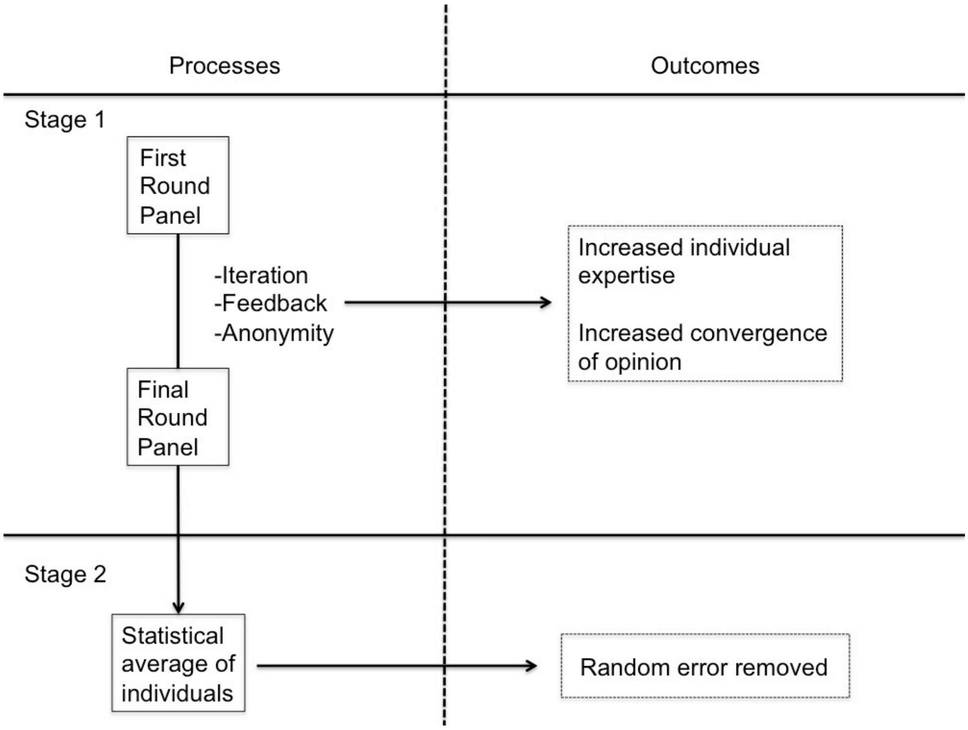

Figure 3.3: The process of a Delphi study. Adapted from (Rowe et al., 1991).

In this Delphi study, the procedure suggested by Okoli and Pawlowski (2004) was relatively closely followed. It was augmented with processes put forward by other authors and changes were made due to the constraints of this study. The main steps of the Delphi study was:

1. Selecting experts
2. Delphi phase 1, brainstorming
3. Delphi phase 2, ranking
4. Final results and report

In relation to Figure 3.3, phase 1 and phase 2 are mainly included in stage 1, while the last steps of phase 2 are included in stage 2.

3.5.4 Selecting experts

As suggested by Okoli and Pawlowski (2004) we divided the experts into panels. Having panels let us compare the perspectives of the different groups. In this study three panels are created: Supply chain experts, Academics and Blockchain experts. It was decided not to specify a certain research field necessary for academic participants but to include academics that have studied and shown interest in the intersection of BCT and SCM.

According to Dalkey and Helmer (1963) the panel size affects two important quality aspects, the group error and the group reliability. They performed experiments where the researchers knew the answers to the questions posed to the experts, showed that group error decreases as panel size increases. This shows that a larger panel comes closer to the true answer. Other experiments where the results of different expert panels were compared to see how much they differed also showed that group reliability increased as panel size increased. This shows that the risk that another composition of experts would come up with a different answer decreases as panel size increases. Both these effects are diminishing.

The aim of this study was to populate the panels with 15 respondents each, following the recommendations of Okoli and Pawlowski (2004) to use panels with 10 to 18 participants. Due to low response rates this was not accomplished. It was decided that each panel should contain at least seven respondents, following the recommendation of Linstone (1978, p. 296) who states that for smaller panel sizes accuracy falls sharply while it only increases slowly for larger panel sizes.

A knowledge resource nomination worksheet was prepared as per suggestion by Okoli and Pawlowski (2004). It is in essence a spreadsheet with the most important literature, organizations and disciplines. The idea was to categorize experts before identifying them to make sure that no knowledgeable and relevant group of experts was excluded. The identified categories, Supply chain experts, Academics and Blockchain experts, were populated with names found in the literature review, both from academic literature and from grey literature. Names were also added through other sources, mainly using search engines to search for organizations or individuals who had shown interest in the technology in terms of publications, conference talks, other speaking assignments or pilot projects.

After exhausting our own ideas, contacts were made with the identified experts. They were however not invited to participate in the actual study yet but informed about our on-going study, that they had been identified as experts, that we required basic biographical information on their qualifications and asked to provide nominations for more experts. The procedure was then repeated for the nominated experts until no new experts were nominated.

The initial idea was to rank the names of all experts independently, and from this ranking select the 15 experts to be included in this study. As the number of experts interested in participating in this study did not exceed 15 for any of the panels, this step was not performed. Instead all experts willing to participate in the study were invited. The exception to this is one expert who acted as the CEO of a company that was temporarily suspended from trading by the United States Securities and Exchange Commissions in 2017. When this was discovered it was decided to not to include the expert as his seriousness could be questioned.

In the invitation the study was explained more in depth, the procedures and the commitment required from participants. Participants were told that three questionnaires were to be completed and that the results would be presented in a short report and be part of a master thesis.

Figure 3.4 illustrates how the panels were formed.

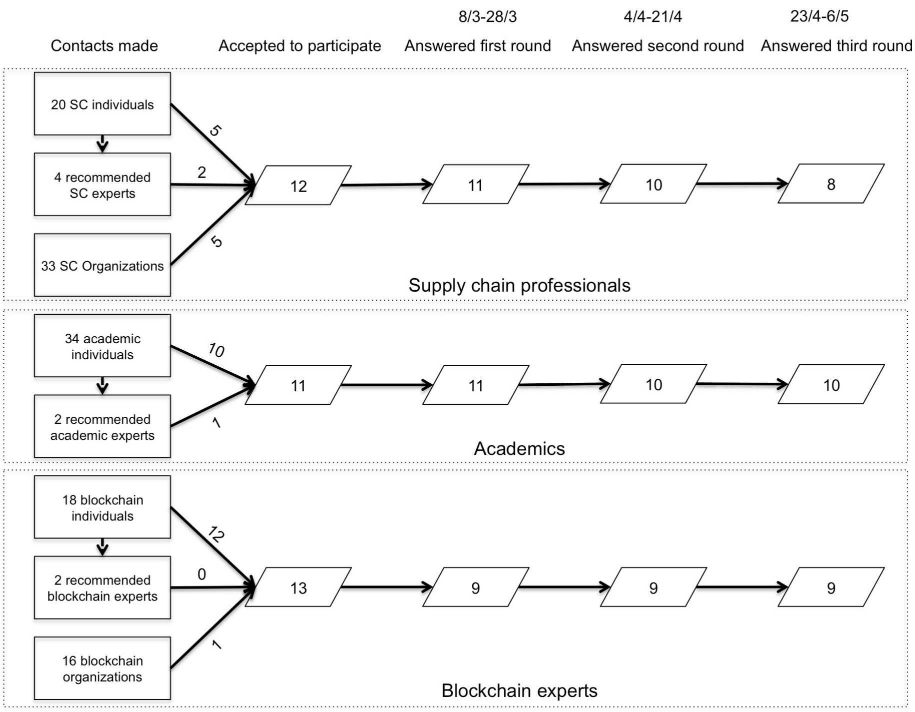

Figure 3.4: Progression of panel participants across the study.

Out of 129 approached experts, or organizations, 31 participated in the first round of the Delphi study. This gives an initial response rate of 24 %. This is slightly lower than the 30 % initial response rate that von der Gracht (2008, p. 48) found as being normal for Delphi studies. This could perhaps be explained by the fact that many organizations were approached, instead of only individuals.

Out of the 31 experts that participated in the first round, 27 completed all rounds. This gives a dropout rate of 13 %. This is lower than the 25-30 % drop-out rate described as normal by von der Gracht (2008, p. 48).

The participants who responded to the first questionnaire can be found in Table 3.7 (Supply chain experts), Table 3.8 (Academics) and Table 3.9 (Blockchain Experts). Each expert was asked to rate his or her knowledge of BCT and SCM on a scale from one to 10. The self-rating was not used to select experts or form groups but can act as an indication of the experts' level of knowledge in the two different fields.

Table 3.7: Participants in the Supply chain expert panel. Expertise in supply chain and blockchain is self-rated.

Title	Industry	Country	Supply chain expertise	Blockchain expertise
Senior Manager Digital Innovation	Chemicals	Germany	7	7
Market and purchasing manager	Steel	Sweden	7	5
Director of Group Transport	Food processing and packaging	Sweden	6	5
Material flow manager	Steel	Finland	9	2
Business consultant	Agriculture	Netherlands	7	7
Chief product officer	Supply Chain IT	Sweden	9	2
Managing Director	Management Consultancy	United Kingdom	10	2
CEO	Trade and development	Switzerland	8	8
		Median	7	5

Table 3.8: Participants in the Academics expert panel. Expertise in supply chain and blockchain is self-rated.

Title	Research field	Country	Supply chain expertise	Blockchain expertise
Associate Professor	Economics	France	6	9
Senior Scientist	Computer Science	Netherlands	8	8
Senior Scientist	ICT in Food supply chain	Norway	9	7
Senior Researcher	Logistics	Germany	9	6
Senior Scientist	Risk and resilience	Netherlands	8	6
Senior Lecturer	Logistics	Netherlands	8	7
Post-doc	Innovation & entrepreneurship	Sweden	2	9
Assistant professor	ICT	Netherlands	7	8
Research Associate	Digital Service Innovation	Germany	9	9
Research Associate	Logistics	Switzerland	8	7
		Median	8	8

Table 3.9: Participants in the Blockchain expert panel. Expertise in supply chain and blockchain is self-rated.

Title	Industry	Country	Supply chain expertise	Blockchain expertise
Founder and software developer	Blockchain	Netherlands	2	9
Principal Scientist	Manufacturing	Switzerland	6	10
Head of Platform Security Research	ICT	Sweden	2	9
Blockchain pioneer	Blockchain	Sweden	6	10
Consultant	Blockchain	Canada	8	9
CEO	IoT	Sweden	8	8
Developer	Blockchain	Sweden	3	8
CEO and Founder	Blockchain	Italy	1	8
Developer	IoT & Blockchain	Italy	9	9
		Median	6	9

Certain participants took part in the study but did not complete all three rounds. As they contributed to the results through providing answers and comments, their background and expertise is also presented in this report (see Table 3.10).

Table 3.10: Participants who answered the first questionnaire but dropped out of the study at a later stage. Expertise in Supply Chain and Blockchain is self-rated.

Title	Panel	Industry/Research Field	Country	Supply chain expertise	Blockchain expertise	Nr. of rounds
Digital officer purchasing	Supply chain experts	Automotive	Sweden	7	4	1
Programme coordinator	Academic experts	Supply chain management	Netherlands	9	5	1
Senior manager logistics	Supply chain experts	Steel	Sweden	9	2	2
Principal Supply Chain Management	Supply chain experts	Management consultancy	Germany	8	6	2

3.5.5 Data collection

This Delphi study was administered using online tools; a so-called e-Delphi. According to Cole et al. (2013) conducting an e-Delphi has certain benefits for the data collection. By allowing participants to reply anywhere and anytime the process was more convenient for the participants. From an administrative point of view the Delphi is simplified by using an e-Delphi because there is no need to send regular mails as in the classical Delphi and the process can be administered from the computer.

The questionnaires were created using Google Survey and panelists were informed every time a new questionnaire was active. The first questionnaire as well as the accompanying communication was tested on a number of persons. These people were not included as experts later in the study. This was based on a suggestion by Vernon (2009), to avoid problems with the questionnaire and make sure it was understood as intended. The two following questionnaires were made to keep logic, layout and terminology to ensure they would be understood as intended and to estimate the time needed to fill them out.

3.5.6 Minimizing non-response

Minimizing non-response in a Delphi study is critical, according to Hsu and Sandford (2007b). The reason for this is that the experts are chosen for their specific skills and can be hard to find. Even if dunning is used and slightly increases the response rate this can be impractical due to time constraints. Ultimately the response rate is linked to the quality and validity of the conducted study.

Hsu and Sandford (2007b) give some useful tips in order to increase response rate. They too recommend having renowned experts suggest other experts and even having them make first contact with these other experts. Contact should be direct and honest to make clear how they were identified as experts and why they are needed. In certain cases, experts made the first contact with the persons they recommended. In other cases, we were simply given contact details and made the initial contact ourselves.

Hsu and Sandford (2007b) further suggest setting clear deadlines and not give more than three extra days for panelists to respond after the deadline has passed. However, it is important for investigators to make contact and communicate that the experts' responses are valuable should no reply be given in time. In this study, the deadline for answering was set to eight working days and communicated when the round was launched. A first reminder was sent out after five working days. A second reminder was sent out to any participants who had not responded after eight working days, informing them that the deadline had been extended by two days and urging them to come back with their replies.

3.5.7 Phase 1: Brainstorming

In the first phase, the approach differed slightly from the one proposed by Okoli and Pawlowski (2004). Hsu and Sandford (2007a) states that it is both common and acceptable to have a first round with structured questions based on an extensive literature review. This modification is common when there is already usable and available basic research about the topic. Even though the subject of blockchain in supply chain is still new in an academic context, there exists some published literature. The experts were also given the opportunity to add issues and applications they considered important. Using the modified Delphi approach was deemed necessary due to the short amount of time available to complete the study in. Essentially, this first questionnaire aimed at validating the factors identified in the literature review. At this stage all panels are contributing to the same list since dividing them into panels at this stage would stifle creativity (Okoli and Pawlowski, 2004). The factors were grouped into categories of similar factors based on the literature review. Every factor was given a short explanation and experts were given the opportunity to suggest modifications to definitions they did not agree with. The experts were asked to state if they agreed that the described issues were issues that could be, at least partially, solved by using Pub-PL BCT. They were also asked to state if they believed the described applications to be suitable applications of permission-less BCT in SCM.

Hsu and Sandford (2007b) list some additional benefits of having a structured first round except for saving time. It decreases the dropout rate of experts otherwise only participating in the first open-ended part of the study. It also ensures that important statements are included that otherwise might have been omitted. Finally, many panel members appreciate a completed survey to respond to, rather than being

3.5.8 Phase 2: Ranking issues and applications

The results from the first round were incorporated into the second questionnaire as experts' motivations for discarding certain issues or applications are provided together with the experts' general view on them. Suggestions of other issues and applications were also incorporated together with provided motivations. The experts were then asked to rank the suitability of BCT to solve a specific supply chain issue could as well as the suitability of specific applications. As in Cole et al. (2013) , a five-point Likert scale was used ranging from total disagreement to total agreement. When measuring agreement five-point scales are common (Lefkothea and Efthimios, 2014). It has been shown that five-point scales have higher quality, reliability and validity than seven-point scales. Having fewer points than five would only make it possible to assess directions of attitudes and not the intensity (Melanie et al., 2013). Figure 3.5 illustrates the Likert Scale.

Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
1	2	3	4	5

Figure 3.5: Five-point Likert scale.

Chyung et al. (2017) states that a five-point Likert scale can be treated as an interval scale, enabling more statistical tools than could be used with a four-point ordinal scale. However, this is an on-going discussion and there are staunch supporters on each side. In this report it will be treated as an interval scale to allow for median ratings and statistical consensus measurements to be computed. It should however be noted that any median ratings between points on the Likert scale cannot readily be translated to a fixed level of agreement. Using (Chyung et al., 2017).

In questionnaire three, the experts are asked to answer the same questions as in round two. They are also provided with data on the median importance of every factor as calculated from the group's answer on the previous questionnaire (Rowe et al., 1991). In this study the experts were also provided with edited comments from the second questionnaire. This allowed experts to consider the argumentation of other experts on their panel. This process provides feedback and gives the chance for the experts to revise their answers, hopefully leading to increased consensus.

According to the literature, there are different ways to determine consensus. It has been suggested that the stability of the experts' answers should be checked through iterations, stability would then indicate consensus (Cole et al., 2013). This was not possible here due to time constraints. Instead the interquartile range (IQR) was chosen as a measurement of consensus. It is a measure of the dispersion of the median and the range consists of 50% of the answers. First, the median of the responses is calculated. The median of the data points below and above the median are then calculated, these medians are referred to as the lower and the upper quartile. The difference between these two quartiles is defined as the IQR[21]. Consensus has been achieved if the predetermined range has been fulfilled.

Using this measure of consensus has both strengths and weaknesses. It is very independent of the number of questions in the Delphi study and is not affected much by group conformity while it is more affected than most other measures in terms of number of experts in the study (Birko et al., 2015). The IQR is usually used in Delphi studies and is in general seen as an objective and rigorous way to determining consensus. Following the recommendations given by von der Gracht (2008, p. 56) the threshold IQR was set to one because of the use of a five-point Likert scale.

3.5.9 Final results and report

As suggested by Delbecq et al. (1975, pp. 105-106) a short final report was prepared presenting the results from every stage. The experts put work into the study and deserve to take part of the result. The final report contained a 10-page summary of the results of the Delphi study, and experts were informed that they could receive the final thesis if they were interested in more detailed results. The report was distributed three weeks after the final round of the Delphi study was concluded.

3.6 Research quality

3.6.1 Reliability and validity

To judge the quality of quantitative research, the terms reliability and validity are often used. Reliability generally refers to the extent to which results of measurements are consistent over time. In quantitative research, replicability of results is a critical aspect for judging the quality and trustworthiness of the research (Golafshani, 2003). Drost (2011) states that validity relates to the question of whether the researcher has measured what was intended to measure in the first place. It is possible to deconstruct the concept of validity into different types of validity. Internal validity looks at the validity of the research itself, e.g. if the discovered relationship between variables is causal. Construct validity deals with the validity of the translation from a construct, e.g. concept or idea, to an operationalized form. External validity looks at the generalizability of the study to other contexts (Drost, 2011). The concepts of reliability and validity can be illustrated using shooting targets (see Figure 5). Target A represents good validity but poor reliability as shots are scattered, but an average comes close to the center point. Target B represents poor validity and good reliability

---

[21] Microsoft Excel was used to calculate these values. To calculate quartiles, QUARTILE.EXC was used. This differs from QUARTILE.INC in that it excludes the median value when calculating the upper and lower quartiles. This gives a slightly larger IQR than when using QUARTILE.INC and therefore represents outliers in a better way.

as shots are grouped together, but far from the center point. Target C represents both good reliability and good validity.

Figure 3.6: Shooting targets representing the concepts of validity and reliability. (Swanson, 2014)

Keeney et al. (2001) state that studies have been conducted comparing Delphi studies conducted at different times and concluding that the result can be considered reliable. Further they say that with a representative expert panel of the knowledge area in question, validity can be assumed. Validity can also be ensured by letting the participant give feedback on groupings and definitions given by the researchers (Okoli and Pawlowski, 2004). Participants of this study were asked to comment on the definitions and terminology used in this Delphi study.

For qualitative research, certain adaptions of these terms have to be made. Lincoln and Guba (1985, pp. 294-300) suggest the concept of trustworthiness as more applicable to quantitative studies. There are a certain number of ways that a qualitative researcher can achieve trustworthiness: credibility, transferability, dependability and confirmability.

3.6.2 Credibility

Credibility is related to the truth value of the findings, or that the results of the qualitative study are representative of the multiple realities that shaped them (Lincoln and Guba, 1985, p. 296). According to Lincoln and Guba (1985, p. 305), one important tool for achieving credibility is triangulation. They list several triangulation techniques: using multiple data sources, multiple methods, multiple theories and even multiple investigators. Through triangulation the validity of results can increases if they are reconfirmed using different approaches.

Triangulation in this study was achieved using a mixed methods research approach. Gallivan (1997) defines mixed methods research as research where at least one data collection method is quantitative and at least one data collection method is qualitative. It further requires both qualitative and quantitative data to be presented analyzed. The data collection methods used in this study are primarily qualitative, but the introduction of the Likert scale in later Delphi rounds add quantitative data to the research.

Another technique to achieve credibility is to continuously expose participants in the study to the developing narrative, so that they can confirm or contradict its validity. Lincoln and Guba (1985, p. 314) refer to this technique as member checking. Member checking was performed using the Delphi study, as the experts were exposed to the developing narrative between each round. They were also invited to give comments and feedback on aspects they disagreed with.

3.6.3 Transferability

The concept of transferability describes the extent to which the results of a qualitative study are transferable to a more generalized context (see external validity in quantitative research). Here, Lincoln and Guba (1985, p. 316) state that the role of the researcher is to provide a thick description, so that appliers of the results can Generalizability is an issue with the Delphi study, as it only provides a snapshot of the expert opinion at a specific moment in time. The generalizability of the findings of this study is therefore limited due to its design.

3.6.4 Dependability

Lincoln and Guba (1985, pp. 316-318) argue that, in a qualitative setting, validity is dependent of reliability and cannot exist without it. They go on to argue that dependability can be assumed to exist if credibility can be proved, but also provide techniques for assuring dependability separately. Stepwise replication includes two research teams following exactly the same research design. An external auditor can also be brought in to examine the processes and products of the research study. Due to limitations in time and resources, none of these steps could be performed. Dependability has therefore been deemed sufficiently strong if credibility can be demonstrated.

3.6.5 Confirmability

Lincoln and Guba (1985, p. 319) note that confirmability is related to the audit proposed above but rather than bringing in an external audit, the researchers develop a clear audit trail in which they document the research activities carried out. This allows readers to judge the methods employed and in turn the trustworthiness of the results. Confirmability of this study is increased by transparently sharing documents that laid the foundation of the results.

3.6.6 Bias

Bias in systematic literature reviews

To ensure validity in a systematic literature review, researchers should be aware of the possibility of bias and know how to prevent this. Felson (1992) identifies three biases in meta-analytical analysis: bias in finding studies, bias in selecting studies and bias in obtaining data.

Bias in finding studies: Publication bias relates to the fact that studies without statistical significance, or with results contradicting accepted and widespread knowledge have a larger probability of not being published. Searching for unpublished literature among working papers and dissertations can remedy this bias (Felson, 1992). Retrieval bias relates to the bias in finding published studies. Felson (1992) suggests a rigorous, computerized database search to avoid this. Grey literature has been included in this study, in the form of whitepapers. A rigorous search of several databases has also been performed to increase the chance of finding all relevant studies.

Bias in selecting studies: Inclusion criteria bias occurs when inclusion criteria exclude articles that could be relevant for the study. It is difficult to avoid, as avoidance requires a large knowledge of the field, a knowledge that is hard to acquire without a systematic literature review. The researcher should try to develop inclusion criteria without taking already known results and publications into account (Felson, 1992). Selector bias occurs when no inclusion criteria exist and selection is made subjectively by the reviewer (Felson, 1992). The inclusion criteria used in this study can be assumed to be free from bias, as the authors have not performed any previous research in the field.

Bias in obtaining data: Extractor bias occurs when data is extracted in an inaccurate way. The use of pre-developed extracting forms minimizes the effect of this bias (Felson, 1992). Expectancy bias occurs when research is influenced by the researcher pre-existing views and expectations. The use of blind synthesis using multiple researchers can reduce this bias (Durach et al., 2017). Pre-developed extraction forms were used in this study and can as mentioned before be found in Appendix C. It was not possible to perform blind synthesis, due to lack of research.

Bias in Delphi studies

Winkler and Moser (2016) list a number of biases that can affect Delphi studies and how these biases can be countered. The description of the five biases listed below is based on their work.

Framing: Framing refers to the effect that the presentation of a certain phenomenon can have on people's views of that phenomenon. Questions and statements in the Delphi questionnaires should be formulated in a neutral manner so that they are not framed in a positive or negative way. Furthermore, framing in the context of Delphi studies can also refer to the effect of the pre-study attitudes, or frames, of participants. More specifically, participants who share the same pre-study attitudes might amplify these attitudes. In the case of this study, it could for example be that many participants who are slightly negative to the prospects of BCT in supply chain could amplify each other's negative views so that the final result is far more negative than any of the participants original attitudes. It is suggested to select a heterogeneous group of panelists to avoid this effect, as diverging pre-study attitudes can neutralize the aforementioned effect. It can also be useful to include individuals who are known to have a maverick perspective of the issues to be investigated. Finally, it is also suggested to avoid selection procedures where experts can recommend other experts as this may cause groupings of individual panelists sharing the same attitudes. Great care was put into selecting experts for the panels. In the first round, the wide range of backgrounds of experts guaranteed heterogeneity. In the second and third round, when responses were evaluated on a panel level, it was important to create panels with a variety of viewpoints. Certain experts included where known to hold extreme positions and added a maverick perspective to the study. Despite the fact that allowing experts to recommend other experts increases the risk for homogenous groups, it was judged that it was more important to get sufficiently large panels to increases reliability of the results.

Anchoring: Anchoring occurs when the final estimate of a value is influenced by an earlier, known value of the same variable. This is more prominent in future-oriented Delphi studies where participants are asked to forecast the value of a variable in a certain amount of years' time, with today's value being known. Once again, a heterogeneous group of panelists is preferable to counter this bias. It can also be effective to warn participants of the possible effects of anchoring. The heterogeneity of the panels in this study has already been discussed. No warnings were administered to the participants as no clear anchors were identified.

Desirability bias: Desirability bias occurs when panelists overestimate the probability of desirable future events. In the context of this study, it could be that participants are excited about the prospects of BCT and therefore overestimate its usefulness in a supply chain setting. As before, a heterogeneous group containing many different points of view can neutralize this effect. The iterative process of the Delphi study also helps counter this bias as experts are exposed to the views of other panelists and therefore forced to reconsider.

Bandwagon effect: The bandwagon effect occurs when a panelists view conforms to the majority, solely based on information that this view is the majority view. It is recommended to not include statistical feedback as this incentivizes consensus rather than accuracy. It is further recommended to filter argumentation from other panelists in the feedback, e.g. through removing duplicates in order not to disclose how many people share the same arguments. The comments and argumentation from participants of this study was carefully filtered before being presented as feedback and duplicates were removed. Results of the previous round were however statistically presented to facilitate consensus and encourage argumentation.

Belief perseverance: Belief perseverance occurs when a panelist overestimates his own judgmental capabilities while underestimating the capabilities of other panelists. The anonymity of the Delphi study both counters and enforces this bias. As respondents are anonymous, they can easily change opinions without losing their face. However, it may also be hard to accept the argumentation of other panelists when they are anonymous. One method to counter this effect is to filter out, and select, high-quality comments to be used as feedback. The comments and argumentation from participants of this study was carefully filtered, and comments that were difficult to understand or unspecific were removed.

Sinha et al. (2011) add two other potential biases to be considered when conducting a Delphi study.

Bias from pre-determined list of issues: It is suggested to begin the Delphi study with an entirely open-ended round in order to avoid potential biases from a pre-determined list provided by the researchers. The first round of this was not completely open-ended. The reasoning for this has been developed earlier in this chapter.

Attrition bias: Participants with minority opinions might be more prone to drop out of Delphi study, causing a false consensus in the final results. Strategies to avoid this includes only inviting people who respond to an initial invitation to participate, as they are more likely to be committed to the entire study. The importance of answering all questionnaires should be communicated to the panelists so that they are aware that dropping out lowers the reliability of the results and might enforce the majority opinion. If people drop out it should be transparently described in the results so that readers can judge the reliability of the results in the light of dropouts. A pre-study invitation was used in this study, and only experts who responded to this were invited to participate in the study. The importance of answering all questions was also stressed throughout the study. For transparency, the number of participants that dropped out at each stage has been clearly presented in this report so that readers can judge on what foundations conclusions from the study were made.

3.6.7 Summary of study quality

The suggested measures to take in order to strengthen the quality of study are summarized in Table 3.11. For each measure, it has been noted whether or not it was performed in this study. If a certain measure was not taken, a short reasoning to why it was not taken is given.

Table 3.11: Measures for ensuring quality of study, Brief explanations to why are provided when the measure was not carried out.

Measure	*Performed?*	*If no, why?*
General		
Triangulation	Yes	
Member checking	Yes	
Thick description	Yes	
Audit Trail	Yes	
Stepwise replication	No	Lack of resources.
External audit	No	Lack of resources.
Literature Review		
Broad database search	Yes	
Use of inclusion criteria	Yes	
Use of unpublished literature	Yes	
Use of extraction forms	Yes	
Blind synthesis	No	Lack of resources.
Delphi study		
Pre-study invitation	Yes	
No recommendation of experts	No	To increase panel size
Create heterogeneous panels	Yes	
Open first round	No	Time constraints and increased response rate
Not distribute statistical feedback	No	Encourage argumentation and facilitate consensus
Distribute filtered feedback	Yes	

4. Literature review

This chapter presents the results of the literature review. A descriptive analysis and a thematic analysis are presented for scientific articles and whitepapers, separately. The identified issues and applications are then presented together, with links to the SCOR framework being made.

4.1 Descriptive analysis of scientific articles

4.1.1 Articles

A total amount of 228 articles were retrieved in the literature search. Initially, 97 duplicates were removed. The pre-determined inclusion criteria were applied to the remaining articles through reviewing title, abstract, keywords and publication. This gave 34 articles to be included, of which a further nine were removed due to not meeting inclusion criteria after having read the full article. The reference lists of the 25 remaining articles were reviewed, which yielded three new candidates of inclusion, of which one was deemed to fulfill the inclusion criteria. For an overview of the process, see Figure 4.1.

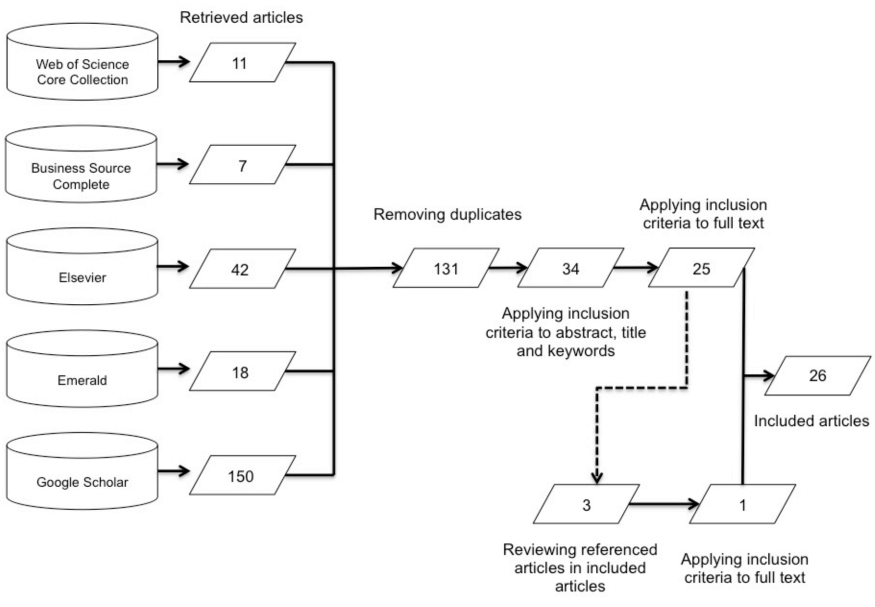

Figure 4.1: Process chart describing the steps of selecting scientific articles for inclusion in the literature review. The numbers represent the number of remaining articles at each stage.

Table 4.1 illustrates which inclusion criteria were not met by the excluded articles. The total numbers in this table adds up to 108, which is more than the 105 that were excluded from this study. This is because some articles failed several exclusion criteria.

Table 4.1: Reasons for exclusions of articles. The number represents how many articles failed to meet up to that specific inclusion criterion.

	Not in scientific journal	*Not in English*	*Published before 2008*	*Did not treat BCT and SCM*
Number of articles	25	1	0	82

The 26 articles that were included in the review are listed in Table 4.2.

Table 4.2: List of reviewed scientific articles.

Number	*Title*	*Reference*
1	Blockchain ready manufacturing supply chain using distributed ledger	Abeyratne and Monfared (2016)
2	Blockchain Platform for Industrial Internet of Things	Bahga and Madisetti (2016)
3	Blockchain and its Scope in Retail	Chakrabarti and Chaudhuri (2017)
4	Blockchains and Smart Contracts for the Internet of Things	Christidis and Devetsikiotis (2016)
5	Managing Online Supply chain finance Credit Risk of "Asymmetric Information	Deng and Chen (2017)
6	The technology of trust: How the Internet of Things and blockchain could usher in a new era of construction productivity	Heiskanen (2017)
7	Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology	Kennedy et al. (2017)
8	IoT security: Review, blockchain solutions, and open challenges	Khan and Salah (2018)
9	Blockchain's roles in strengthening cybersecurity and protecting privacy	Kshetri (2017)
10	Blockchain's roles in meeting key supply chain management objectives	Kshetri (2018)
11	How the Blockchain Revolution Will Reshape the Consumer Electronics Industry [Future Directions]	Lee and Pilkington (2017)
12	Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing	Li et al. (2018)
13	Visibility and digital art: Blockchain as an ownership layer on the Internet	McConaghy et al. (2017)
14	Time-temperature abuse in the food cold chain: Review of issues, challenges, and recommendations	Ndraha et al. (2018)
15	Trading Real-World Assets on Blockchain An Application of Trust-Free Transaction Systems in the Market for Lemons	Notheisen et al. (2017)
16	Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems	O'Leary (2017)
17	Trustworthy data-driven networked production for customer-centric plants	Preuveneers et al. (2017)
18	Runtime verification for business processes utilizing the Bitcoin blockchain	Prybila et al. (Forthcoming 2018)
19	Challenges & Opportunities for Blockchain Powered Healthcare Systems: A Review	Rabah (2017)
20	Blockchain technology: A panacea or pariah for resources conservation and recycling?	Saberi et al. (2018)
21	Blockchain technology in the chemical industry: Machine-to-machine electricity market	Sikorski et al. (2017)
22	Blockchain Technology Review and Its Scope	Sharma (2017)
23	A cyber-anima-based model of material conscious information network	Shen et al. (2017)
24	Blockchains as security-enabler for industrial IoT-applications	Skwarek (2017)
25	Future applications of blockchain in business and management: A Delphi study	White (2017)
26	Blockchain Technology Adoption Status and Strategies	Woodside et al. (2017)

4.1.2 Publication year

All included articles were published between 2016 and 2018. The majority of all retrieved papers were also published in these years, with only a few outliers (see Table 4.3). This reflects the novelty of the field and goes hand-in-hand with Gartner's view of blockchain in the supply chain as being on the rise (van der Meulen and Pettey, 2017).

Table 4.3: Publication years of scientific articles retrieved and included in the literature review.

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Included articles	-	-	-	-	-	-	-	-	2	20	4
Retrieved articles	1	-	1	-	-	-	1	1	13	94	18

4.1.3 Geographical spread

The authors of the included articles are affiliated with a wide range of research institutes. Table 4.4 lists the number of articles where at least one of the authors was affiliated with a research institute in the specific region. In parentheses, the number also includes authors without any clear affiliation to a research institute, but with affiliation to another organization in the region. In the included literature, these authors had an industry background either as consultants or as founders of a blockchain-based company.

Table 4.4: Geographical spread of publications. The table presents the number of articles with at least one author from the specific region. Figures when authors without academic affiliation are included are displayed in parentheses.

	North America	Europe	Asia	Africa	Oceania
Number of articles	8	11 (13)	8 (9)	1	0 (1)

4.1.4 Research methods

Out of the included articles, six described detailed blockchain applications for use in the supply chain. These applications were designed by the authors of the articles. Another six performed a case study, five of which were single case studies. Twelve articles were reviews, although rarely structured and transparent in terms of search methods and inclusion criteria. Most of the reviewed literature in these reviews was not published in peer-reviewed journals, demonstrating the lack of published literature in this field. This also meant that very few relevant articles for this study could be found in literature reviews performed in the past. One Delphi study was included and one article combined an environmental analysis using the PESTEL framework with a text analysis of Annual Reports and a financial analysis of the blockchain industry. Many researchers seem to want to present a current overview of the field, perhaps due to the low level of real-world implementation or to introduce readers to an unfamiliar topic.

4.1.5 Field of publication

Out of 26 included articles, 10 were published in journals focusing on Computer Science, Software Engineering or Information Systems. Another four were published in publications concerning Engineering Science in general. Three articles were retrieved from journals in business and economics while the remaining articles were retrieved from industry-specific journals such as *Applied Energy*, *Food Control* and *Construction Research & Innovation.* The pattern seems to reveal that interest for the subject of BCT in SCM in the academic world has been higher on the technology side of the field. This mimics the result of White (2017) when conducting a review of blockchain applications in a more general business environment. Publications are also common in industry-specific publications, demonstrating use-cases and application for that specific industry. Given that blockchain is a new, complex technology it is reasonable to assume that research will primarily be aimed at the technological community. Also given the hype surrounding certain applications of the technology in the supply chain it is reasonable that publications with close connections to concerned industries want to look into these applications. As managerial adoption and understanding of the technology progresses, it is probable that scientific publications on a more general supply chain level will follow.

4.1.6 Distinction between permissioned and permission-less blockchains

14 out of 26 articles did not make a distinction between permissioned and permission-less blockchains. The authors of this study believe that such a distinction is necessary to fully evaluate the benefits of applications as the two types have different characteristics. The fact that more than half of the included articles fail to make this distinction strengthens the case for this study of Pub-PL BCT.

4.1.7 Quality

Quality was varying; impact factors of included journals ranged from 0.386 (*International Research Journal of Engineering and Technology*) to 7.5 (*Applied Energy*). When reviewing the quality on an article-level, five articles were flagged as being of low quality while others ranged from medium- to high-quality. In accordance with general practice, quality was not used as an inclusion criterion. Filtering out only high-quality articles would also give a significantly smaller sample.

4.2 Thematic analysis of scientific articles

4.2.1 Issues

Issues that were identified by the scientific articles as being possible to solve using BCT are presented below. They have been divided into four main issues: transparency, visibility, efficiency and security. Definitions and variations of these issues are presented under their respective header.

Lack of supply chain transparency

The concepts of supply chain transparency and supply chain visibility are linked and might lack a clear distinction. It should be noted that no clear definition of the distinction exists and that the terms are often used interchangeably. In this report, the distinction provided by Dr. Shay Scott of the University of Tennessee is used: "Visibility provides a company with knowledge of activities across its supply chain; transparency is what and how it communicates that knowledge to customers, partners, and stakeholders" (Inbound Logistics, 2017) . In this study, the term transparency has been used to describe information sharing with external stakeholders such as end customers, financial institutions and regulators. Visibility is instead used to describe information sharing between supply chain partners.

Lack of transparency is described as a supply chain issue in several articles. They describe a growing trend among consumers, demanding more information about the products they buy (Abeyratne and Monfared, 2016; Chakrabarti and Chaudhuri, 2017; Kshetri, 2018; Lee and Pilkington, 2017). This could be information on ethical conditions, product sustainability or quality. To the extent that this information exists today, it is collected, aggregated and verified by third parties such as certification bodies, who in turn might not be fully transparent about their methods (Abeyratne and Monfared, 2016). One of the experts in the Delphi study of (White, 2017) stated that BCT could help bring transparency to these types of certification systems.

Notheisen et al. (2017) describe the Nobel-prize winning example of Akerlof (1970) and how information asymmetry negatively affects the market for used cars in Denmark. As Akerlof (1970) described; when the seller knows more about the true quality of the car than the buyer, the buyer is likely to base his value estimate on an average value of all cars on the market. This will drive high quality cars out of the market and eventually cause the market to collapse. This is referred to as adverse selection and illustrates the possible effects of low transparency towards customers. Notheisen et al. (2017) go further to define three characteristics of issues that can be resolved by BCT: multiple actors with conflicting interests, asymmetric distribution of information and a system into which at least two conflicting parties can enter data.

Apart from customer demands, regulatory bodies can also demand increased transparency through directives, e.g. Waste Electrical and Electronic Equipment Directive (Saberi et al., 2018).

Other stakeholders such as financial institutions might also have an interest in increased transparency. Deng and Chen (2017) describe the online Supply chain finance (SCF) market in China. To define SCF, the definition proposed by the Supply chain finance Forum is used: "Supply chain finance is defined as the use of financing and risk mitigation practices and techniques to optimize the management of the working capital and liquidity invested in supply chain processes and transactions" (Global Supply Chain Finance Forum, 2016). Deng and Chen (2017) focus on the situation where a financial institution provides financing to supply chain actors. Small and medium-sized enterprises, acting as suppliers in China, are generally opaque and financial institutions either don not have access to records and documentation, or there is a high risk that these are forged or manipulated. This is related to the concept of moral hazard, a situation where one actor bears the risk of another actor's actions (Krugman, 2009, p. 62). In this case, the financial institutes bear the risk of the suppliers that have been granted credit.

Lack of supply chain visibility

McConaghy et al. (2017) stated that data is critical for supply chains to survive. However, most companies lack information on the activities of their second and third tier suppliers (Abeyratne and Monfared, 2016). Kshetri (2018) gave the specific example of the 2015 E. Coli outbreak at Chipotle Restaurants and blames this on poor upstream visibility. Downstream visibility can also be poor, as Rabah (2017) noted in the case of poor point-of-sales visibility for pharmaceutical companies in African markets. Panel members in White (2017) stated that BCT could be the first opportunity for real SCM information tracking.

Prybila et al. (Forthcoming 2018) state that collaborative processes in a supply chain lack trusted end-to-end verification methods. Collaborative processes consist of activities that different supply chain actors are responsible for carrying out. In a supply chain, one actor rarely controls the entire process, as process ownership is instead passed from one actor to the other. Without a trusted verification method, it is difficult to detect and punish actors who fail to perform their activities as stipulated in the contract. This might decrease the willingness to participate in these types of collaborative processes.

A related concept to supply chain visibility is traceability; defined by the authors as the ability to track a product's flow throughout the production process and supply chain. Shipment tracking is brought up as an important retail supply chain issue by Chakrabarti and Chaudhuri (2017) and Sharma (2017). Christidis and Devetsikiotis (2016) note that shipment information is generally stored on the individual actors separate databases, with the possibility of inconsistencies restricting traceability. Ndraha et al. (2018) provide the example of temperatures in food transportation, something that is often specified in contracts but is hard to monitor.

Low supply chain security

Closs and McGarrell (2004) define supply chain security management as "the application of policies, procedures, and technology to protect supply chain assets from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain." In this report, the term contraband is interpreted in a wider sense so that it includes counterfeited goods.

The increased use of IoT-devices in industrial settings, related to the popularity of Industry 4.0 and smart manufacturing, has led to an increased attack surface for malicious users (Preuveneers et al., 2017). Up until now, security has been maintained through keeping security mechanisms hidden from other parties, with a drawback that once weaknesses are discovered by outside parties they can be exploited through a single point of failure (Kshetri, 2017). The security mechanism of BCT is instead public but does not have a single point of failure due to its decentralized structure (Kshetri, 2017). Both Khan and Salah (2018) and Skwarek (2017) note that IoT-devices have small computational capabilities, as energy-consumption must be kept at a minimum. This means that on-board security mechanisms are weaker than those found in regular computers, and the devices are therefore more vulnerable for attacks. Woodside et al. (2017) make the broader statement that BCT can protect the supply chain from malicious attacks, but they are referring to the private blockchain implementation of IBM.

Another supply chain security issue is counterfeiting. A panel member in White (2017) proclaimed that BCT could help overcome the issue of product authenticity. Kennedy et al. (2017) discuss how additional manufacturing allows counterfeiters to manufacture machine parts that are visually indistinguishable from the original but do not share the material properties. Rabah (2017) also stated that counterfeiting is weighing down the medical drug supply industry.

Low supply chain efficiency

Efficiency is defined as “the minimum use of resources […] for achieving optimal results” (Kusrini et al., 2014). As efficiency can be increased through using fewer resources to accomplish the same output, non-value adding work and the need of trusted intermediaries are issues that the reviewed articles consider. O'Leary (2017) describes the need for accountants and other trusted intermediaries in the supply chain while Bahga and Madisetti (2016) stress the need of such intermediaries in a cloud-based manufacturing system. Non-value adding work in the form of administration and quality control is a burden to the construction industry (Heiskanen, 2017), food industry (Kshetri, 2018) and electricity trading (Sikorski et al., 2017).

A summary of the identified issues and the articles they were featured in can be seen in Table 4.5

Table 4.5: Identified issues and the articles in which they were described. Articles are referenced using the assigned numbers from Table 4.2.

Issue	*Article*
Lack of supply chain transparency	
Transparency towards customers	1, 3, 10, 11, 15, 25
Transparency towards regulators	20
Transparency towards financial institutions	5
Lack of supply chain visibility	13, 18, 25
Lack of upstream visibility	1, 10
Lack of downstream visibility	19
Lack of traceability	3, 4, 14, 22
Lack of supply chain security	26
Security of IoT-devices	8, 9, 17, 24
Counterfeiting	7, 19, 25
Low supply chain efficiency	
Need for trusted intermediaries	2, 15
Non-value adding work	6, 10, 21

4.2.2 Applications

A few articles also presented more specific applications of the BCT. Presentation of applications ranged from describing pilot projects or proof-of-concepts in the real world to proposing applications designed by the authors themselves. Some authors did not distinguish between permissioned or permission-less blockchains and therefore did not describe the applications as based on one or the other. When possible, the characteristics of the blockchain are presented together with the application.

Proving provenance

Among the applications identified by Kshetri (2018) was the certification of authenticity and origin of diamonds. A certificate of authenticity and origin is issued and secured in the blockchain. Consequent transactions are then registered on the blockchain, allowing for end-consumers to verify the full transaction history of a specific diamond and connect it with its certificate of authenticity. Kshetri (2018) does not specify the type of blockchain, although the company behind the application, Everledger, state that they run on a public/private-hybrid blockchain (Everledger, 2017).

Abeyratne and Monfared (2016) designed a supply chain wide blockchain application that would allow consumers to access transparent information on provenance and certifications for the raw materials in their products. This application also had many other uses and is therefore presented more in detail under the next heading.

Improving traceability

Abeyratne and Monfared (2016) designed an application, built on the Ethereum blockchain, for the manufacturing supply chain. It allows suppliers, manufacturers, certification bodies and customers access to data about the product life cycle. In the case of certification, the possibility to remain anonymous is removed, as certification bodies must be able to provide transparent information on the certification process. The blockchain could also be regarded as semi-private as all parties do not have the same read/write permissions. As the product progressed along the supply chain, smart contracts were used to allow current product owners to add data. Each actor would have access to different data, pre-defined by the rules of the blockchain. Information such as ownership, location, environmental impact and the time when a certain activity was carried out could be registered on the blockchain. This data could be entered manually or transmitted from devices such as GPS trackers. To illustrate their application, the authors provided an example of the supply chain of a cardboard box. The supply chain extended from forestry to paper manufacturers, packaging manufacturers, filling plants, distributors, retailers, and waste recyclers. The specific benefits in this supply chain related to certifications of raw materials, information on raw materials included in the product, tracking products in distribution and closing the loop through tracking the use of recycled material.

Christidis and Devetsikiotis (2016) described the design of a blockchain network where the transfer of goods between seller, transporter and buyer can be secured on the supply chain. This could be done through digital signatures but could also be done using IoT devices that, for example, detect when a product arrives at a warehouse and automatically adds a transaction on the blockchain. The authors also provided a more developed view on the possibility of connecting the transfer of a physical asset (e.g. shipping container) to the transfer of a digital asset (e.g. cryptocurrency token), with the digital asset mirroring the physical asset. These applications are not specific for permissioned or permission-less blockchains and the authors did not take a stance, acknowledging both configurations.

Improving business process management

Prybila et al. (Forthcoming 2018) investigated an application of BCT in Business Process Management Systems. The documentation and verification of performed tasks in a B2B-environment was deemed an interesting use-case for BCT. The authors' prototype was based on the Bitcoin blockchain and allowed process owners to hand over the process to supply chain partners assigned with carrying out certain tasks. The handover was made through transactions of tokens containing metadata on the process to be carried out. The connection to the Bitcoin blockchain allows processes and the completion of tasks to be stored in a verifiable manner. Although the authors noted that long transaction times are an issue with this approach, they deemed that supply chain and logistics processes are exemplary use-cases, as the tasks tend to be more time-consuming. The envisioned application is illustrated in Figure 4.2 as three firms sharing a process. Tasks are handed between actors and information on who performs which task, when it was handed over and when it has been performed is posted on the blockchain.

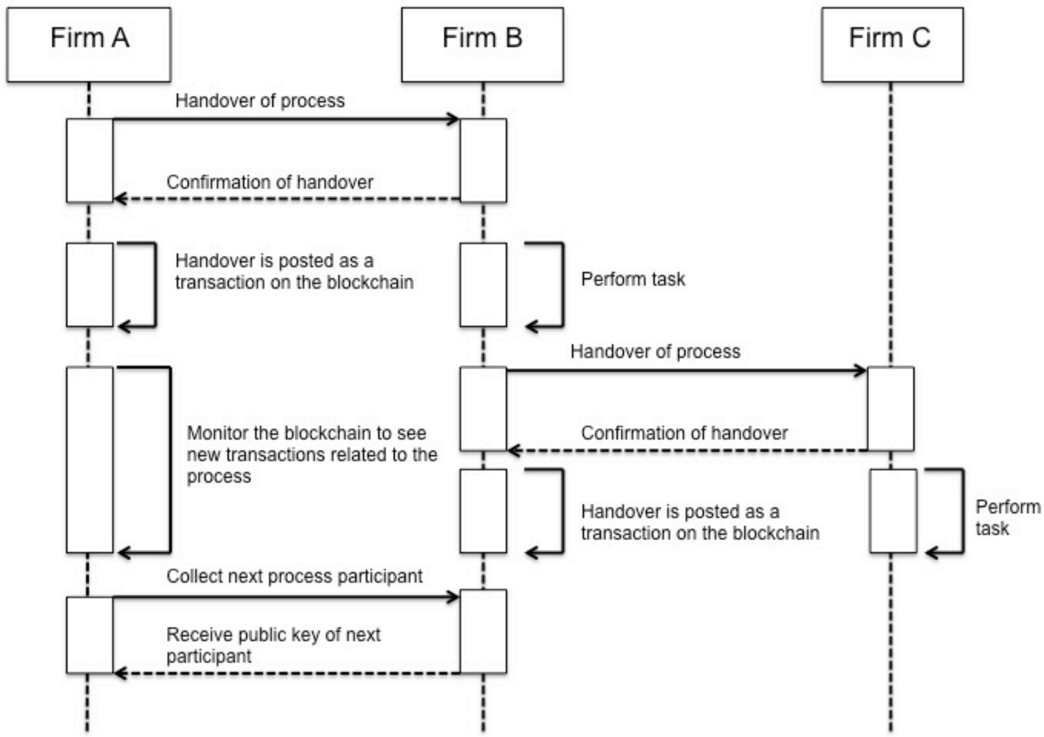

Figure 4.2: Process handover and monitoring as envisioned by Prybila et al. (Forthcoming 2018). Adapted from Prybila et al. (Forthcoming 2018).

Monitor cold-chain transportation

In his study, Kshetri (2018) describe the case of cold-chain transportation of pharmaceuticals. To comply with current regulations, all shipments of pharmaceuticals need to be done by expensive refrigeration trucks. It is however not necessary from a product quality perspective to transport all products at the low temperatures in the refrigeration truck. Some products are what is referred to as ambient products, that can be stored in 15-25 °C. It is, however, necessary to prove that products were not exposed to higher temperatures for a longer period of time throughout the transportation and refrigeration trucks are therefore used anyway. Using trusted sensors that report the temperature to the blockchain could create a trusted record that products were not exposed to high temperatures and remove the need of using costly refrigeration trucks. The application described by Kshetri (2018) was piloted by the Swiss start-up Modum, using the public Ethereum blockchain. Cold-chain transportation is not exclusive to pharmaceuticals, as Kshetri (2018) points out in the case of monitoring the temperature of seafood during transportation. Intel have provided a demonstration of how this could be achieved using blockchain infrastructure (Kshetri, 2018).

Issue targeted recalls

Kshetri (2018) provides the example of Walmart's partnership with IBM, which focused on the ability to quickly identify the source of contaminated food and issue a targeted recall of these products. Using a private blockchain to store all transactions allows for near-instant traceability, reducing the time needed to trace the origins of a product from days to minutes. Instead of having to recall an entire product-line, Walmart could identify the source of the contamination to the lowest possible level, e.g. a specific farm, and make a much more targeted recall. Targeted recalls were also brought up as a possible application in the healthcare industry (Rabah, 2017), without specifying the type of blockchain, and for the manufacturing industry (Bahga and Madisetti, 2016), utilizing a public and permission-less blockchain.

Anti-counterfeiting

Kennedy et al. (2017) present an application for fighting counterfeiting of parts produced using additive manufacturing technologies. In each part, a specific chemical signature is introduced in the material. In this case, the chemical signature consisted of a certain fluorescent emission. This signature was then posted on the permission-less Ethereum blockchain. A QR code referencing this blockchain transaction was printed on the part. Scanning the QR-code allowed for a receiving company to instantly check the authenticity of the part. The application also allowed for changes in ownership to be registered, creating a transparent chain of custody. Kshetri (2018) also presented an application in anti-counterfeiting, once again developed by Everledger. This time, BCT in combination with tamper-evident RFID-tags was used to prove authenticity of fine bottles of wine. The RFID-tags are attached to the cork to notice any attempts of refilling bottles with a cheaper product. Any attempt of this would be logged on the blockchain, as would the entire transaction history of the bottle.

Provide IoT security

A number of articles proposed BCT as an infrastructure for countering security threats to IoT-devices in an industrial setting. Preuveneers et al. (2017) provided a private blockchain protocol for an IoT network enabling communication between trustworthy nodes while ignoring malicious nodes. A private blockchain was chosen due to high transaction costs associated with public blockchains running on a PoW consensus algorithm. A coded implementation of the protocol was presented in the article. Skwarek (2017) had a similar approach; transactions between IoT devices were stored on the blockchain and consensus algorithms among the nodes would in most cases hinder malicious nodes trying to transmit faulty measurements. Khan and Salah (2018) and Kshetri (2017) also pointed out the security benefits of anchoring an IoT network in a blockchain, although not giving deeper technical explanations.

Support Smart Manufacturing

There are several different terms being used to describe the new, connected industrial landscape. Industry 4.0 was initially a German initiative, launched in 2011. In an attempt at a definition of the term, Hofmann and Rüsch (2017) come up with three necessary characteristics: consistent connectivity and computerization, self-adapting production systems based on transparency and predictive power, and autonomous and decentralized decision-making. Industry 4.0 is also referred to as Smart Manufacturing (Hofmann and Rüsch, 2017). The term Smart Manufacturing is used in this report as it separates the phenomenon from the specific German initiative of Industry 4.0.

The Ethereum-based application proposed by Bahga and Madisetti (2016) opens up for cloud-based, on-demand manufacturing where manufacturing machines are connected to the blockchain and consumers, or even other machines, could order manufacturing services through direct interaction with these machines. The blockchain also allowed for machines to self-diagnose, connect with spare-parts providers and automatically create an order and a transaction. For a visualization of this process, see Figure 4.3. This specific application's source code was presented in

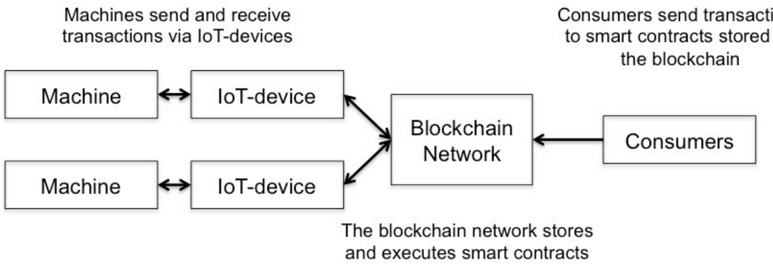

Figure 4.3: Descriptive figure of a blockchain application for customer-to-machine and machine-to-machine interaction. Adapted from Bahga and Madisetti (2016).

Sikorski et al. (2017) presented the isolated case of blockchain-enabled machine-to-machine trading of electricity and made the important observation that the near-instantaneous transfer of electricity provides a beneficial use-case as longer distribution times increases the risk of discrepancies between the blockchain and reality. The source code for the application was presented in the article.

Li et al. (2018) proposed an application where blockchain is the infrastructure that enables smart manufacturing, with smart contracts expressing the relationships between and responsibilities of customers, manufacturers and suppliers. They treated sharing of both services (e.g. manufacturing capacity) and knowledge (e.g. descriptions of processes) that allows for better utilization of slack resources. In their application, all supply chain data is anchored in the blockchain and applications run on this data will then provide trustworthy results to supply chain actors. An illustration of their proposed infrastructure can be seen in Figure 4.4.

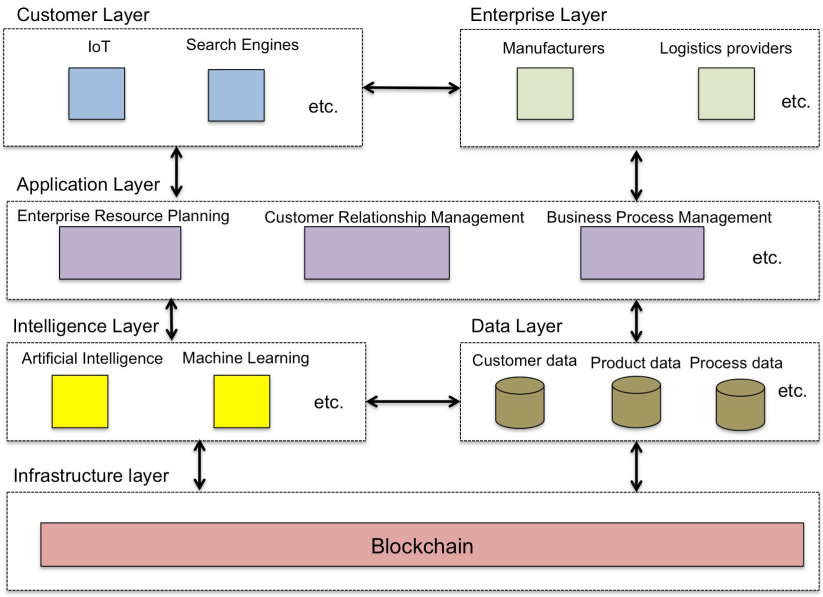

Figure 4.4: Illustration of how Li et al. (2018) imagine BCT as an infrastructure for a smart manufacturing network. Adapted from Li et al. (2018).

Create marketplaces without trusted intermediaries

Notheisen et al. (2017) developed an application for the Danish market for used cars, in collaboration with the Danish tax authorities and the Danish motor register. The application was built on a public blockchain based on the Ethereum protocol, with proof-of-work as the consensus mechanism. Participation in the network required Danish citizenship but was otherwise permission-less. The prototype presented in the article implemented the transaction of a vehicle between seller and buyer, with the blockchain application acting as a marketplace platform and an escrow service. An illustration of this prototype is shown in Figure 4.5. The marketplace acts as a trusted intermediary that automatically re-assigns ownership of vehicles and tokens as the physical transaction is concluded. The proposed application would also allow access to trusted third parties such as service stations and car dealers to provide information on inspection and repairs. The authors noted that this reintroduces the risk of fraud to the system, as these parties may not act in an honest way. Given that a sufficiently large number of honest parties exist, historical discrepancies in data could be spotted and flagged. Internet of things is also proposed as a solution to this issue, replacing trusted third parties by trusted IoT-devices that monitor the characteristics of the vehicle.

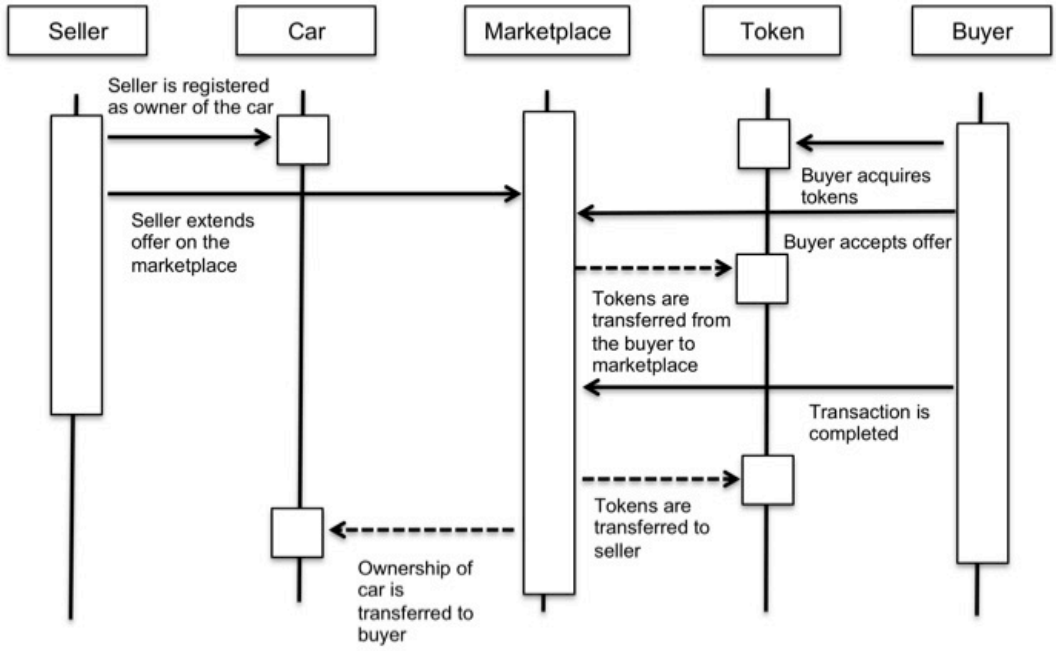

Figure 4.5: Overview of a transaction on the application proposed by Notheisen et al. (2017). The application includes a buyer and a seller, a vehicle where owner information and other characteristics are stored on the blockchain, a marketplace where offers can be posted and a token that can be used to transact on the marketplace. Adapted from Notheisen et al. (2017).

Shen et al. (2017) describe a type of marketplace where customers, retailers, manufacturers and other stakeholders and actors can interact with each other without using any intermediaries. They envision a world of multiple blockchains, interoperable with each other so that demand can be matched with supply by traversing these blockchains. Information on supply and demand would be posted on the blockchains and certain blockchains would be interconnected with each other. The idea is that any demand should not be more than six interconnected blockchains away from the relevant supply to be matched with, similar to the theory of six degrees of separation. In their article they mainly focus on the customer experience in these networks.

Reduce paperwork

Kshetri (2018) described the application proposed by Maersk and IBM. The application arose from the observation that 30 approvals were required on a container's journey from East Africa to Europe, most of them paper-based. This slows down the journey, increasing the risk of product spoilage, and increases the risk for fraud using counterfeited documents. The application digitizes the supply chain documents, allowing actors to digitally sign them. A private, permissioned blockchain is used as an infrastructure for securing the data in a trustworthy manner.

Sikorski et al. (2017) stated that energy trading today comes with high costs for drafting purchase agreements and administration of billing. The M2M-based energy trading system proposed in the article could remove these costs. Offers for selling energy are posted on the blockchain and smart contracts are executed to exchange energy for money.

Smart tendering of transportation

Lee and Pilkington (2017) described, based on a pilot project, how the blockchain can enable smart tendering. Pallets or containers, equipped with RFID tags can broadcast their transport needs on the blockchain, and transporters can then bid for the task to transport these pallets or containers. Smart contracts are then executed to award the task to transport the pallets or containers.

Other applications

McConaghy et al. (2017) presented an application within the digital supply chain, using digital art as an example. Securing digital assets on the blockchain creates an ownership history of these assets. As digital assets are prone to being copied and distributed, it has been difficult to create a functioning market for them. Using BCT a digital artist can create an artwork, publish a number of editions and manage ownership transactions such as selling, renting and loaning the piece of art.

The use of customer data, secured on the blockchain, for forecasting was presented by Chakrabarti and Chaudhuri (2017). As this claim was not underpinned by argumentation or references to secondary sources, did not emerge in any other articles, and was presented in an article of low overall quality, this potential application should be treated cautiously.

Table 4.6: Identified applications and the articles that mention them. The type of blockchain that the article mentions is also presented. Articles are referenced to using their assigned numbers from Table 4.2.

Application	*Permission-less*	*Permissioned*	*Unspecified*
Prove provenance			1, 10
Improve traceability			1, 4
Improve business process management	18		
Monitor cold-chain transportation	10		10, 14
Issue targeted recalls	2	10	19
Anti-counterfeiting	7		10
Provide IoT-security	24	17	8, 9
Support smart manufacturing	2, 12, 21		
Create marketplaces	23		15
Reduce paperwork	21	10	
Smart tendering			11
Increased visibility in the digital supply chain	13		
Forecasting			3

4.3 Descriptive analysis of whitepapers

4.3.1 Whitepapers

Initially, 170 links were retrieved based on a search using the building blocks in Table 3.5. Broken or non-functioning links were not considered. The process of reducing the number of initial result from the search in the Google search engine can be seen in Figure 4.7. The process began by removing 89 duplicate links. Out of the remaining links, 39 were for whitepapers. In the cases where a later version of a retrieved whitepaper was available this was chosen instead. Despite searching only for public blockchains nine results had to be removed due to not considering these types of blockchains. One whitepaper was found to be too vague and mostly focusing on raising money for the project through an initial coin offering[22] (ICO). This paper was excluded from the study, hence leaving a total of 23 whitepapers in the review. However, not all papers were in their entirety dedicated to open permission-less blockchains, but discussed them in sufficient detail to warrant inclusion.

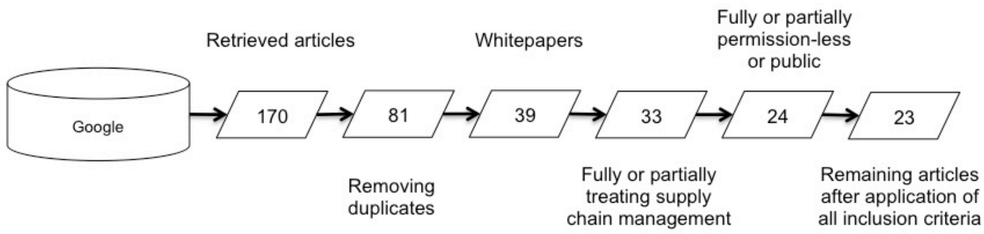

Figure 4.7: The process of selecting whitepapers to be reviewed. The number of remaining articles at each step is displayed.

[22] An initial coin offering (ICO) is similar to an initial public offering in that it is used to raise capital for companies in the blockchain sphere. If the company offers a blockchain service that has a native cryptocurrency it can raise capital through selling this cryptocurrency, where investors hope that the coin will gain value as the service increases in popularity. (Jaffe, 2018)

The 23 reviewed whitepapers can be found in Table 4.7. They differed in some important characteristics, further described below.

Table 4.7: List of whitepapers reviewed.

Nr.	*Name*	*Reference*	*Type of paper*
1	Achain	(Achain, 2015)	Application
2	Ambrosus	(Ambrosus, 2017)	Application
3	Infosys	(Banerjee, 2017)	Exploratory text
4	Genesis of Things	(Blechschmidt and Stöcker, 2016)	Application
5	Cognizant	(Cognizant, 2016)	Recommendations
6	Sutardja Center Berkeley	(Crosby et al., 2016)	Exploratory text
7	Evry	(Evry, 2015)	Text proposing strategies
8	Oracle and IDC	(Fearnley, 2017)	Recommendations
9	Hong Kong Monetary Authority	(Hong Kong Monetary Authority, 2016)	Proof-of-concept
10	Container Streams	(Jabbar and MacDonald, 2016)	Application
11	SophiaTX	(Kacina et al., 2017)	Application
12	Modum	(Modum, 2017)	Application
13	Sweetbridge	(Nelson et al., 2017)	Application
14	One Network	(Notani, 2017)	Application
15	The Blockchain Potential for Port Logistics	(Oude Weernink et al., 2017)	Exploratory text
16	IEEE	(Peck, 2017)	Proposals for research
17	Provenance	(Project Provenance Ltd., 2015)	Application
18	OriginTrail	(Rakic et al., 2017)	Application
19	BBiller	(Rowlison and Holman, 2018)	Application
20	Shipchain	(Shipchain, 2017)	Application
21	The Chamber of Digital Commerce	(Smart Contracts Alliance and Deloitte, 2016)	Text about smart contracts
22	Blockfreight	(Smith, 2016)	Application
23	SyncFab	(SyncFab, 2018)	Application

4.3.2 Publication year

The year of publication was not always clear and the situation becomes more complicated by the fact that some whitepapers are updated. The publishing years for most whitepapers were clearly stated in the beginning or end of the whitepapers. For some whitepapers an educated guess could be done even if no publishing year was clearly stated in the whitepaper and for three whitepapers it was too farfetched to make a credible guess. The publishing years for the whitepapers were a year could be determined can be seen in Table 4.8. There seems to be a trend towards more whitepapers being published each year.

Table 4.8: Distribution of publishing year of the whitepapers, only the ones where it was possible to determine publishing year were included.

	2015	*2016*	*2017*	*2018*
Included whitepapers	4	4	10	2

4.3.3 Publisher

Most of the reviewed papers were published by private companies, specifically trying to sell the proposed application. However, among the publishers were also universities, research institutes, professional organizations, consulting firms, software companies, and a government authority.

4.3.4 Type of paper

The whitepapers can be divided into two broad groups. One describes some kind of application, often in the form of a product developed to be sold and implemented for the benefit of some other party. The other type is a more general text. Many of the more general texts are meant as an introduction to the topic and the benefits of BCT. The more general papers are mostly quite superficial in terms of description of the technology.

Whitepapers describing an application and product also in many cases provided a business plan and information about an ICO, see which ones in Table 4.9. *Project Plan* means that there is a somewhat clear plan for what will happen with the project in the future and "Extensive information about ICO" means that there is some discussion about how coins will be generated and sold. This can be interesting to keep in mind since commercial interests most probably affect these whitepapers.

Table 4.9: Type of application found in whitepapers. The corresponding whitepapers are referenced using their assigned numbers from Table 4.7.

Nr	*Application type*	*Project Plan*	*Extensive information about ICO*
1	Platform for use of Blockchain	Yes	No
2	Increase product traceability	No	No
4	Smart manufacturing	No	No
10	Improve information sharing	Yes	No
11	Improve information sharing	Yes	Yes
12	Increase product traceability	Yes	Yes
13	Improve Supply chain finance efficiency	Yes	Yes
14	Platform for use of Blockchain	No	No
17	Increase product traceability	No	No
18	Improve information sharing	No	No
19	Improve information sharing	Yes	Yes
20	Increase product traceability	Yes	Yes
22	Platform for use of Blockchain	No	No
23	Smart manufacturing	Yes	Yes

4.3.5 Quality

The quality of the whitepapers in relation to Pub-PL blockchains differed quite much. A few papers did not explicitly make any separation between the type to be studied in this thesis and other types, some only dedicated a short section to them while others focused on them. The ones focusing on Pub-PL blockchains were mostly the ones proposing applications. This follows naturally from how the selection of articles was made, if describing an application of another type of blockchain the paper would not have been included. More general texts were not excluded as long as they considered Pub-PL blockchains. Some papers describing applications were blockchain agnostic, i.e. they did not specify which blockchain to be used in the solution they provided and left the choice open.

Quality also differed in how detailed the explanations given in the texts were and if there seemed to be understanding behind the statements made or if they were merely repeating what others have said about BCT. In general, it can be said that the whitepapers not proposing a specific application stated the benefits of BCT without giving very much background information to why the technology could provide these benefits. The ones proposing applications were good at explaining what they intended to do but explaining exactly how was treated in various depth.

It was not always clear how the validation of new blocks works, which could make some applications permissioned. However, care has been taken to ensure that the reviewed applications are at least based on public blockchains.

4.4 Thematic analysis whitepapers

All papers concerned themselves with issues solvable with Pub-PL BCT, in various levels of detail.

4.4.1 Issues

Six main issues were identified and can be seen in Table 4.10, along with which papers that brought up these issues. The approach to the issues and exactly which part of the main issues concerned differed. Below each of the issues will be elaborated on. Perhaps some of the listed issues could be considered to be sub-issues to other issues but the chosen classification was done to highlight important themes and allow for a more detailed evaluation. Examples of this are *Lack of supply chain flexibility* and *High supply chain complexity*

How issues were presented differed somewhat between different whitepapers. Some explicitly stated issues and then went on to propose applications solving these issue while others more implicitly stated what benefits BCT could have in supply chains. In the latter example the issue would be connected to how the situation would be in the lack of BCT or another technology having the same function.

It is worth keeping in mind that many of the whitepapers are trying to sell a concept or a product. Perhaps this leads to biased identification of issues.

Table 4.10: Identified issues and the whitepapers in which they are discussed. Whitepapers are referenced to with their assigned number from Table 4.7.

Issue	*Paper*
Low efficiency	1,2,3,4,7,8,9,12,13,15,16,18,19,20,21,22,23
Lack of flexibility	13
High supply chain complexity	2
Lack of trust	1,2,4,5,6,7,9,11,14,15,18,20,22
Lack of visibility	1,2,3,4,6,8,11,12,13,14,15,16,18,19,20,21,22,23
Lack of transparency	2,3,4,6,14,15,17,18,23
Compliance with regulations	10,12
Intellectual property rights	23

The concepts of efficiency, trust, transparency and visibility are tightly linked and affect each other. Efficiency refers to how well current resources are used. By having visibility in the supply chain a company can better know what to expect and design its processes accordingly. Having transparency without visibility is useless, following the definitions used in this thesis. Even if other stakeholders can access the same information as the company in question (high transparency) this is useless if the company does not properly know its supply chain (low visibility). Low levels of trust generate extra work and so inefficiency. If a company perceives another as trustworthy they might be more inclined to work for mutual visibility and transparency.

Low efficiency

Low efficiency in the supply chain was often brought up as an issue. It is a broad concept and was characterized differently in different papers focusing on inefficiencies that could be solved with the proposed application. In some cases the actual word efficiency was not explicitly written but implied by an application considerably increasing efficiency in some part of the supply chain. The level of efficiency has to be seen in the context of other alternatives.

Many papers were quite general in their statement of inefficiency in supply chains. For example Banerjee (2017) just stated that the inefficiencies stemmed from more complex supply chains. The whitepaper of Ambrosus (2017) stated that they intended to be a remedy to complex supply chains and so, *High supply chain complexity* was identified as a sub-issue to inefficiency.

However, the general theme in the papers stating an actual inefficiency is related to information. The issues brought up were both concerning the quality and availability of information. Blockfreight stated that there is "…inefficiency and variability in the data associated with each and every movement of container freight" (Smith, 2016). Sweetbridge by Nelson et al. (2017) approached inefficiency similarly by saying that many of the supply chain's inefficiencies have roots in data inaccuracies, but also inefficient resource allocation and lack of liquidity. In this whitepaper another issue was also identified as a sub-issue to low efficiency, *lack of flexibility*. In this setting flexibility would mean ability to adapt to changes in the environment of the company.

Some whitepapers focused on inefficiencies in specific supply chains such as Oude Weernink et al. (2017) that focused on port logistics and inefficient exchange of information because of many manual processes and the lack of integration of all relevant partners in the system. SyncFab (2018) highlighted the procurement process as inefficient, stating that inefficiency comes from not using procurement software or using company specific software that is slow and hard to use across the supply chain. The reasoning by Blechschmidt and Stöcker (2016) was similar when they wrote about verifying the trustworthiness of the manufacturing process and the products. Gathering all data about the manufacturing process is cumbersome and difficult; in effect the process of verification reduces efficiency in the economy.

While lack of data or lack of high-quality data seemed to be the main issue the efficiency of processes was also mentioned. It was touched on in SyncFab (2018) in the previous section, by not using software fitting its purpose it is difficult to ensure the correct information at the right time. According to IDC and Oracle process inefficiencies could be solved with blockchain (Fearnley, 2017). This whitepaper does not go further into explaining which these inefficiencies are and both Evry (2015) and Smart Contracts Alliance and Deloitte (2016) explained in similar detail but focus on how smart contracts could increase efficiency. Shipchain (2017) considered the lack of a unified communications platform a source of inefficiency

Lack of trust

The issue of trust was frequently mentioned as can be seen in Table 4.10. Many whitepapers set out to solve the issue of lack of trust in the supply chain, however why this was actually an issue remained unclear. OriginTrail implied that there could be no business without trust (Rakic et al., 2017). In transactions you have to be guaranteed to get your part. It was solved by having a third party, whom both transacting parties trust, verifying that the transaction was conducted as it should (Crosby et al., 2016).

This third party, often a bank, was seen as something you would like to remove, reducing the number of actors in each transaction. Cognizant (2016) suggested that there are more efficient ways to handle the issue of trust than currently and that the current way is more expensive than necessary. Third parties were further mentioned by for example "The Blockchain Potential for Port Logistics" (Oude Weernink et al., 2017) and Evry (2015).

In the whitepaper of OriginTrail it was written that "…one of the biggest challenges faced by the global economy - opaque, inefficient and untrusted supply chains" (Rakic et al., 2017), indicating the importance of trust in supply chain. Blechschmidt and Stöcker (2016) stated that trust historically has been hard and costly to establish. Achain (2015) wrote that the cost of trust needs to be decreased through better information. This showed a somewhat different approach to trust, not the trust in a third party validating, but in the actors the company is transacting with. However, the different views are connected as the need for third parties, such as banks, are currently used because of lack of trust in other supply chain actors.

The main theme seemed to be that trust was needed for transactions to be possible. From this need stemmed the use of third parties. Costs increased trying to create trust, whether with banks or otherwise.

Lack of visibility

The distinction between visibility and transparency was not very clear in most whitepapers. Many different terms were used, intended to mean one thing in some papers and other things in other papers. This demanded some interpretation of the whitepapers; just because visibility was mentioned in a paper did not mean it meant visibility according to our chosen definitions. Traceability was frequently mentioned together with visibility, suggesting a close connection.

Going by this thesis' definition of visibility almost all papers in some way described lack of visibility (see Table 4.10). The general theme was that it is hard to see what happens in the supply chain. The whitepaper of OriginTrail by Rakic et al. (2017) compared lack of visibility to keeping data in siloes where other actors cannot see it. This lack of visibility hurts efficiency. The paper stated in a later part that blockchain can help promote visibility further than one step upstream and one step downstream in the supply chain, indicating that visibility further than this was a weakness of supply chains. Achain (2015) brought up similar issues in that data was scattered and not properly visible but in the context of SCF. Modum (2017) put visibility in the context of trust and argued that with proper visibility no trust was needed.

Banerjee (2017) expanded on why lack of visibility was an issue. By not having proper visibility it is hard to evaluate a product. Ambrosus (2017) put this in a time perspective; complexity reduces transparency and makes it hard to locate problems in time to contain them. The visibility can sometimes be so bad that shippers do not know which carriers are transporting their freight (Shipchain, 2017). Low visibility seems to imply low control and promote inefficiency. Lack of control gives opportunity for dishonest practices, such practices involves fraud and counterfeiting (Fearnley, 2017). In the case of SyncFab (2018) lack of visibility was mainly discussed in terms of finding manufacturers. Low visibility made it complicated to find manufacturers with proper capabilities.

Lack of transparency

Perhaps the whitepaper that emphasized transparency in the supply chain the most was Provenance written by Project Provenance Ltd. (2015). The main point of the application was to provide transparency for end-customers. The issue identified was that without knowledge about the supply chain of goods consumers cannot make the right choices and will contribute to many negative practices. Transparency was in a way seen as a control and feedback mechanism to ensure proper conduct in companies. Ambrosus (2017) stated that consumers are demanding more transparency than ever. The issue of transparency in both those cases seemed to spring from the demand of the consumers.

Banerjee (2017) wrote about lack of transparency in the whitepaper for Infosys. Lack of transparency would according to him lead to a lack of accountability. The discussion was primarily related to environmental damage and illegitimate practices.

It could also been seen from an authenticity perspective, as in Blechschmidt and Stöcker (2016). If the consumer cannot be sure that a product is what it pretends to be, how can they know what they are buying? For more expensive products this certainty and some kind of proof is important.

Compliance with regulations

Two whitepapers stated that the issue in their focused supply chain their products were developed for was new regulations. The regulations imposed certain requirements on control in the respective supply chains. The papers then went on to state that the issues posed by the regulations were solvable with BCT.

Modum (2017) discussed the tightened regulations of chapter nine of the European Union's Good Distribution Practice regulation. It required proof that medicinal products for human use has not been subject to conditions that could compromise its quality. The current solution to this was temperature-controlled trucks, which is an unnecessary expense for most products.

Container Streams dealt in its first phase with meeting the requirements of SOLAS VGM, which aimed to make sea freight safer, according to Jabbar and MacDonald (2016). It required the weight of each container to be sent to the shipping line before delivery of the container to the loading port.

Intellectual property rights

Only SyncFab (2018) mentioned intellectual property rights, and even so just briefly. Statistics taken from a report of a consulting firm were given as argument for that the protection of intellectual property right were in fact an issue. It was framed in the setting that bigger companies can afford cyber-security of their own while for smaller companies it might be harder to find a solution.

4.4.2 Applications

When identifying applications only actually implemented applications were considered. This was to ensure that there was enough feasibility of the application and not just speculation.

Applications of Pub-PL blockchains in supply chain can be categorized in many ways. In this thesis they were grouped according to type, i.e. kind of application. The application types can be seen in Table 4.11; in this table only actual implementations of the applications are considered. The whitepapers grouped together share certain similarities and these will be further examined.

Table 4.11: Identified application types and the whitepapers in which they are mentioned. Whitepapers are referenced to using their assigned number from Table 4.7.

Application Type	*Paper*
Platform for use of blockchain	1,14,22
Increase product traceability	2,12,17,20
Improve information sharing	10,11,18,19
Smart manufacturing	4,23
Increase Supply chain finance efficiency	13

However, not just the whitepapers in Table 4.11 discussed applications. In fact, every whitepaper in some way discussed how BCT could be used in supply chains to solve issues. The whitepapers not included in the table did not specify applications but rather mentioned what areas an implementation of a blockchain solution would affect, i.e. the outcomes of implementing BCT.

As can be seen in Table 4.12 almost all papers implemented applications or suggested that applications using BCT could provide visibility in the supply chain in one way or another. Transparency was often mentioned with visibility with some confusion in the whitepapers to exactly what was intended. Other common themes were automation of payments and transactions, information sharing and anti-counterfeiting. Smart contracts were used as argument for automation while a public blockchain was said to be easy to share information on because of its openness to all parties. Anti-counterfeiting was seen as an effect of the irreversibility of the blockchain combined with creating a digital identity for the goods. Quality certifications were related to the same concepts. Through easy sharing of information and the use of smart contracts SCF was brought up in terms applications for increasing of liquidity.

Table 4.12: Function of applications and techniques used. Corresponding whitepapers are referenced to using their assigned numbers from Table 4.7.

Areas of functions of the application	*Paper*
Supply chain finance	1,8,13,21
Information sharing	1,3,5,7,8,9,10,11,14,15,16,18,19,20
Automation of payment/transaction	1,5,7,8,9,13,15,19,22
Anti-counterfeiting/IP protection	4,6,8,11,16,17,21
Quality certification	2,12
Provides transparency	1,2,3,4,5,6,9,14,15,17,18,23
Provides visibility, traceability and provenance	1,2,3,4,5,6,8,9,11,12,13,14,15,16,18,19,20,21,22,23

Techniques	*Paper*
Smart contracts	1,2,3,4,5,6,7,8,9,10,12,13,15,17,19,21,22,23
IoT integral part of product	2,5,12,15,23
Token	1,2,11,12,13,18,19,20,22,23

Table 4.12 also shows some techniques used or proposed to be used in implementing the application. Smart contracts, IoT and tokens are often heard in the context of BCT and it can be seen that they are frequently mentioned in the papers in Table 4.12. The terms were mentioned more than can be seen in the table, where only the ones properly discussing them are featured. This choice was made since the terms smart contract, token and IoT were often mentioned in passing without giving them a proper explanation or context. Smart contracts can be seen to be a part of most applications.

Some applications could without too much argumentation have been included in other groups but the most fitting group was chosen. Below the applications will be briefly described in terms of what function they have, how the applications work and what part the blockchain plays.

Platform for use of blockchain

The whitepapers in this group were meant to provide more basic infrastructure for the use of BCT in the supply chain. Their common denominator was that they provided platforms for building other applications.

Achain (2015) launched a blockchain network with the main goal to be secure and stable, trying to solve some issues they identified with current solutions. The whitepaper listed security risks of smart contracts, connectivity between different blockchains, connection between data on the blockchain and the real world, scalability and slow transaction speed as issues Achain intended to solve. Achain aimed at building a platform for the use of smart contracts that not only could access data on the associated blockchain but from the outside world as well. To provide flexibility Achain envisioned a network of blockchains through easy forking of the main chain in order to get blockchains specialized for certain purposes. These blockchains would then communicate through a special protocol. The first two areas of use of Achain proposed were SCF and authentication of products. The chain is public but uses a consensus mechanism called Result-delegated Proof-of-Stake, implying some degree of centralization.

As explained by Smith (2016) in the Blockfreight whitepaper, it set out with the arguably ambitious goal to be an as big revolution in the information flow in supply chains as the Blockfreight blockchain was introduced as being adapted especially to the needs of supply chains. Compared to many of the other applications presented in the literature review Blockfreight was a low-level protocol to act as a basis for other applications. The blockchain was public but not permission-less in that there were specific validators. The blockchain supported Ethereum smart contracts and put emphasis on this as a capability of the Blockfreight blockchain. The need for standardization of freight data on blockchain was brought up and it was suggested that Blockfreight could help in that process.

One Network's whitepaper by Notani (2017) was on the borderline to be included in the review or not. It featured a complicated setup with many blockchains to simultaneously have transparency and privacy. It was finally decided to include it since it contains a public blockchain. The setup used was more complicated than in other implementations but in short the users of the application has to trust an actor that can see all transactions unencrypted. However, what differs from a traditional database is that this trust only has to be transient because in due time transactions are visible on the "frontchain", i.e. the blockchain visible to all. This application highlights that it can be an issue to have all of your supply chain data publicly visible. However, using public blockchains has certain strengths and that there exists trials like this trying to reconcile what seems irreconcilable.

Increase product traceability

The applications categorized as increasing product traceability focused on tracing goods, how the goods had been treated and which conditions the goods endured through the supply chain.

Modum (2017) implemented an application where the temperature of trucks carrying pharmaceuticals was monitored to comply with regulations on pharmaceuticals. Loggers measuring temperature were put in the packages holding the pharmaceuticals to record the temperatures. When close to a phone running a mobile application developed for the purpose the logger sent the recorded data. This data was then taken through the system and recorded on a blockchain, which made it unalterable. An illustration of the system, and the interaction between front end and back end, can be seen in Figure 4.8. The loggers were identified as risks, as they could be compromised. Countermeasures, such as keeping lists of all components using serial numbers, were taken. The whitepaper stated that the focus was on last mile deliveries in the pharmaceutical supply chain. When a change of ownership of the goods occurred, parameters decided upon beforehand were checked against a smart contract.

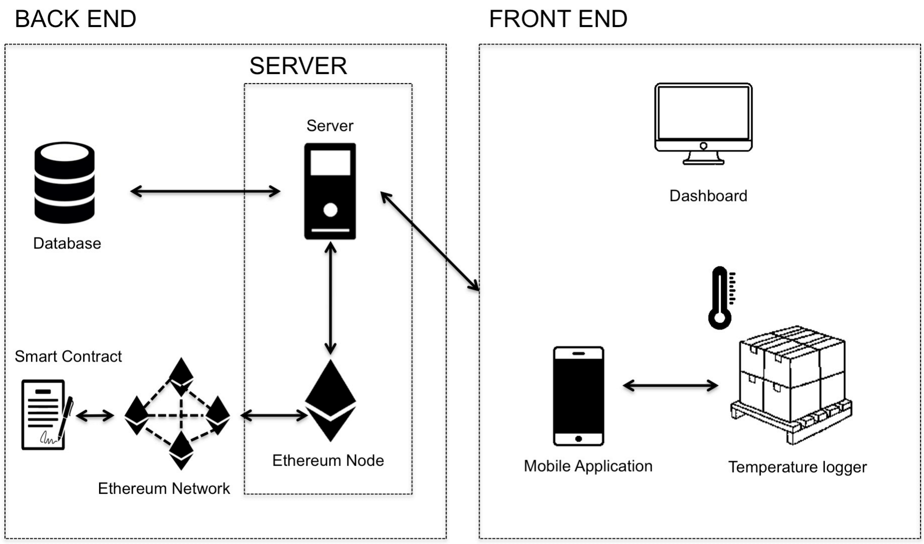

Figure 4.8: Illustration of front end components and back end components and the interaction between them in the application proposed by Modum. Adapted from Modum (2017).

Ambrosus (2017) also have a physical component connected to their blockchain solution and share other similarities with Modum. Different sensors provide input to the blockchain network. The vision is a system with three main parts. Quality assurance sensors, connected to each other to form a system, that record the entire history of a product make up the first part. This recorded data is stored in the second part, which is a blockchain meant to protect the integrity and verifiability of the data and in effect the product. The third part implements smart contracts to automate supply chain governance and manage commercial relationships between actors in the supply chain. The blockchain used was not the main Ethereum chain but a public new version of it.

Provenance, as explained in the whitepaper by Project Provenance Ltd. (2015), set out to provide every physical product with a digital passport, which could prove that a product was what it claimed to be and had the origin it claimed. It tried to solve the problem of selling of fake goods, fraudulent use of certifications and provide transparency. There were a number of possible users of the system including but not limited to producers, standards organizations, certifiers and end-consumers. By linking physical goods through for example barcodes to their digital identity a bridge between the physical and digital world was achieved. Actors handling the goods through the supply chain could then through apps provided by Provenance log the actions taken on the goods, may it be some production process or certification. A use-case on tracking tuna was provided on the company website. An adapted illustration of the path from fisherman to consumer is shown in Figure 4.9. Each actor in the supply chain adds information to the blockchain, while a third-party NGO provides certification that the involved actors comply with certain sustainability standards.

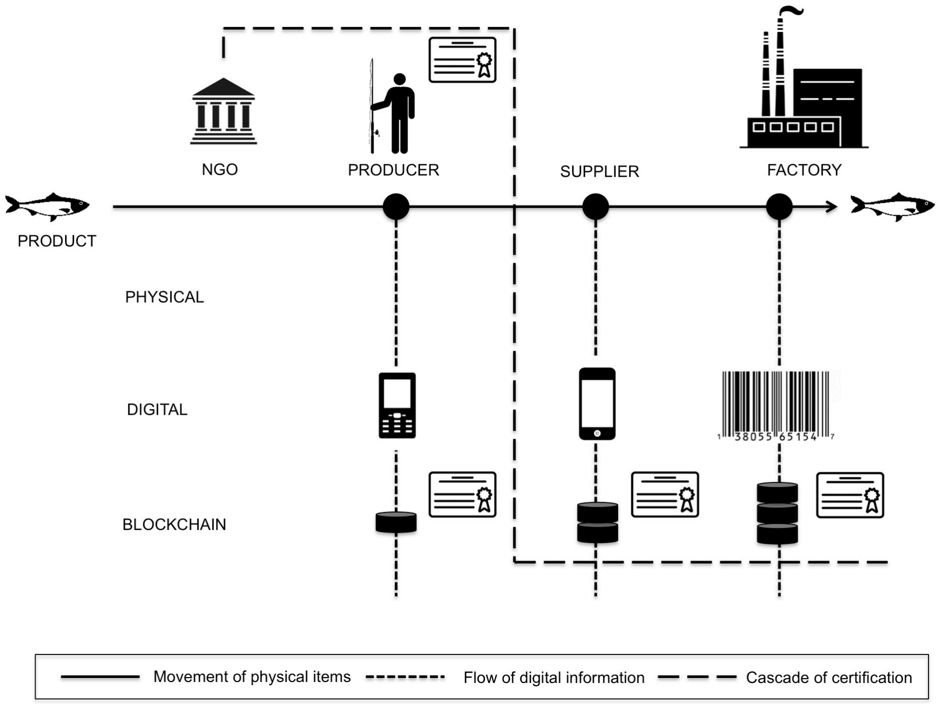

Figure 4.9: Illustration of the path from fisherman, via suppliers and factories, to consumer and how blockchain interacts with the product along its way. Part of a case study carried out by Provenance. Adapted from Project Provenance Ltd. (2016).

Shipchain (2017) aimed to track a product from the moment it leaves the factory to when it was delivered to the end-customer. When a shipment order was launched a smart contract was initiated. Waypoints were then recorded in the smart contract and when finally delivered the contract would be completed. The smart contracts were supposed to state how any disputes should be handled. To improve privacy and efficiency, sensitive data could encrypted and stored on a sidechain running a version of Ethereum, i.e. an interconnected blockchain adapted for its purpose. This blockchain could be the one operated by ShipChain or private ones run by other companies. This not only provided privacy but also reduced the number of transactions on the main Ethereum blockchain and saved money through reduced transaction fees. Another part of the application aims to connect shippers to carriers through a decentralized brokerage system. When booking transport all information would be provided in smart contracts, saving paperwork and time. Customs could get access to the platform if needed.

Improve information sharing

The common denominator for the three applications put in this group was that they facilitated sharing of data and had a function of adapter for this purpose between other systems, i.e. they ensured data from a system was available in a form that could be used by another system to make them interoperable. This category had similarities to the Platform for the use of blockchain category in that they in some respect functioned as platforms for other things to be used on. However, they had more specific uses compared to the ones placed in the other category.

Rowlison and Holman (2018) wrote the whitepaper for Bbiller which presented the application as a decentralized accounting system on the first page of the whitepaper, further specifying that it is a decentralized document and billing platform. The aim of the application was to create a peer-to-peer system for payments in the supply chain. Its main functions were providing a platform for data exchange, such as status updates, payments in any currency, including cryptocurrencies, and possibility to integrate IoT. Smart contracts were generated to make processes efficient. The audit trail created by storing all transactions on the blockchain was presented as a further benefit. Access to the blockchain was presented as theoretically open to anyone but a solution where less knowledgeable companies used other companies as access points was presented as likely.

Container Streams, whose whitepaper was written by Jabbar and MacDonald (2016), had two applications working together as part of a larger solution. The first was an adapter for SOLAS VGM and the other Container Streams ecosystem. SOLAS VGM is short for Safety Of Lives At Sea – Verified Gross Mass. As explained in the issues section this requires data of a container to be sent in advance to the loading port. The adapter aimed at making all actors communicate through a common system that connected their legacy systems to a blockchain and further through an API to shipping line with the data in any format required. In a longer perspective the adapter was seen to be part of a Container Streams ecosystem that automatizes data collection and distribution from weighbridges used to weigh containers. In even longer term the ecosystem was seen as a tool for other actors such as customs and include more data collection than just from weighbridges. The ecosystem would be public for the whole shipping industry but the data stored on the blockchain would be encrypted.

SophiaTX, developed by Kacina et al. (2017), was intended especially as an integrator for ERP systems and BCT. There were three parts to the application: a blockchain, a development platform for integration with APIs and a marketplace for apps. The blockchain was chosen to be public to allow for a more holistic collaboration between supply chain actors. In terms of permissions the blockchain leaned towards the permission-less type using a consensus process based on Delegated Proof-of-Stake. Tokens were implemented for use as payment for transactions in the system and as reward to miners. The main idea behind the application was to enable the use of blockchain in conjunction with ERP systems, such as SAP, in an integrated way and to enable different actors to access the same data stored on the blockchain with their own systems. This was meant to bring transparency, peer-to-peer information exchange and a common ground when solving disputes.

OriginTrail was a purpose-built protocol for supply chain based blockchains by Rakic et al. (2017). Much like SophiaTX it was aimed at connecting systems, especially ERP systems, at different supply chain actors to each other. This would let them exchange more data and make the exchange easier. The application was a platform for data exchange and could possibly have been categorized as a Platform for use of blockchain but the emphasis of the system was data exchange. On this platform called OriginTrail Decentralized Network apps could be used for specific tasks, while the connection between ERP systems functioned also without these apps. The Decentralized Network tried to get the benefits of blockchain without storing all data on the underlying blockchain since the cost would be comparably high. The blockchain itself was used to ensure data integrity. The application was public but to be able to use it, users would have to be approved by the stakeholders one step upstream and one step downstream in the supply chain. As a consensus mechanism the system uses something called a Zero Knowledge Proof, this means that data is proven to be right without actually showing the data to unauthorized parties.

Support smart manufacturing

Two whitepapers suggested applications related to the concept of smart manufacturing. Genesis of Things did not have an application ready for the market but had performed a pilot study (Blechschmidt and Stöcker, 2016). SyncFab on the other hand claimed to be the world's first peer-to-peer manufacturing supply chain (SyncFab, 2018).

SyncFab (2018) envisioned a platform increasing visibility and connecting actors in manufacturing supply chains. The application was designed to be possible to be implemented with both private and public blockchains. One of the main points of the platform was to store information about order history and manufacturing capabilities, among other things, on the blockchain and match orders to suppliers this way. It was intended to speed up the process and save money. Further smart contracts were used to automatically execute processes. The whitepaper stated that a token would be used to incentivize suppliers to perform traditionally uncompensated tasks such as putting together quotes. An illustration of the connections and transactions between different actors in this eco-system can be seen in Figure 4.10.

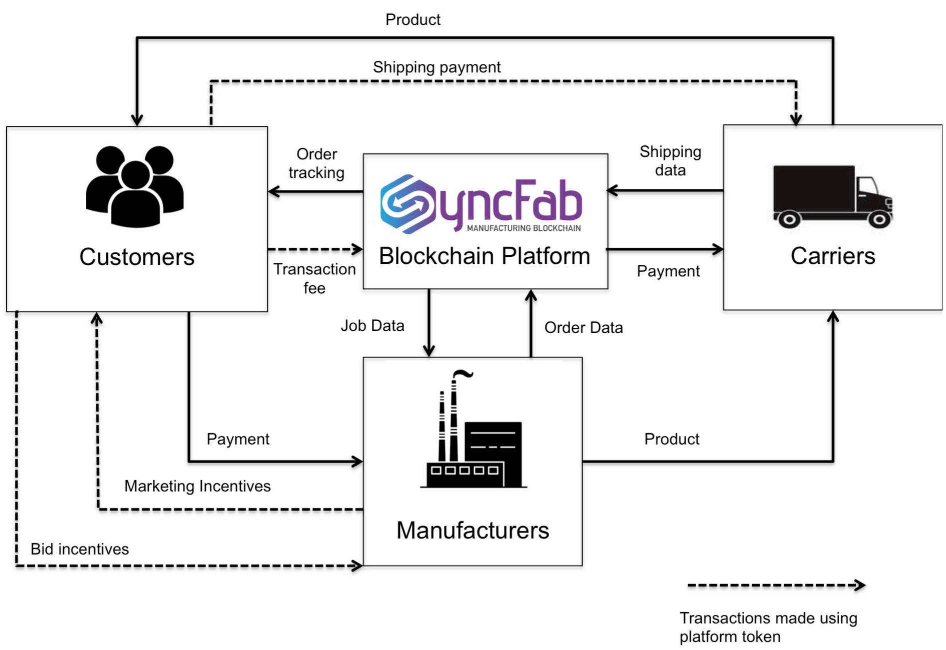

Figure 4.10: Illustration of the ecosystem proposed by SyncFab and the flow of transactions between participants. Adapted from (SyncFab, 2018).

Genesis of Things proposed a 3-D printing platform, as explained by Blechschmidt and Stöcker (2016). The application was meant to make contact between buyer and supplier easier. The design of the product was recorded on the blockchain and accessible to the producer. Because all transactions were recorded on a public ledger anyone could see where a product had been and where it came from, providing transparency. The designer of the product would get royalties when the design was used. By using the blockchain for exchanging information a lot of paperwork was saved. By providing each product with a QR code is was possible to link every specific product to a certain digital product history.

Increase Supply chain finance efficiency

While Achain (2015) listed SCF as one of its main applications its main focus was not on providing a solution for issue related to this but rather to be an infrastructure. When mentioning SCF the approach was also very focused on availability of data.

The one whitepaper that in its entirety was dedicated to SCF was Sweetbridge by Nelson et al. (2017). In its first stage of development the focus was on increasing liquidity of firms through their solution. The application was built in layered protocols that would stack and work together. Ultimately Sweetbridge will include more layers handling transaction settlement, accounting, resource sharing and optimization. The idea was to provide protocols for peer-to-peer interactions without any bank involved in the financing.

Nelson et al. (2017) write in the whitepaper that Sweetbridge raised liquidity by allowing firms to use a variety of assets as collateral and take out loans on them inside Sweetbridge network, i.e. the network of firms using the Sweetbridge protocol stack. For this purpose, a smart contract was used and the loan was recorded on the blockchain. The payments for the collateral would be in Bridgecoin, one of the two native cryptocurrencies in the system. Further it included a function for risk management in the network by making all unsettled invoices and orders public. This first liquidity layer functioned as a basis for the other layers. The second native cryptocurrency, called Sweetcoin, would also be launched and used in the network to reduce interest rates and reduce fees in the network.

4.5 Synthesis and framework

This chapter will synthesize what was found in the two parts of the literature review and link it to the SCOR framework. Firstly issues will be associated to applications. Following that there will be a discussion on the issues in the light of SCOR and finally the applications will be linked to the framework.

The purpose of this literature review was to create a list of identified issues and applications to act as input to the first round of the Delphi study. The identified issues and applications from the literature review have therefore been synthesized and compiled into a list. One identified issue was removed from this final list, lack of intellectual property rights. Even though intellectual property rights are important for many companies the issue had a poor connection to other issues and fell outside of the system studied in this thesis.

Two identified applications were removed, using blockchain for demand forecasting and using blockchain as infrastructure for the digital supply chain. The first was removed due to only being mentioned in one article, and not being underpinned by data or convincing argumentation. The second was removed partly because it was only mentioned in one article and partly because it was very different from the other applications, and also only related to a few specific supply chains. The digital supply chain is featured in the SCOR framework, but only as an emerging practice. Fully digital supply chains could very well become more common in the future and many of the findings of this study could probably be transposed into a fully digital environment.

Identified issues were either grouped together or split into different sub-issues in order to facilitate comprehension and ensure a sufficient level of detail. As an example, *Lack of supply chain security* was divided into *Lack of security for IoT-devices* and *Counterfeited products.* Likewise, *Lack of efficiency* was treated in many other issues, such as inefficient information sharing. *Paperwork* was however an efficiency-related issue that emerged from *Lack of efficiency*. *Compliance with regulations* was not included as its own issue since it is a question of if the applications found potentially could help to comply with regulations, rather than if BCT itself satisfying regulations. It is present in the issues in the form of *Lack of transparency for regulators*.

In total, 13 issues and 15 applications that were identified in the literature review and considered in the first round of the Delphi study. The issues can be seen in Table 4.13 and the applications can be seen in Table 4.14.

Table 4.13: Identified issues that were included in the first round of the Delphi study.

Number	*Issue*
1.	Lack of upstream visibility
2.	Lack of downstream visibility
3.	Lack of upstream traceability
4.	Lack of downstream traceability
5.	Lack of transparency for customers
6.	Lack of transparency for regulators
7.	Lack of transparency for financial institutions
8.	Lack of trust
9.	Paperwork
10.	Counterfeited products
11.	Lack of security for IoT-devices
12.	Lack of flexibility
13.	High supply chain complexity

Table 4.14: Identified applications that were included in the first round of the Delphi study.

Number	*Application*
1.	Smart tender of transportation
2.	Improve product traceability
3.	Monitor transport conditions
4.	Prove provenance
5.	Improve information sharing
6.	Verify supply chain activities
7.	Create trusted marketplaces
8.	Anti-counterfeiting
9.	Issue targeted recalls
10.	Increase Supply chain finance efficiency
11.	Provide secure communication for IoT-devices
12.	Provide infrastructure for M2M-interaction
13.	Provide infrastructure for C2M-interaction
14.	Reduce paperwork
15.	Automate payments and transactions

Issues and applications are linked in the sense that certain applications can help solve certain issues. Some issues are more specific than others and are therefore easier to connect to applications. Issues like lack of trust, lack of flexibility and high supply chain complexity are broader and are indirectly influenced by many applications. Table 4.15 illustrate the direct links between issues and applications that have been identified.

Table 4.15: Links between issues and applications. Issues are presented in text, with their corresponding number from Table 4.13 in brackets. Applications are presented with their corresponding numbers from Table 4.14.

Issue	*Related application(s)*
Lack of upstream visibility (1)	5, 6, 8, 12, 13
Lack of downstream visibility (2)	1, 5, 6, 8, 12
Lack of upstream traceability (3)	2, 3, 4, 9
Lack of downstream traceability (4)	2, 3, 9
Lack of transparency for customers (5)	4, 8
Lack of transparency for regulators (6)	4
Lack of transparency for financial institutions (7)	10
Lack of trust (8)	7
Paperwork (9)	12, 13, 14, 15
Counterfeited products (10)	8
Lack of security for IoT-devices (11)	11
Lack of flexibility (12)	12, 13
High supply chain complexity (13)	5, 6

4.5.1 Issues

An issue could be defined as less than optimal performance in some area. The SCOR framework concerns itself with performance in terms of performance attributes. These are strategic characteristics of supply chain performance expressed in terms of different metrics meant to guide the supply chain towards the general business strategy and its goals. On a superficial first level the issues identified in the literature review seem to be somewhat relatable to the performance attributes given by SCOR; Reliability, Responsiveness, Agility, Cost and Asset Management Efficiency. SCOR states that attributes themselves cannot be measured and introduces metrics in three levels to measure the ability to achieve what is expressed by the attributes.

However, the performance attributes consider performance from a process execution point of view. The issues identified in the literature review are satisfactorily covered by the first level metrics presented in the framework. Of course, the issues would impact the metrics but many linkages would be all too speculative to add any value. The issues are on a high level and while SCOR focuses on the outcomes of supply chain process execution the identified issues are more issues of the design and setup of the supply chain.

To give just one example consider the issue lack of trust. It is difficult to quantify how this would affect the supply in different metrics even if it is frequently mentioned as an issue in the literature.

Instead, identified issues were schematically connected to the enable process as can be seen in Table 4.16. It should not be viewed as a hard or definitive mapping, the issues are wider than the enabling processes. From this follows that the mapping is only meaningful on the primary level. The idea is that some of the enabling processes can capture at least part of the issue. No process adequately handling paperwork was found and the issue of trust was too wide to be appropriately mapped.

The enable process in SCOR is "associated with establishing, maintaining and monitoring information, relationships, resources, assets, business rules, compliance and contracts required to operate the supply chain as well as monitoring and managing the overall performance of the supply chain" (APICS, 2017) which goes well with a technology such as blockchain. Issues would then signify unsatisfactory performance of a process.

Table 4.16: Connections between issues (presented with their corresponding numbers from Table 4.13) and SCOR processes on a first and second level.

First Level	*Second Level*	*Issue(s)*
Enable	sE3 Manage Data and Information	1,2,3,4,5,6,7,10,11,12,13
	sE5 Manage Supply Chain Assets	12,13
	sE6 Manage Supply Chain Contracts /Agreements	1,2,3,4,5,6,7,10,11,12,13
	sE8 Manage Regulatory and Voluntary Compliance	1,2,3,4,5,6,7
	sE9 Manage Supply Chain Risk	1,2,3,4,5,6,7,8,10,11,12,13
	sE11 Manage Supply Chain Technology	1,2,3,4,5,6,7,11,12,13,14

4.5.2 Applications

Applications are easier to connect directly to the SCOR framework, in terms of which processes they affect. An attempt to make this connection can be seen in Figure 4.11, where the relevant applications are displayed above each first level process.

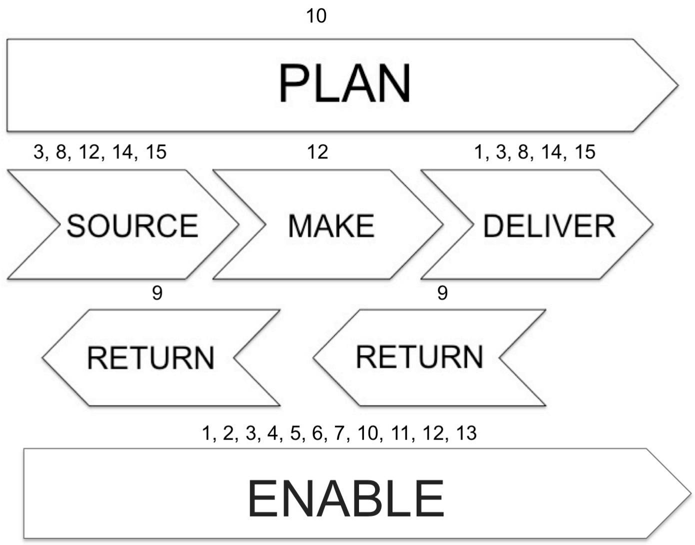

Figure 4.11: Illustration of connections between applications (presented with their corresponding numbers from Table 4.14) and first level SCOR processes.

Applications have been linked to SCOR-processes in Table 4.17. When possible, links all the way down to third-level processes have been made. Some applications were determined to affect a second-level process but it was not possible to distinguish a relevant third-level process. In these cases, only the link to a second-level process was made.

Table 4.17: Connections between applications (presented with their corresponding numbers from Table 4.14) and SCOR processes on a first, second and third level.

First Level	*Second Level*	*Third Level*	*Application(s)*
Plan			
	sP1 Plan Supply Chain		10
Enable			
	sE2 Manage performance		2, 11
	sE3 Manage Data		2, 3, 5, 6, 11
	sE5 Manage Supply Chain Assets		11
		sE5.5 Inspect, Maintain and Repair	12
	sE6 Manage Supply Chain Contracts/Agreements		
		sE6.4 Review contractual performance	3
	sE7 Manage Supply Chain Network		10, 11
	sE8 Manage Regulatory and Voluntary Compliance		4
	sE9 Manage supply chain risk		10, 11
	sE10 Manage Supply Chain Procurement		7
		sE10.4 Supplier Selection to Participate in ITT / RFQ / Negotiation	1
		sE10.6 Bid, tender evaluation and validation	1
		sE10.7 Contract award and implementation	1
Source			
	sS1 Source Stocked Product		
		sS1.2 Receive product	14
		sS1.3 Verify product	3, 8
		sS1.5 Authorize supplier payment	15
	sS2 Source Make-to-Order Product		
		sS2.2 Receive product	14
		sS2.3 Verify product	3, 8
		sS2.5Authorize supplier payment	15
	sS3 Source Engineer-to-Order Product		
		sS3.2 Receive product	14
		sS3.3 Verify product	3, 8
		sS3.7 Authorize supplier payment	15
Make			
		sM.2.1 Schedule production activities	12

First Level	*Second Level*	*Third Level*	*Application(s)*
Deliver			
	sD1 Deliver Stocked Product		
		sD1.13 Receive and verify product by customer	3, 8, 14
		sD1.15 Invoice	15
	sD2 Deliver Make-to-Order Product		
		sD2.2 Receive, Configure, Enter and Validate Order	13
		sD.2.7 Select Carriers	1
		sD2.8 Receive Product from Source or Make	3, 8
		sD2.13 Receive and verify product by customer	3, 8, 14
		sD2.15 Invoice	15
	sD3 Deliver Engineer-to-Order Product		
		sD3.13 Receive and verify product by customer	3, 8, 14
		sD.3.15 Invoice	15
	sD4 Deliver Retail Product		
		sD4.2 Receive product at store	3, 8
Return			
	sSR1 Source Return Defective Product		
		sSR1.3 Request Defective Product Return Authorization	9
	sDR1 Deliver Return Defective Product		
		sDR1.3 Request Defective Product Return Authorization	9
	sSR2 Source Return MRO Product		
		sSR2.3 Request MRO Product Return Authorization	9
	sDR2 Deliver Return MRO Product		
		sDR2.3 Request MRO Product Return Authorization	9

5. Delphi study

This chapter presents the findings of the Delphi study. The results of each round are presented and analyzed, with emphasis being placed on the results of the final round. Expert comments are then summarized, synthesized and presented in a structured narrative.

5.1 Round 1

Delphi round 1 was carried out between 8/3-28/3. 31 participants responded to the questionnaire. This meant that 86 % of experts who agreed to participate in the study responded to the first questionnaire.

For each identified issue, the experts were asked if they agreed that this is an issue that could, at least partially, be solved using Pub-PL BCT. For each identified application, the experts were asked if they agreed that this is a suitable application of Pub-PL BCT in the supply chain. The experts could in this round either answer "Yes", "No" or "Don't know". The results can be seen in Figure 5.1 and Figure 5.2.

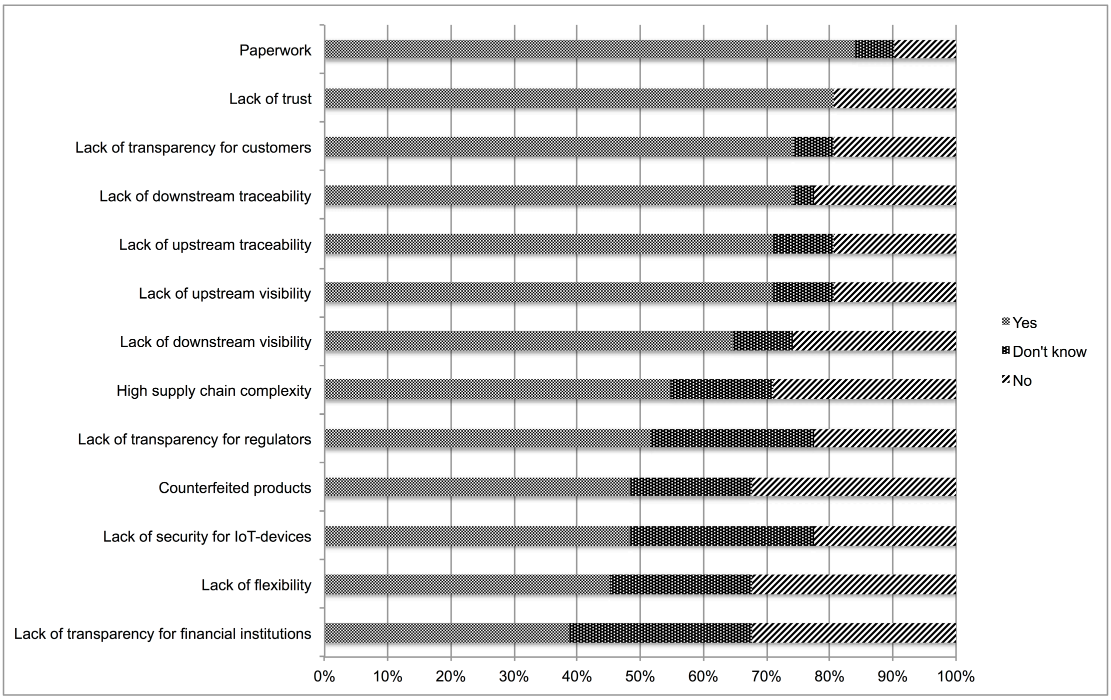

Figure 5.1: Distribution of responses among all participants of Delphi round 1. The question asked was "Do you agree that this issue, at least partially, could be solved using public and permission-less blockchain technology?"

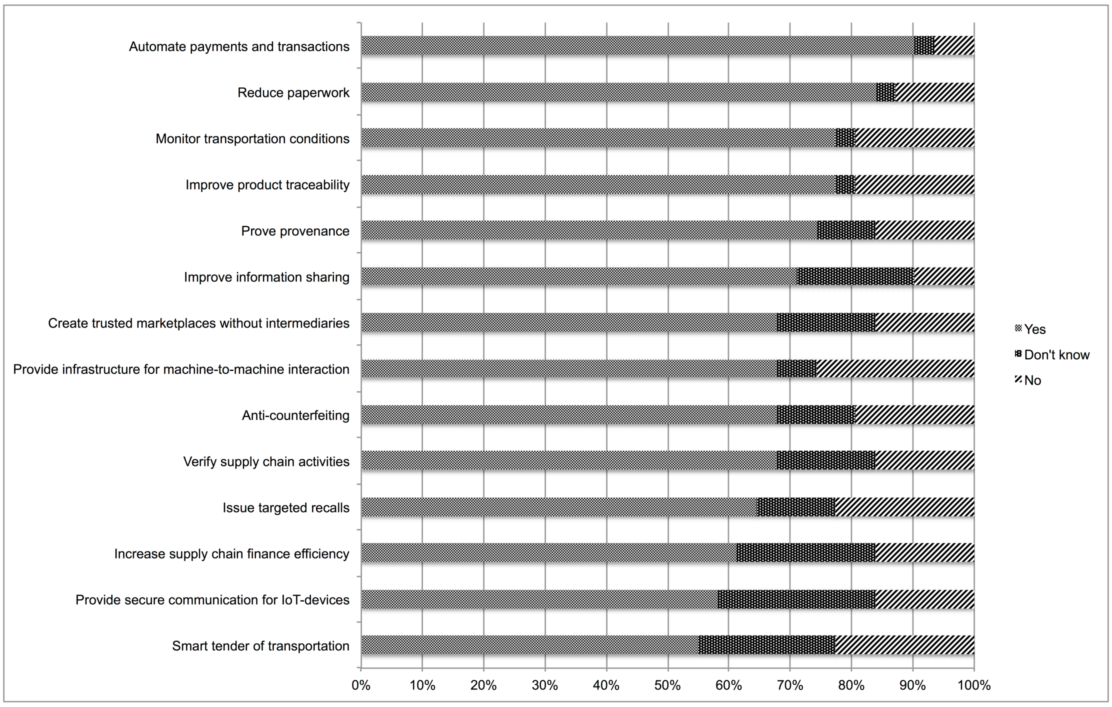

Figure 5.2: Distribution of responses among all participants of Delphi round 1. The question asked was "Do you agree that this is a suitable application of Pub-PL blockchain technology in the supply chain?"

Given the small sample size, these results should not be seen as statistically significant. In this study they were primarily used as a validation of the literature review and as a foundation for discussion in future rounds, together with the provided comments. It can however be noted that the experts were generally positive to the potential of BCT in SCM. For nine out of 13 issues a majority of experts responded "Yes" to the question of whether BCT could, at least partially, solve this issue. For all applications, a majority of experts believed that they were suitable.

The experts were asked to give comments to their replies. A lot of comments, in total 307, were received. These were of varying quality and detail. 182 edited comments were included in the second questionnaire. The excluded comments were either excluded due to low quality[23] or being too similar to included comments.

Two proposed applications were included into the second questionnaire: *Sharing infrastructure using IoT-devices* and *Monitoring assets at suppliers*. The first application refers to sharing infrastructure such as machinery or trucks among different supply chain actors. IoT-devices are used to monitor capacity and availability, as well as for handling requests for usage. The capacity would be posted on the blockchain, and this application is therefore somewhat similar to *Smart tender of transportation*. The second application refers to the possibility of monitoring assets such as machinery at the supplier. This could also mean monitoring capacity and availability, as well as general performance. The role of blockchain would be to act as a trusted database of information on the machinery.

[23] Either impossible to understand, off-topic or not detailed enough. An example of the last case would be the comment "Yes, that is a good application".

In the first round all responses were treated together, without looking separately at the different panels. Results on a panel level are however interesting for comparison with results from round two and three. It can be seen that Blockchain experts were in general more cautious about the prospects of BCT in supply chain, with the exception of certain issues, such as *Lack of security for IoT-devices*, and applications, such as *Creating trusted marketplaces*.

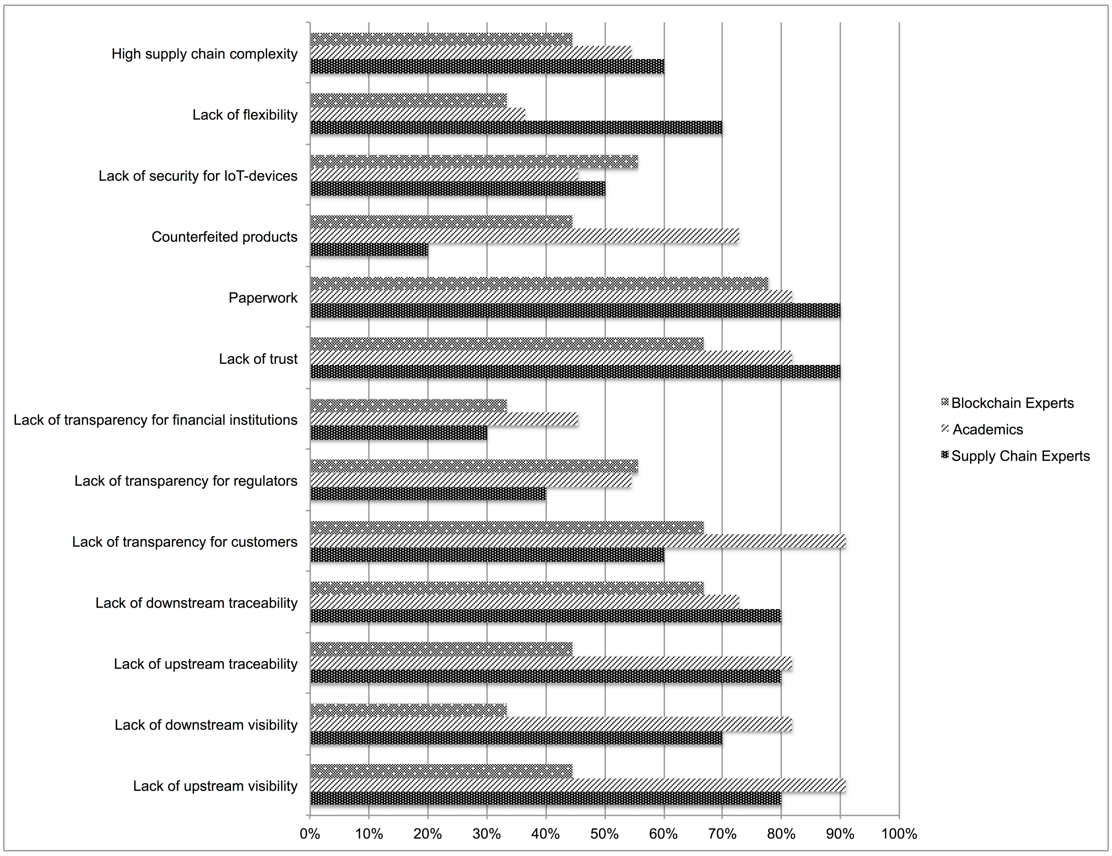

Figure 5.3: Percentage of participants on each panel that answered "Yes" when asked: "Do you agree that this issue, at least partially, could be solved using public and permission-less blockchain technology?"

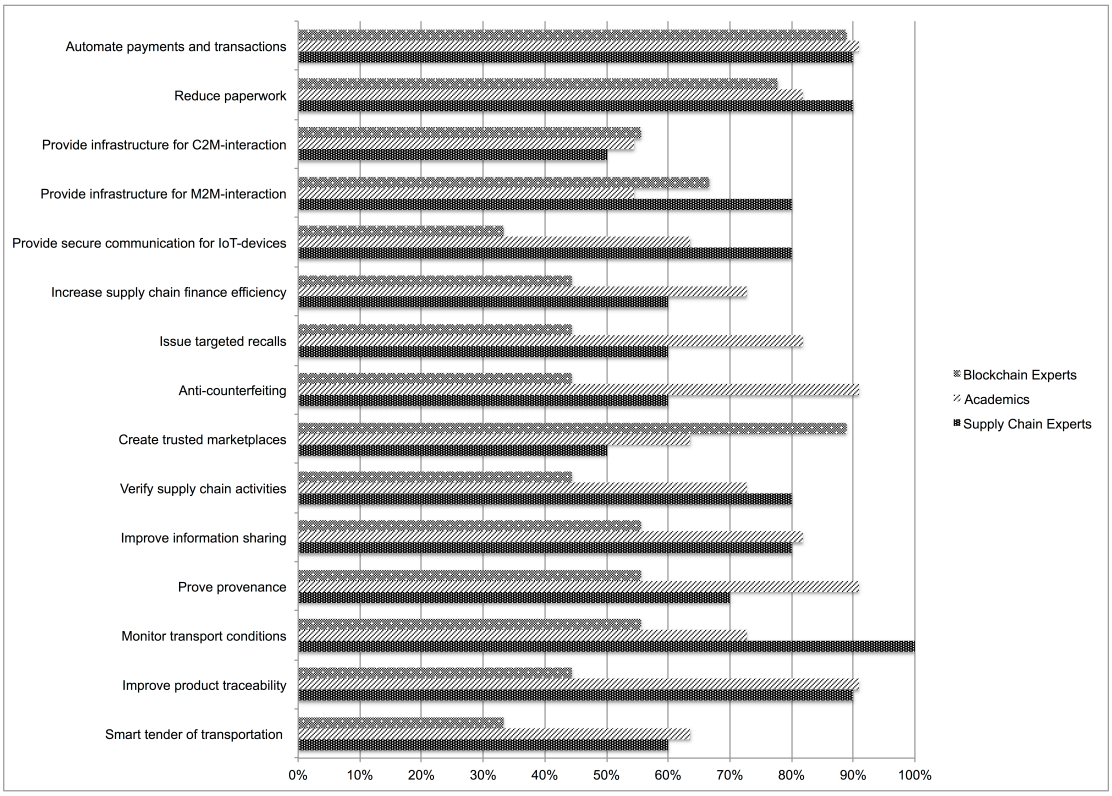

Figure 5.4: Percentage of participants on each panel that answered "Yes" when asked: "Do you agree that this is a suitable application of public and permission-less blockchain technology in the supply chain?"

The background data for Delphi round 1 can be found in Appendix D.

5.2 Round 2

The Delphi round 2 was carried out between 4/4-21/4. 29 participants responded to the questionnaire, with two experts dropping out of the study. There were 10 remaining Supply chain experts, 10 remaining academics and nine remaining blockchain experts.

As the experts who dropped out did so before being exposed to the opinions of other experts, it is difficult to speculate on how the results could have turned out if they had stayed in the study. Their answers to the first questionnaire can give a view of how positive they were to BCT in supply chain. This could help form a view as to in which direction they would have influenced the end results. Their replies to the first questionnaire are presented in Table 5.1.

Table 5.1: Opinions held by dropped out experts in the first round.

	Yes	*Don't know*	*No*
Issues			
Expert 1	9	1	3
Expert 2	8	1	4
Applications			
Expert 1	15	0	0
Expert 2	12	0	3

As seen in Table 5.1, both dropped out experts were generally positive to the prospects of BCT in SCM. They generally agreed with the majority opinion, so this should not be considered a case of attrition bias. In fact, both experts stated in correspondence that lack of time was their reason for dropping out.

5.2.1 Results

The main results from the second round were the Likert ratings that each participant provided. This study used a five point Likert scale ranging from Strongly Disagree to Strongly Agree. The experts were asked whether they agreed that Pub-PL BCT could solve the listed issues and whether they agreed that the listed applications of Pub-PL BCT were suitable.

For each panel, the first quartile, the median, and the third quartile of the provided Likert ratings were calculated. The difference between the third and the first quartile constituted the IQR, which was used as a consensus measurement. An IQR of less than, or equal to, one indicates that there is consensus among the experts. The results for the identified issues can be found in Table 5.2. The results for each issue is given on a panel-by-panel basis, and also calculated for all participants together.

Table 5.2: Results from grading identified issues the second round of the Delphi study. The IQR is given in brackets, and in bold when the predetermined consensus threshold of IQR ≤ 1 is reached.

Issue	*Supply chain experts*	*Academics*	*Blockchain experts*	*Total*
Lack of upstream visibility	3.5 (2.25)	3 (2.25)	2 (2)	3 (2)
Lack of downstream visibility	4 (2)	3.5 (2.25)	2 (2)	3 (2)
Lack of upstream traceability	4 (1.25)	4 (2.25)	4 **(1)**	**4 (1)**
Lack of downstream traceability	4 **(1)**	4 (2)	3 (2)	4 (2)
Lack of transparency for customers	4 (1.25)	4 (1.25)	3 (2)	4 **(1)**
Lack of transparency for regulators	4 (2.25)	4 (1.5)	4 (2.5)	4 (2)
Lack of transparency for financial institutions	3.5 (1.5)	3 (2.25)	4 (2)	3 (2)
Lack of trust	4.25 (2.25)	2,5 (2.25)	2 (3)	3 (2)
Paperwork	4 (1.25)	4 (2.5)	4 (2)	4 (2)
Counterfeited products	4 (1.25)	4 (1.5)	4 (2.5)	4 (1.5)
Lack of security for IoT-devices	4 (1.5)	2 (2.25)	2 (2.5)	3 (2.5)
Lack of flexibility	2.5 (2)	2 **(1)**	2 (2.5)	2 (1.5)
High supply chain complexity	3 (2.25)	2 (2.25)	3 (2)	3 (2.5)

The results can be visualized using box plots, as has been done for the total results in Figure 5.5. Black squares marks the median rating, grey rectangles the IQR and thin black lines extended to the extreme answers. As can be seen, the second round, i.e. the first round using the Likert scale, included individual responses from one to five for all issues. The issues have been ordered from most to least consensus, with the median rating as a second criterion.

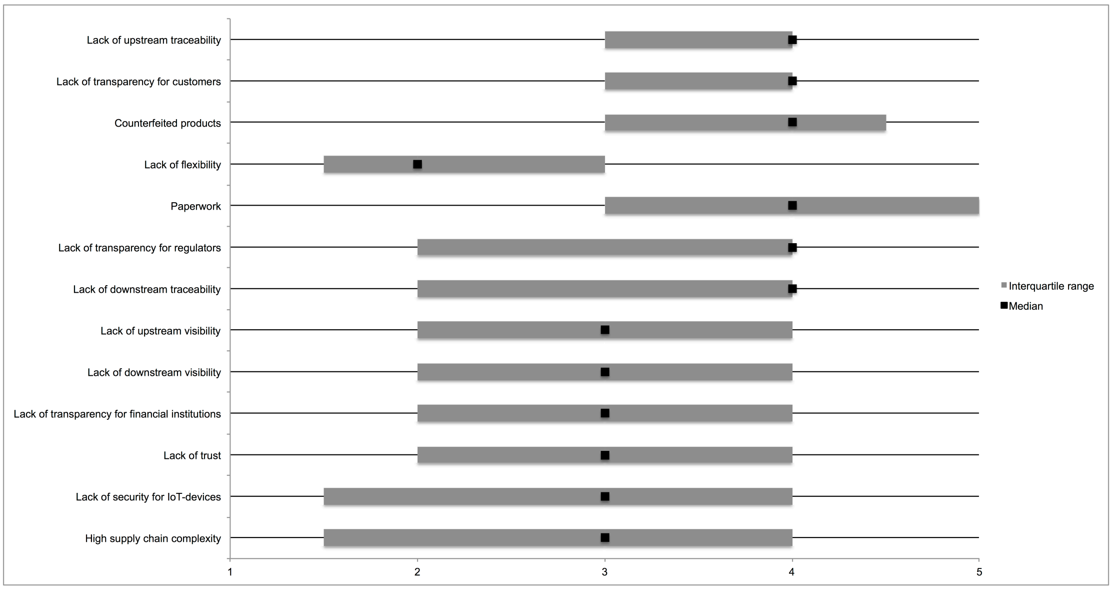

Figure 5.5: The total results of all experts' answers for issues considered together in the second round of the Delphi study. Median Likert rating and IQR visualized, with IQR ≤ 1 meaning consensus.

When viewing the total result a few issues with positive results, defined as when the IQR does not extend below three on the Likert scale, emerged. These are *Lack of upstream traceability*, *Lack of transparency for customers*, *Counterfeited products* and *Paperwork*. Of these, consensus was only reached for *Lack of upstream traceability* and *Lack of transparency for customers* and consensus was generally not reached on a panel level for these issues. On the other hand, *Lack of flexibility* received mostly negative ratings. The result for the other issues was uncertain, as the IQR extends on both sides of three on the Likert scale.

As another rating method has been introduced, it is difficult to compare the results of the first and second round. It could however be noted that, in the first round, more than 80 % of experts believed that the issue of *Lack of trust* could be solved by Pub-PL BCT. That should indicate that the entire IQR should be on the positive side of the Likert rating in the second round, which is not the case. For the issue of *Lack of trust*, it therefore seems as if the experts have adjusted their view negatively.

The identified applications were also graded using the same Likert scale and the results were treated in the same way as for the identified issues. The results for the identified applications can be found in Table 5.3.

Table 5.3: Results from grading identified applications the second round of the Delphi study. The IQR is given in brackets, and in bold when the predetermined consensus threshold of IQR ≤ 1 is reached.

Application	*Supply chain experts*	*Academics*	*Blockchain experts*	*Total*
Smart tender of transportation	4 **(1)**	4 **(0.75)**	3 (2)	4 **(1)**
Improve product traceability	**4 (1)**	4 **(0.75)**	4 (2.5)	4 (1.5)
Monitor transport conditions	4 (2)	4 (2.25)	4 (2.5)	4 (2)
Prove provenance	4 (2.25)	4 (1.5)	4 (2)	4 (3)
Improve information sharing	3 **(1)**	4 (2.25)	3 (2)	3 **(1)**
Verify supply chain activities	3.5 **(1)**	3.5 **(1)**	4 (2)	4 **(1)**
Create trusted marketplaces	3.5 **(1)**	4 (1.25)	5 **(1)**	4 (2)
Anti-counterfeiting	4 (1.25)	3.5 (2)	3 (2)	4 (2)
Issue targeted recalls	4 **(1)**	3 (2.25)	3 (2)	3 (1.5)
Increase Supply chain finance efficiency	4 **(1)**	4 (2.5)	4 (2)	4 (1.5)
Provide secure communication for IoT-devices	3 (1.25)	3 (2.25)	4 (2.5)	3 (2)
Provide infrastructure for M2M-interaction	3.5 (1.25)	3.5 (2.25)	3 (2.5)	3 (1.5)
Provide infrastructure for C2M-interaction	3 **(1)**	3 (1.25)	3 (1.5)	3 **(1)**
Reduce paperwork	4 **(0.75)**	4 (3)	4 (1.5)	4 (1.5)
Automate payments and transactions	4.5 (1.25)	4 (1.5)	5 **(0)**	5 **(1)**
Monitor assets at suppliers	3 (1.5)	3 (2)	2 (2)	3 (2)
Sharing infrastructure using IoT	3 (1.5)	4 (2)	4 (2.5)	4 (2)

The same visualization as for issues has been produced for applications and can be seen in Figure 5.6. Here, too the spread of answers was big with all except one application having answers in both extremes.

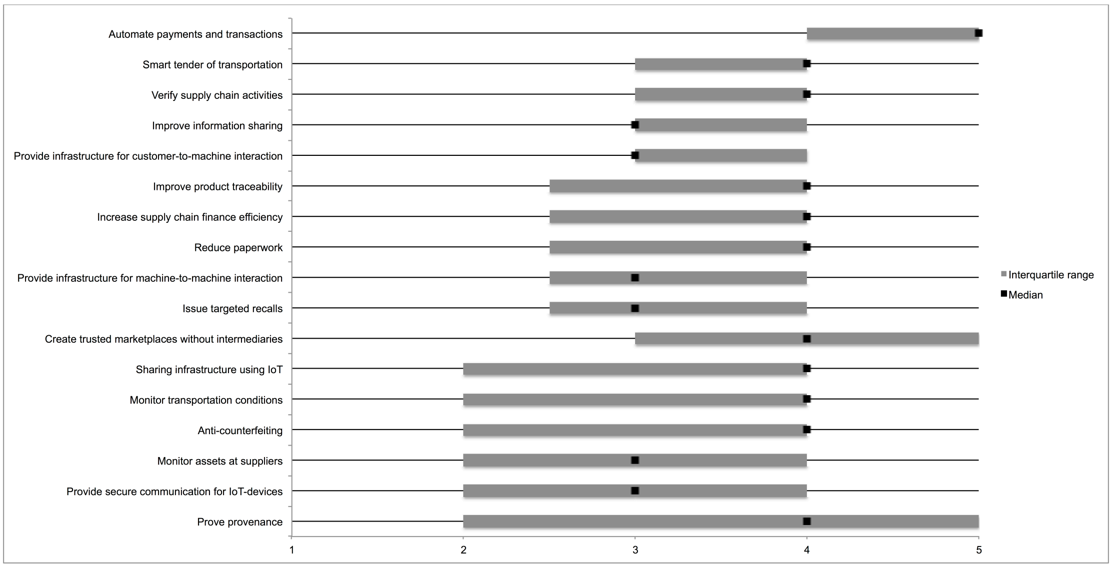

Figure 5.6: The total results of all experts' answers for applications considered together in the second round of the Delphi study. Median Likert rating and IQR visualized, with IQR ≤ 1 meaning consensus.

When looking at the visualization, a few applications with positive results can be singled out. These are *Automate payments and transactions*, *Smart tender of transportations*, *Verify supply chain activities*, *Improve information sharing* and

Create trusted marketplaces. There are no applications with clear negative results, and most applications have uncertain results.

5.2.2 Consensus within panels

The IQR was used as a consensus measurement in this study. An IQR less than, or equal to, one signaled consensus among panel members. Table 5.4 and Table 5.5 illustrate the consensus among panels for issues and applications.

Table 5.4: Consensus within panels and for all experts together on listed issues. The number of issues in the specific IQR range is presented for each panel.

Panel	*IQR ≤ 1*	*1 < IQR < 2*	*2 ≤ IQR*
Supply Chain	1	6	6
Academics	1	4	8
Blockchain	1	7	5
Total	2	2	9

Table 5.5: Consensus within panels and for all experts together on listed applications. The number of issues in the specific IQR range is presented for each panel.

Panel	*IQR ≤ 1*	*1 < IQR < 2*	*2 ≤ IQR*
Supply Chain	9	6	2
Academics	3	7	7
Blockchain	2	10	5
Total	5	5	7

As seen in the tables, consensus was generally not reached as a result of this second round. The exception to this was that Supply chain experts generally agreed on the ratings of applications. In general, there was more consensus concerning applications than issues. The general lack of consensus supports the need for a third round.

5.2.3 Consensus between panels

As the panels generally did not achieve internal consensus, any analyses of inter-panel consensus should be treated carefully. It could, however, be noted that almost all median ratings were three or higher on the five-point Likert scale. This signals a generally positive outlook on the suitability of Pub-PL blockchains in SCM.

The three panels had the same median rating for four of the issues. Where the median ratings were different, the Supply chain experts were generally more positive to the possibility of BCT to solve the identified issues. Their median rating was higher than the two other panels for five issues. As a contrast, the Blockchain experts had lower median ratings than the other two panels for five of the identified issues.

The panels had the same median rating for six of the applications. Where the ratings differed, it was not possible to single out one panel as generally more positive, or negative, than the others.

5.3 Round 3

Delphi round 3 was carried out between 23/4-6/5. 27 participants responded to the questionnaire, with two supply chain experts not responding to the questionnaire. There were eight remaining supply chain experts, 10 remaining academics and nine remaining blockchain experts.

5.3.1 Results

As the panels were exposed to different feedback from Round 2, no total result is given for this round. This is in line with the methodology of using different panels in a Delphi study. Instead, results will be presented on a panel level. The same visualization, using box plots, as in Figure 5.5 and Figure 5.6 will be used. The grey area illustrates the IQR, while black squares mark the median rating. The thinner lines extending from the grey area illustrate the entire spread of ratings.

Supply Chain Experts

Figure 5.7 illustrates the third-round results for the supply chain panel regarding rating identified issues.

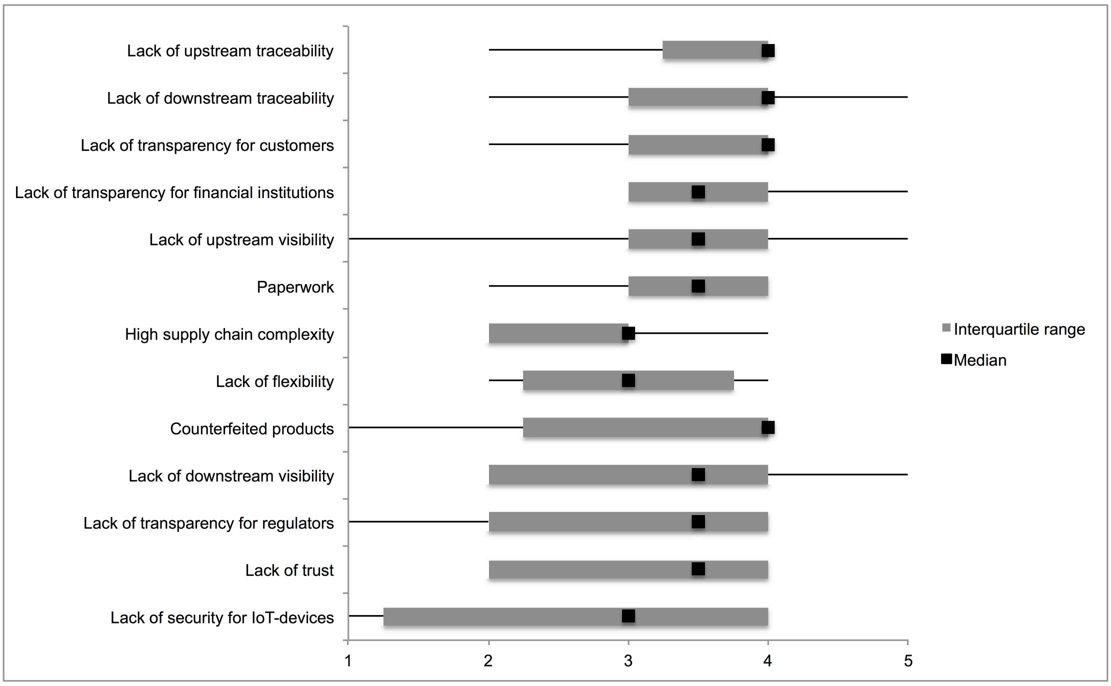

Figure 5.7: Final results of the Delphi study's third round for issues for the Supply chain experts panel. Median Likert rating and IQR visualized with IQR ≤ 1 meaning consensus.

It can be seen that consensus was reached for seven issues, with a clear positive rating for *Lack of upstream traceability* and positive ratings for *Lack of downstream traceability* and *Lack of transparency for customers.* With a median rating of three, experts were more neutral to BCT's potential to solve the *Lack of transparency for financial institutions*, *Lack of upstream visibility* and *Paperwork*. The issue of *High supply chain complexity* also received a median rating of three, but as the IQR did not extend above three a majority of experts seem to be more skeptical to the potential of BCT to solve this issue.

Figure 5.8 visualizes the panel ratings for identified applications.

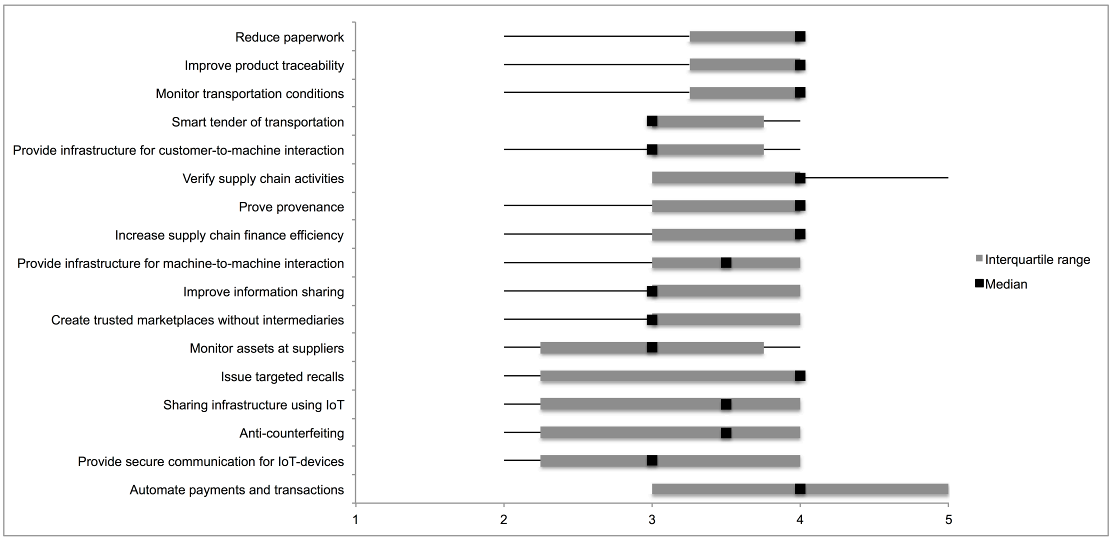

Figure 5.8: Final results of the Delphi study's third round for applications for the Supply chain experts panel. Median Likert rating and IQR visualized with IQR ≤ 1 meaning consensus.

The third round resulted in consensus for the ratings of 11 out of 17 applications with all of them having a median rating of either three or four. This enforces the view, which emerged in the second round, of the Supply chain experts being generally favorable towards BCT in the supply chain.

Academics

Figure 5.9 shows how the academic panel rated the identified issues in the third round.

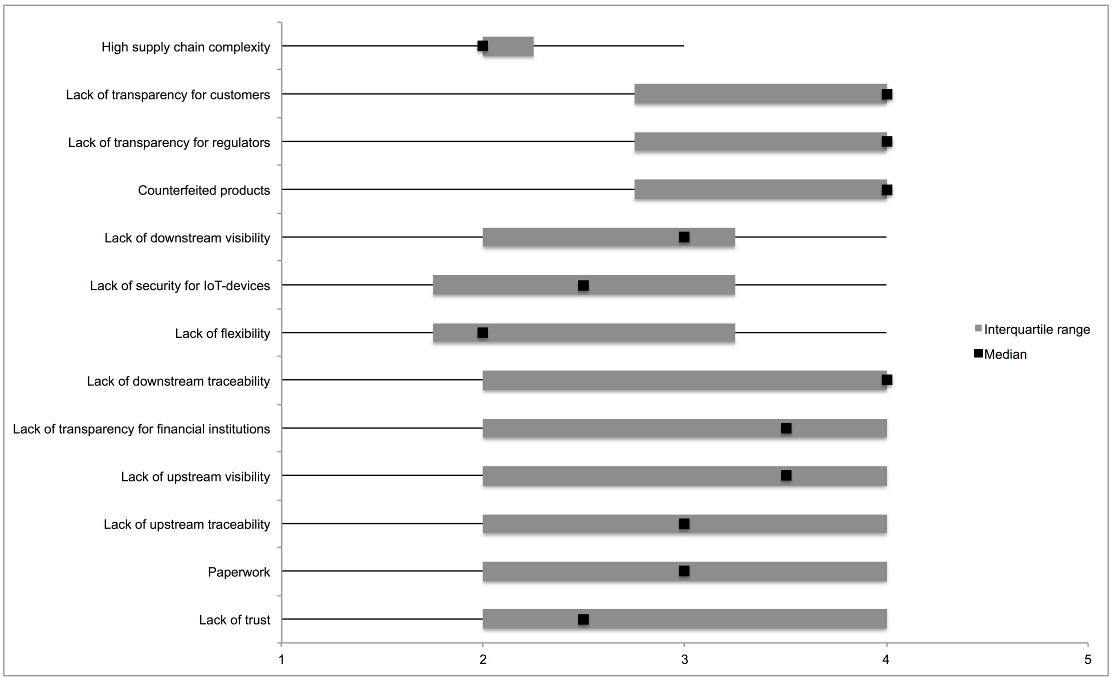

Figure 5.9: Final results of the Delphi study's third round for issues for the Academics panel. Median Likert rating and IQR visualized with IQR ≤ 1 meaning consensus.

When looking at the box plots, it can be seen that Academics in general did not reach consensus. For six of the issues, the IQR extends from two to four, making it difficult to draw any definite conclusions. The academic panel did however reach consensus around a low rating for *High supply chain complexity.* There also seems to be an emerging, positive rating for *Lack of transparency for customers and regulators* and *Counterfeited products.*

Figure 5.10 illustrates how the Academic experts rated the identified applications in round three.

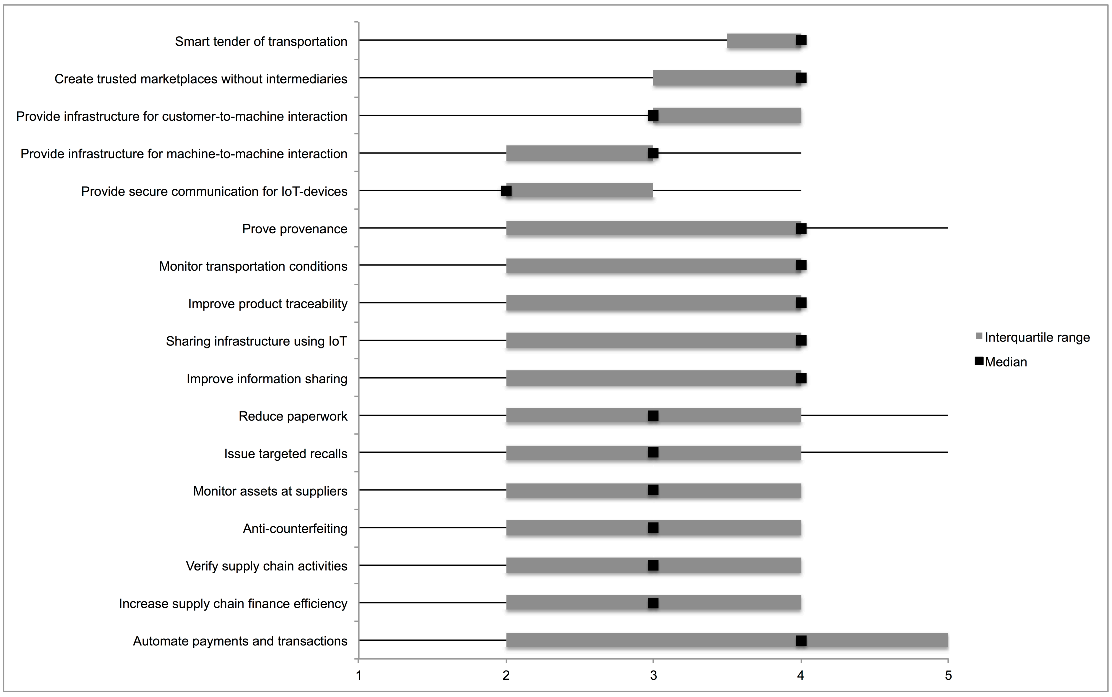

Figure 5.10: Final results of the Delphi study's third round for applications for the Academics panel. Median Likert rating and IQR visualized with IQR ≤ 1 meaning consensus.

Also for applications, the academic panel reached consensus on many issues. A clear positive rating for *Smart tender of transportation* emerged, as did a positive rating for *Creating trusted marketplaces*, a neutral rating for *Providing infrastructure for M2M- and C2M-interaction* and a negative rating for *Providing security for IoT-devices.*

Blockchain Experts

The Blockchain expert panel's view of the identified issues is visualized in Figure 5.11.

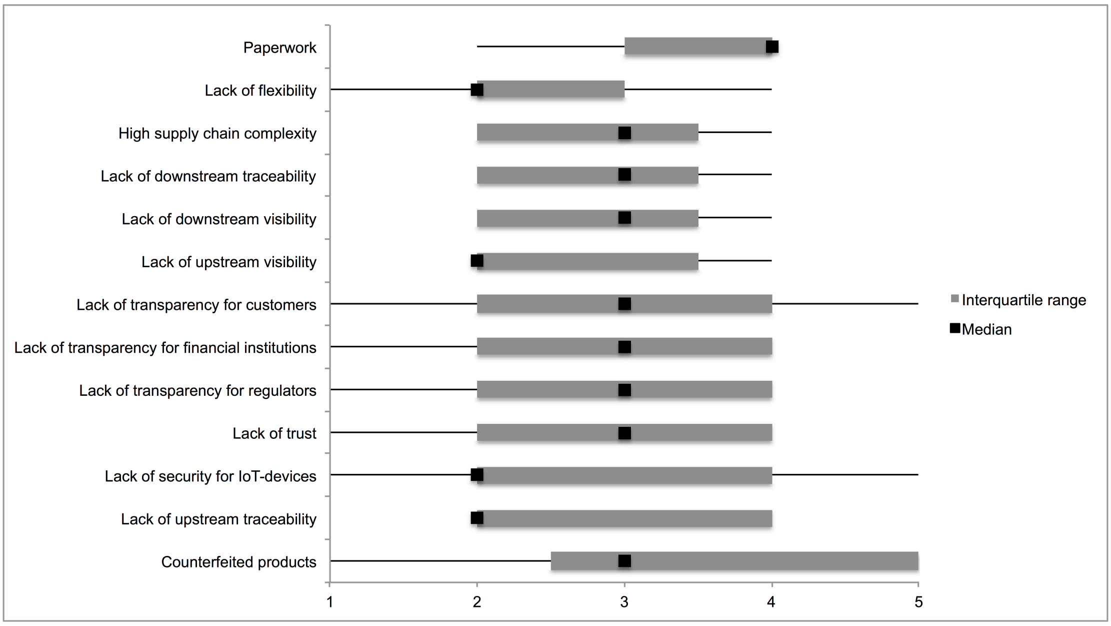

Figure 5.11: Final results of the Delphi study's third round for issues for the Blockchain experts panel. Median Likert rating and IQR visualized with IQR ≤ 1 meaning consensus.

The Blockchain experts agreed on a positive rating for *Paperwork* and a negative rating for *Lack of flexibility* while most other ratings were neutral and lacked consensus.

The panel ratings for the identified applications are shown in Figure 5.12.

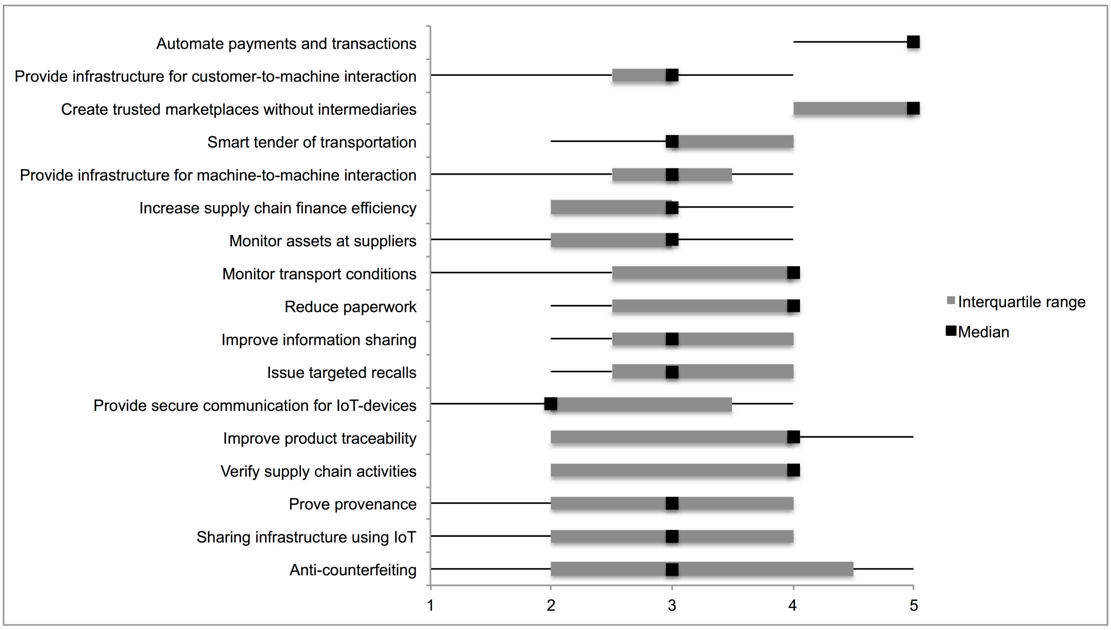

Figure 5.12: Final results of the Delphi study's third round for applications for the Blockchain experts panel. Median Likert rating and IQR visualized with IQR ≤ 1 meaning consensus.

Blockchain experts showed the strongest measured consensus in this study for their high rating of *Automate payments and transactions*. All except one expert answered 5, hence the IQR is not clearly visible in the graph since it is on rating 5. Another high rating was given for *Create trusted marketplaces* while other applications with consensus were given a more neutral rating.

Agreement and disagreement between panels

In Table 5.6 and Table 5.7 the median ratings for the issues and applications for all three panels are presented side by side to simplify comparison. The order the issues and applications are listed in is the same as they have been treated before and does not indicate any sorting.

Table 5.6: Results from grading identified issues the third round of the Delphi study. The median Likert rating for each issue is given on a panel-by-panel basis. The IQR is given in brackets, and in bold when the predetermined consensus threshold of IQR ≤ 1 is reached.

Issue	*Supply chain experts*	*Academics*	*Blockchain experts*
Lack of upstream visibility	3.5 **(1)**	3.5 (2)	2 (1.5)
Lack of downstream visibility	3.5 (2)	3 (1.25)	3 (1.5)
Lack of upstream traceability	**4 (0.75)**	3 (2)	2 (2)
Lack of downstream traceability	**4 (1)**	4 (2)	3 (1.5)
Lack of transparency for customers	**4 (1)**	4 (1.25)	3 (2)
Lack of transparency for regulators	3.5 (2)	4 (1.25)	3 (2)
Lack of transparency for financial institutions	3.5 **(1)**	3.5 (2)	3 (2)
Lack of trust	3.5 (2)	2.5 (2)	3 (2)
Paperwork	3.5 **(1)**	3 (2)	**4 (1)**
Counterfeited products	4 (1.75)	4 (1.25)	3 (2.5)
Lack of security for IoT-devices	3 (2.75)	2.5 (1.5)	2 (2)
Lack of flexibility	3 (1.5)	2 (1.5)	**2 (1)**
High supply chain complexity	3 **(1)**	2 **(0.25)**	3 (1.5)

For many issues it is difficult to draw any sharp conclusion because of the lack of consensus. The supply chain panel has more consensus and so less spread of opinions compared to the other panels. In terms of median ratings, no issue had a completely positive or negative result when considering all panels. At least one panel always had a median rating of, or on the other side of three compared to the other panels. Blockchain experts seem to be more level in their median ratings often giving threes or twos, while being positive only in the case of *Paperwork*. In this case they even reach consensus, as do Supply chain experts, also on slightly positive median rating, while Academics as a panel are undecided and neutral. Overall the spread of answers for different issues in terms of being above or below three are higher in the academic panel compared to the others and Supply chain experts seem to be the most positive.

Compared to the issues the applications' median results are more positive. Ratings where no consensus has been reached should be treated with caution but having this in mind it can be seen that the median rating of all three panels for *Improve product traceability* and *Monitor transport conditions* was four, while for *Monitor assets at suppliers* it was three. *Automate payments and transactions* received positive ratings from all panels.

Table 5.7: Results from grading identified applications the third round of the Delphi study. The median Likert rating for each issue is given on a panel-by-panel basis. The IQR is given in brackets, and in bold when the predetermined consensus threshold of IQR ≤ 1 is reached.

Application	*Supply chain experts*	*Academics*	*Blockchain experts*
Smart tender of transportation	3 **(0.75)**	4 **(0.5)**	3 **(1)**
Improve product traceability	4 **(0.75)**	4 (2)	4 (2)
Monitor transport conditions	4 **(0.75)**	4 (2)	4 (1.5)
Prove provenance	4 **(1)**	4 (2)	3 (2)
Improve information sharing	3 **(1)**	4 (2)	3 (1.5)
Verify supply chain activities	4 **(1)**	3 (2)	4 (2)
Create trusted marketplaces	3 **(1)**	4 **(1)**	5 **(1)**
Anti-counterfeiting	3.5 (1.75)	3 (2)	3 (2.5)
Issue targeted recalls	4 (1.75)	3 (2)	3 (1.5)
Increase Supply chain finance efficiency	4 **(1)**	3 (2)	3 **(1)**
Provide secure communication for IoT-devices	3 (1.75)	2 **(1)**	2 (1.5)
Provide infrastructure for M2M-interaction	3.5 **(1)**	3 **(1)**	3 **(1)**
Provide infrastructure for C2M-interaction	3 **(0.75)**	3 **(1)**	2 **(0.5)**
Reduce paperwork	4 **(0.75)**	3 (2)	4 (1.5)
Automate payments and transactions	4 (2)	4 (3)	5 **(0)**
Monitor assets at suppliers	3 (1.5)	3 (2)	3 **(1)**
Sharing infrastructure using IoT	3.5 (1.75)	4 (2)	3 (2)

Create trusted marketplaces is interesting because there is consensus but on three different ratings. Supply chain experts only gave a lower rating than Blockchain experts on *Automate payments and transactions* and *Create trusted marketplaces*. All panels reached internal consensus on a number of applications: *Smart tender of transportation, Create trusted marketplaces, Provide infrastructure for M2M-interaction* and *Provide infrastructure for C2M-interaction.* The Blockchain experts' ratings ranged from two to five and this group was the only one awarding a median rating of 5. It did so for *Creating trusted marketplaces* and *Automate payments and transactions.* Both Academics and Blockchain experts had a median rating of two for *Provide secure communication for IoT-devices.*

5.3.2 Changes from round 2

The results of Round 3 can be compared to those of the previous round to see the emergence of consensus and the stability of the results. For each issue or application, two measurements could change between round two and round three; the median rating and the IQR. Both these measurements could increase or decrease and the development of each issue and application can be mapped in a matrix. The issues and applications are represented by the numbers introduced in Table 4.13 and Table 4.14.

Supply Chain Experts

The changes of consensus and median ratings of issues and applications between round and two can be seen in Table 5.8 and Table 5.9.

Table 5.8: Changes in consensus and median rating for issues among Supply chain experts.

	Increased level of consensus	No difference	Decreased level of consensus
Increased median	12	-	-
No difference	1, 3, 5, 7, 13	4	10
Decreased median	6, 8, 9	2	11

Table 5.9: Changes in consensus and median rating for applications among Supply chain experts.

	Increased level of consensus	*No difference*	*Decreased level of consensus*
Increased median	-	6	17
No difference	2, 3, 4, 11, 12, 13	5, 10, 14, 16	9
Decreased median	1	7	8, 15

In general consensus was strengthened between round two and three, with increased consensus for nine out of 13 issues, but only seven out of 17 applications. For six out of these issues, and two of the applications, the increased consensus resulted in an IQR below, or equal to, one. For one of the applications, *Issue targeted recalls*, the decrease in the level of consensus meant that the IQR moved from being within the limit of consensus to being outside of it, even though the median rating stayed the same.

Academics

The changes of consensus and median ratings of issues and applications between round and two can be seen in Table 5.10 and Table 5.11.

Table 5.10: Changes in consensus and median rating for issues among Academic experts.

	Increased level of consensus	*No difference*	*Decreased level of consensus*
Increased median	1, 7, 11	-	-
No difference	6, 8, 10, 13	4, 5	12
Decreased median	2, 3, 9	-	-

Table 5.11: Changes in consensus and median rating for applications among Academic experts.

	Increased level of consensus	*No difference*	*Decreased level of consensus*
Increased median	-	-	-
No difference	1, 3, 5, 7, 9, 13	16,17	2, 4, 6, 15
Decreased median	10, 11, 12, 14	8	-

For Academics, the consensus was also generally strengthened between round two and round three, although four applications and one issue saw a decrease in the level of consensus. Of the issues and applications where consensus was strengthened, one issue and four applications where strengthened sufficiently to go from being outside the limit for consensus to being in it. As a contrast, one issue and two applications fell out of the consensus zone as an effect of reduced levels of agreement between experts.

Blockchain Experts

The changes of consensus and median ratings of issues and applications between round and two can be seen in Table 5.12 and Table 5.13.

Table 5.12: Changes in consensus and median rating for issues among Blockchain experts.

	Increased level of consensus	*No difference*	*Decreased level of consensus*
Increased median	2, 8	10	-
No difference	1, 4, 9, 12, 13	5	11
Decreased median	6	7	3

Table 5.13: Changes in consensus and median rating for applications among Blockchain experts.

	Increased level of consensus	*No difference*	*Decreased level of consensus*
Increased median	16	-	-
No difference	1, 2, 3, 5, 9, 12	6, 7, 14, 15	8
Decreased median	10, 11, 13, 17	4	-

The blockchain expert panel saw the clearest trend of increased consensus out of the three panels. The only issue for which there was consensus after round two, *Lack of upstream traceability* saw a decrease in consensus and had an IQR of two in round three. For two issues, *Paperwork* and *Lack of flexibility,* the consensus was increased to an IQR of one. The one application with consensus after round two, *Automate payments and transactions*, was joined by four more after round three.

5.3.3 Sensitivity of supply chain panel results

As the supply chain panel suffered from two dropouts between round two and round three, it is possible that this affected the results. Once again, the potential influence that other expert opinions would have had on these two participants is impossible to assess. In order to somehow quantify the sensitivity of the third-round results, the results if the two experts would have responded with the same rating as in round two has been calculated. As when describing the changes between round two and round three, the consensus and median could either increase, decrease or remain the same when the second-round replies of the two dropped out participants are included. The effects on the rated issues and application are mapped in Table 5.14 and Table 5.15. Two possible effects that important to note and take into consideration. The first is when inclusion of these two replies causes the consensus of the third-round results to decrease, from an IQR below, or equal to one, to an IQR strictly larger than one. This indicates that the consensus reached on that specific issue might be weak. The second one is for issues where the third-round results showed an IQR of less than, or equal to, one and the inclusion of these results caused the median to change while the IQR remained within the limits of consensus. This would show that the median rating of round three might have been over- or underestimated.

Table 5.14: Sensitivity of ratings for issues among Supply chain experts.

	Increased level of consensus	*No difference*	*Decreased level of consensus*
Increased median	11	6	1, 7
No difference	10, 12, 3	4, 8, 9	13
Decreased median	-	2	5

All of the issues for which consensus decreased were issues where the IQR after round 3 was one, and the inclusion of the two dropped out experts increased the IQR to 1.25. These issues were *Lack of upstream visibility (1)*, *Lack of transparency for customers and financial institutions (5,7),* and *High supply chain complexity (13*). The changes in median rating only occurred for issues where no consensus was reached in round three or where the round three consensus was disrupted by the inclusion of these results.

Table 5.15: Sensitivity of ratings for applications among Supply chain experts.

	Increased level of consensus	*No difference*	*Decreased level of consensus*
Increased median	-	15	-
No difference	9, 11, 13, 16, 17	4, 5, 10	1, 2, 3, 14
Decreased median	8	12, 6	-

Of the applications where consensus decreased, only the IQR of *Reduce Paperwork (14)* went from being within the limit for consensus to being outside of it. The median rating of two applications with consensus, *Verify supply chain activities (6)* and *Provide infrastructure for M2M-interaction (12)* was lowered by half a point.

5.4 Expert comments

The comments provided by participating experts provide valuable insights into their motivations and reasoning. Summarized comments are presented in this section. Comments have been shortened or reformulated when necessary. They have also been adapted to create a narrative. No attempt to analyze the comments are made in this section, this is instead performed in Chapter 6.

5.4.1 General comments

Some experts expressed some hesitancy, believing in the concept of blockchain but stating that the technology is still immature and that it has to be developed before its potential benefits can be judged clearly.

Two members of the blockchain panel believed that a symbiosis of private and public blockchain solutions could be useful in many cases. The public blockchain would provide a security layer for the private blockchain applications.

One expert stated that even though Pub-PL blockchains possibly could be used for many purposes the culture of firms and individuals regarding privacy might stand in the way of those implementations. The expert predicted that we would see systems of interconnected private blockchains instead.

Others were more adamant in stating that Pub-PL blockchains did not have a future in SCM and that any blockchain solutions in this field would have to be private and permissioned. The issues with Pub-PL blockchains were considered to be privacy, throughput and scalability.

One comment expressed the view that as a blockchain cannot be queried like an ordinary database, it has no use in the supply chain. Other experts argued against this claim, stating that applications with querying capabilities can be built upon a blockchain infrastructure. One example of this is IPFS, which could act as a database with pointers to data secured on the blockchain.

An issue with BCT, which was brought up by some experts, is the problem of garbage in, garbage out. This means that if the data that is entered into the blockchain is not accurate, trust in the data on the blockchain would diminish and problems could arise due to the creation of immutable bad data. One expert pointed out that garbage in, garbage out, is not a blockchain specific issue, but something that is present for all supply chain data.

One comment detailed the concept of anonymity on Pub-PL blockchains. According to the comment, actors not only can be but also have to be anonymous since not being so would enable miners to discriminate known actors' transactions. Since actors and transactions cannot be connected, due to anonymity, neither can products and transactions. This means that it is impossible to create a digital identity on the blockchain disqualifying most use cases. Another comment highlighted the difficulty, and current inability, to satisfactorily link the blockchain to external values such as products.

5.4.2 Issues

Lack of visibility

One expert saw opportunities for displaying capacity and availability of machinery. Just like a wallet can give a trusted balance of cryptocurrencies, the same could be achieved for displaying available transport capacity and machine time on the blockchain. This could be accomplished through issuing tokens to represent capacity and machine time. Another expert argued that there is no trusted way of capturing this data, and as trust between actors would still have to exist there are no clear benefits of using BCT. A counter-argument to this is that a blockchain would provide transparency of claims, so that claims can be attributed to the person or organization that made it. This would act as a deterrent to post false data on the blockchain. Many experts expressed their doubts about this kind of data being shared on a public blockchain as it could be considered sensitive and private. One expert suggested that data posted on the blockchain should only be accessible by the right private keys. The throughput capacity of a Pub-PL blockchain to handle all this data was also questioned. The permanence of the blockchain was framed as a disadvantage in a supply chain in need of flexibility in one of the comments. Another expert believed that the main challenge would not be technological but educational.

Lack of traceability

One expert stated that BCT does not improve traceability as such, but the fact that claims are transparent would increase trust in the data. The connection between physical qualities and digital representation, e.g. using IoT or RFID, is important and difficult to achieve. One expert stated that this was not possible and the only meaningful traceability was for digital assets. Another one said that the link between the product ID and the blockchain needed to be mapped by a database which would constitute a single point of trust, in effect meaning that the value added by the blockchain would amount to nothing. Transaction costs and willingness to share data were considered barriers to this solution with one expert claiming the data would be too sensitive. One expert claimed that BCT could reduce the traceability costs, making it easier for smaller actors in the supply chain to adopt traceability systems. One expert noted that even though a blockchain solution could work, there are functioning solutions already on the market. The usefulness of a BCT solution could also depend on the type of goods to be traced. Products like wheat, where goods from multiple producers are mixed during storage and shipping, would be more difficult to trace.

Lack of transparency for customers

Many experts believed that customers want more transparency than what they are being offered today. One expert envisioned sustainability certificates being recorded on the blockchain for customers to access. Question marks regarding the willingness of customers to pay for this solution were, however, raised. Other experts questioned whether the data could be trusted, referencing the issue of garbage in, garbage out, and stated the fact that data does not become more accurate because it is recorded on a blockchain. One expert stated that transparency is not a technology issue, but a business process issue and the introduction of BCT would not alter these business processes.

Lack of transparency for regulators

Many experts argued that even though blockchain can provide a secure record of an assessment or certification having been carried out, there would still be a need for trusted regulators. Once again, the lack of trusted connections between the physical and digital identity of products or companies would make it hard to trust any data stored on the blockchain.

Lack of transparency for financial institutions

Proponents of a blockchain-based solution to this issue stated that blockchain could help avoid forgery of financial documents such as purchase orders and invoices. The caveat was that interoperability between different blockchains has to be ensured for this to truly work. One supply chain expert stated that they were testing use-cases where payments were triggered by smart contracts through IoT load carriers. Another supply chain expert believed that the solution would be especially interesting in global trade. Once again, some experts believed that this information would be better to communicate using a private blockchain solution.

Lack of trust

Lack of trust seemed to be an issue where the experts held many different opinions. Some experts stated that simply through making claims transparent and immutable, trust among actors would naturally increase even though the accuracy of the claims cannot be trusted. Some experts saw the last part of that statement as something that hinders BCT from creating trust among supply chain partners. Other experts argued that trust is something that is created outside of contracts and databases, and that the introduction of BCT would not help this. Scalability was once again considered a drawback of Pub-PL blockchains but one expert expressed hope that current research might improve scalability in the future.

Paperwork

One expert provided a specific example of how BCT could help reduce paperwork. Customs usually require information to be sent before a shipment, with paper copies needing to be submitted when the shipment reaches the customs. BCT could remove the need for this duplicate work. Other experts agreed that the ability to create and hash one instance of a document could reduce the paperwork. Some experts stated that digitalization of processes could solve this issue, regardless of whether it is built on BCT or not. One expert emphasized that the reduction of paperwork depended on how well the traceability system was integrated rather than the underlying data structure. Another expert saw a number of obstacles for development of solutions using blockchain for this mentioning scalability issues and regulations requiring actual paper as documentation.

Counterfeited products

The prospects of BCT in this field seem to hinge on if tamper-proof devices guaranteeing authenticity can be created and if links between the product and its digital representation can be achieved. Identified industries where this solution would be interesting were high margin industries such as luxury fashion, pharmaceuticals and wine. One expert raised the concern of false positives being stored on the blockchain, if a verification code can be successfully copied. Another expert agreed that there is a risk for this but in comparison with today's systems, the counterfeiter could only sell one counterfeited product per copied verification code as the blockchain would raise an alert if several products were sold using the same verification code. One expert also stated that there is always a risk that counterfeiters might corrupt people inside the companies to provide false verification statements.

Lack of security for IoT-devices

Some experts agreed that BCT could restrict communication to verified devices, minimizing the risk of unauthorized access. BCT could make hacking economically unviable, but there might always be hackers who are driven by other incentives. BCT could also flag when data has been manipulated, so that false data could be spotted. Other experts saw IoT security as something that has to be incorporated into the device and that the blockchain cannot provide this. Some experts believed that the attack surface would not diminish with the use of blockchain and that the IoT devices would face the same threats independently of if they post data to the blockchain or not. One expert saw benefits in that even if bad data were posted it would be possible to trace and prove fraud.

Lack of flexibility

Some experts stated that blockchain could increase flexibility through increasing data quality, allowing for better predictions and reactions. But, BCT is neither fast nor flexible. In certain situations, adding BCT could reduce the flexibility as immutability and smart contracts are inflexible to their nature. Still one expert believed that vendor managed inventory with automatic reordering process through smart contracts could improve planning and forecasting.

High supply chain complexity

Many comments focused on how the level of complexity was not directly affected by BCT; the supply chain could however become better at dealing with this complexity. Interoperability between blockchain was once again deemed important to make this work, as is creating incentives for all supply chain actors to want to participate. One expert suggested that complexity could be reduced by storing all data related to a product on the blockchain to have one place to access all information about it. Another expert believed that in the long term smart contracts could decrease complexity.

5.4.3 Applications

Smart tender of transportation

Positive comments usually added the stipulation that the transport sector would have to be interested. There was some concern that large companies might not want to participate in such a solution, as it would lower prices. Lacking the interest of large players, the capacity on the network would be too small to be useful. Interoperability between different blockchains would also be important in the case of international, multi-modal transports. When looking at different use-cases, one expert concluded that this application would probably be most useful for e-commerce goods. Many of the negative respondents stated that a regular auction system would probably do the job as good as a blockchain-based application. The gain for companies purchasing transportation could also be too small when compared to the cost of giving up the traditional relationship with a known provider of transport services.

Improve product traceability

The lack of trust in the conversion from physical status to digital representation would, according to some experts, reduce the usefulness this application. An example was that GPS signals could be faked, although one expert stated that the new Galileo satellite system[24] could give signals that could not be tampered with. A successful implementation would require the participation of all supply chain partners. There was also some concern that such an application would be better to implement on a private blockchain, in order to make sure that actors would share correct information.

Monitor transport conditions

The positive comments envisioned a system were a public blockchain would certify the truthfulness of condition monitoring that would occur on a private blockchain or on another off-chain application. Some experts also envisaged an application running solely on a private blockchain. Trusting the IoT-devices was identified as one of the main problems to this blockchain. Regular database structures could, according to some experts, provide the same benefits and BCT is not therefore a necessary part of the application.

[24] Galileo is a European global satellite based navigation system developed by European Global Navigation Satellite Systems Agency. It is meant as an alternative to the American GPS and Russian GLONASS and to be interoperable with these systems to provide better coverage.

Prove provenance

The experts' comments for this application were similar to those for increasing product traceability, many of the experts saw provenance as a result of traceability. The difficulties of connecting the physical world with its digital representation were once again brought up as an argument against the suitability of this application. Experts who were positive to the application still stated the products needed to have a sufficiently high value to justify the cost.

Improve information sharing

According to experts, BCT is not good at storing large amounts of data but could be used to prove the validity of shared data, through pointers to hashes stored on the blockchain. The problem with latency was also brought up and the question of how fast you need to share information. Different supply chain actors would probably also want to share different amounts of data. Again, the issue of lookup of data in a database based on the ID on the blockchain was brought up.

Verify supply chain activities

One expert saw this as a good use-case as errors could be detected early. An example would be that an end-consumer could see immediately if the wrong goods were loaded at the manufacturer. The verification would however only be as good as the trustworthiness of the person or organization that is making a claim. Even if experts seemed to agree that this would be an interesting application of smart contracts, one expert pointed out that it could be dangerous to set up smart contracts in a volatile supply chain, as smart contracts are inflexible to their nature. Correcting wrongly entered data would also be difficult, due to the immutable nature of BCT. One expert predicted that many of these solutions would start on private blockchains but that public blockchains could probably also be used to good effect.

Create trusted marketplaces without the need for trusted intermediaries

One expert predicted BCT replacing current platform business models and giving more control over personal data. Another saw it simply as the introduction of a new intermediary. Many seemed to agree that for on-chain[25] assets this would be a good application. One blockchain expert brought up the concept of atomic swaps[26] and how

[25] Digital assets that exist only on the blockchain.

[26] Atomic swaps are the exchange of cryptocurrency from two different chains without the need for a trusted third party. It is based on a concept called hash time-locked contracts that ensure that both parties are fulfilling their part of the deal. Additionally it requires certain functions to be implemented on each blockchain involved which currently is just starting to be used, hence it has not been used in a practical way yet. (Madeira, 2018)

they could be extended from being used for cryptocurrencies to also be used for digital representations. This would allow for trading of digital assets between different blockchains. Scalability was once again brought up as a barrier. One expert mentioned the off-chain[27] application of auctioning transport of goods through smart contracts.

Anti-counterfeiting

As in the case of the issue of counterfeited products, the success of this application is dependent on the possibility to create tamper-proof IoT devices. Some experts believed this could be done, while other were more skeptical. Some experts also pointed out the human corruptibility as an issue, as people on the inside could post counterfeited products as originals. Once again, the link between the digital identity and the product was deemed problematic.

Issue targeted recalls

A successful application would require improvements of point of sale technology to track batches. All affected customers would also need to be notified of the recall in order for this to work successfully. In general, there seemed to be some doubt whether BCT would be a crucial building block in this application or whether current traceability systems, if improved, could perform these tasks equally well. There are also some specific issues regarding assigning unique identifiers to products. One expert brought up pigs that, unlike cows, are not given a unique identifier at birth. Processes within plants were mentioned as important for traceability purposes and by putting this information on public display sensitive data about production could be revealed.

Increase Supply chain finance efficiency

Positive comments came with caveats that processes needed to be updated and that full digital representations where necessary. Negative comments believed that this is a good application for BCT, but that it should be implemented on a private blockchain without specifying in more detail why a private blockchain would be more suitable than a Pub-PL blockchain.

Provide secure communication for IoT-devices

Even though this would be theoretically possible according to some experts, it would require incentives to be in place. Incentives could be incorporated into consensus mechanisms but one expert dismissed PoW as being too costly and PoS as requiring

[27] Assets that exist off the blockchain, in this case transportation capacity, but are represented on the blockchain as a digital on-chain asset.

external trust. Another expert saw this application as being possible in three to seven years' time. Some experts said that such a communications channel only gives immutability and not confidentiality and authentication that are also often needed.

Provide infrastructure for M2M-interaction

Negative comments believed that this could be implemented without using BCT. One expert however saw BCT as an emerging standard for M2M-interaction, in an eco-system that currently lacks standards. The use-case of monitoring airplane maintenance was given as an example by an expert that believed that this application could be used for certain, specific use-cases. One expert believed that the use of smart contracts were central but only manageable in a private and permissioned blockchain.

Provide infrastructure for C2M-interaction

One expert stated the need of code that allowed machines to prioritize capacity according to willingness to pay among customers. Another said that it could be useful for 3D-printed replacement parts, but not unique customer orders as customers would require more tailored service. Negative comments either saw current systems as fully functional or envisioned an application based on private blockchains. As in the previous application one expert expressed the opinion that smart contracts on a Pub-PL blockchain was a bad idea.

Reduce paperwork

If the transaction only involves digital representations, this is a suitable application according to one expert. Some experts were skeptical to the necessity of BCT to reduce paperwork. Electronic signatures could for example be used to good effect in many cases, and this does not require BCT. Experts also noted that the legality of BCT transactions could also be a barrier, questioning whether customs would accept blockchain data as valid.

Automate payments and transactions

Smart contracts and the Lightning network[28] were considered building blocks of such an application. It would, however, require updates of the business processes. One

[28] The Lightning Network allows two users to set up a payment channel containing a fixed amount of Bitcoin. The users can then transact using this payment channel. Only the opening and closing of a channel generates a transaction on the Bitcoin blockchain, reducing the amount of transactions on the chain. If user A and user B have opened a channel, and user B and user C have opened a channel, user A can transact with user C through channeling money through both channels. (Torpey, 2017)

expert would rather see this implemented on a private blockchain. Another expert believed this was only suitable for on-chain assets not relying on external conditions. It was also mentioned that firms might not want to automate since they would lose control.

Monitor assets at suppliers

One expert saw this as an interesting use-case for big, unique assets or for large assets in need of regular maintenance such as buildings or airplanes. Some saw this as an application more suitable for private blockchains due to data sensitivity and lack of scalability.

Sharing infrastructure using IoT

The few comments that were given for this application were negative. One pointed out that this is competition-sensitive information and would be better to communicate on a private blockchain. Another simply pointed out that there are better database structures for this application.

6. Discussion

This chapter discusses the result of our Delphi study, compares the results of different panels and contrasts with the findings of the literature review. A general synthesis of the results is applied to the technology adoption framework of Iacovou et al. (1995) Finally, 11 propositions are given, to summarize our finding and to be investigated in future research.

6.1 Analysis of Delphi study

The Delphi study provided some issues and applications that would benefit from BCT. In order to compare the results from different panels easier the results from the Delphi round 3 were interpreted in Table 6.1 and Table 6.2. They can be seen as a more intuitive visualization of Table 5.6 and 5.7. The rating for each panel was transferred to one of five classifications, ranging from "++" to "--", with 0 as the middle classification. The classification of "++" was awarded to issues with a median rating above three and where the lower end of the IQR was strictly larger than three. A "+" was awarded to issues with a median rating above three and where the lower end of the IQR was equal to three. A "0" was awarded to any issues with a median rating of three or where the lower end of the IQR was strictly less than three and the upper end of the IQR was strictly larger than three. The classifications of "-" and "--" were awarded in an inverse manner to those of "+" and "++".

The issues and applications have been sorted according to the total rating, calculated by adding the individual panel ratings together. If two issues had the same total rating, the one where most panels reached consensus was ranked higher. If the same number of panels had reached consensus, the highest panel rating of each issue was used as a final criterion. The ranking should not be considered a strict and final ranking of the issues and applications. It is rather meant as a general guide to the results of the Delphi study.

It should be noted that even for those issues and applications with positive outcomes, the comments are in general negative. The reason for this is that experts with extreme and outlying opinions were specifically asked to provide comments for better understanding of their reasoning. Hence, there could be positive outcomes with only negative comments.

6.1.1 Issues

As can be seen in Table 6.1, and which has been noted earlier, the supply chain expert panel showed larger consensus and were in general more positive in their ratings.

Table 6.1: Classification of Delphi results for the rating of issues. A C within brackets signals consensus.

Issue	*Supply chain experts*	*Academics*	*Blockchain experts*
Lack of upstream traceability	**++ (C)**	0	0
Paperwork	**+ (C)**	0	**+ (C)**
Lack of transparency for customers	**+ (C)**	+	0
Lack of upstream visibility	**+ (C)**	0	0
Lack of downstream traceability	**+ (C)**	0	0
Lack of transparency for financial institutions	**+ (C)**	0	0
Lack of transparency for regulators	0	+	0
Counterfeited products	0	+	0
Lack of downstream visibility	0	0	0
Lack of trust	0	0	0
Lack of security for IoT-devices	0	0	0
Lack of flexibility	0	0	**- (C)**
High supply chain complexity	**0 (C)**	**-- (C)**	0

There are no issues for which all panels have reached consensus around a rating. The three panels had the same ratings for three issues; *Lack of downstream visibility, Lack of trust* and *Lack of security for IoT-devices.* There were no issues where one panel awarded a positive rating while another panel awarded a negative rating. For one issue, *Paperwork*, two panels awarded a positive rating.

In the discussion below, results are classified according to two characteristics. Positive, neutral or negative results refer to whether the panels thought the issues could be solved using Pub-PL BCT or not. Clear results, less clear results and unclear results refer to whether the panels reached consensus internally and whether the three panels agreed with each other's ratings. Clear results occurred when the three panels agreed with each other and a general high level of internal consensus was reached. Less clear results occurred where one panel might diverge in their ratings or where consensus levels were lower, but where we deemed that a sufficiently strong trend among the opinions could be noticed. Unclear results are issues where there were low levels of consensus and the panels disagreed. It is impossible to draw any conclusions for these issues.

Positive results

Clear results

There were few clear conclusions to be made from the expert panels opinions on the identified issues as consensus among Academics and Blockchain experts was rare and clear agreements between the panels were hard to identify. *Paperwork* was the only issue for which a clear conclusion could be made as both Supply chain experts and Blockchain experts found consensus around a rating above three. This indicates that Pub-PL has the potential to solve the issue of excessive paperwork in the supply chain. More neutral opinions were also prevalent in the panels, demonstrated by the fact that the IQR included a rating of three. The academic panel disagreed internally, with responses spread across the scale. Regulatory adoption was cited as an obstacle while some experts with a more negative opinion saw this issue as being solvable with other, existing technologies.

Less clear results

For a few issues a slight positive trend could be spotted. This trend was mostly underpinned by a positive consensus among Supply chain experts, as for *Lack of traceability.* Even though Academics did not reach any consensus on these issues and Blockchain experts were more skeptical, a slight positive trend for at least *Lack of upstream traceability* could be spotted. It should however be noted that this positive trend can be contrasted with many skeptical comments regarding how a physical product can be linked to a digital representation in a trusted manner. This quickly becomes a matter of trust, the role of which will be expanded upon later in this chapter.

Lack of transparency saw a clearer positive trend, especially for *Lack of transparency of customers.* It seems as if for transparency issues, the type of data to be made transparent is important for the possibility to solve this issue using BCT. This relates to earlier comments on how a physical condition could be converted to a digital representation. In the case of regulators, a third-party audit or verification would often still be needed, for example to make a claim that a certain product has been sustainably produced. Trust for these parties would still need to be maintained. For transparency towards customers the issue of willingness to pay was also raised. The customers may be interested in trustworthy data on their products, but are they willing to pay enough to cover the costs of such a solution?

Negative results

Less clear results

Two issues had a slight negative verdict, although not all panels agreed: *Lack of flexibility* and *High supply chain complexity*. Expert comments focused on the inherent inflexibility of BCT, after all the data entered in the blockchain is to stay the same forever which might have implications if the data entered for some reason were incorrect. Comments implied that blockchain interoperability was needed if the complexity should be reduced but overall the experts did not make a connection between lowering complexity and using BCT. Many comments mentioned the poor connection between supply chain complexity and BCT. Academics were very negative to *High supply chain complexity*, while Supply chain experts were neutral. Blockchain experts were negative to *Lack of flexibility* while the other panels had a neutral rating but did not reach consensus.

Unclear results

For a number of issues, no panel reached consensus around their individual ratings, and any conclusions drawn about these issues would be very weakly underpinned. *Lack of visibility* is one of these although the Supply chain experts were positive, with consensus, regarding *Lack of upstream visibility*. Discussions touched upon several aspects of this issue, including business models and whether a private blockchain would be a safer solution for sharing private data. One disagreement, which occurred throughout the study, was whether data on the blockchain could be trusted and if this potential lack of trust meant that any attempts to introduce a blockchain-based solution would be fruitless. This ties into the disagreements around the issue of *Lack of trust*. Two camps among the experts emerged, one that stated that there is no way of ensuring that any data on the blockchain is correct and that existing trust therefore is a prerequisite for any blockchain solution. Others saw a trusted, decentralized database as a way of increasing trust, as any claims made would be immutable and traceable. This seems to be a somewhat circular argument; you have to trust your supply chain partners in order to increase trust in the supply chain. The idea seemed to be that if you could trust the data not to change you would be more prone to trust other actors in the supply chain. Even if the initial data was not correct, these characteristics could increase the levels of trust among supply chain actors. The concept of trust, in relation to BCT and the supply chain, will be discussed in further detail later in this chapter.

BCT as a solution to *Counterfeited products* also saw a lot of disagreement, mainly surrounding the possibility to introduce tamper-free verification methods. In the arguments surrounding the possibility to copy verification tags it was interesting, and a bit surprising, to see that no expert brought up that ownership of products could also be registered on the blockchain. A system where the signature of the owner of the product is required to complete a transaction on the blockchain could be argued to make copying of verification tags useless. Since no expert brought this up, the technical feasibility of such a solution is impossible to judge and it has to be concluded that no clear verdict regarding the potential of BCT to solve the issue of counterfeiting can be made.

Finally, *Lack of security for IoT-devices* also saw high levels of disagreement within the panels. This could perhaps be the most technologically complex of the issues and where the experts pre-existing level of knowledge varied the most. Some comments surrounded the prospects of making hacking economically unviable, but that hacking based other incentives would still prevail. Many experts seemed to believe that security would have to be integrated on a device level and could not be provided through the blockchain.

6.1.2 Applications

In Table 6.2 the processed results for the applications can be seen. Once again, the Supply chain experts are more positive than the other panels. They also generally reached more consensus.

Table 6.2: Classification of Delphi results for the rating of applications. A C within brackets signals consensus.

Application	*Supply chain experts*	*Academics*	*Blockchain experts*
Create trusted marketplaces	**0 (C)**	+ **(C)**	++ **(C)**
Automate payments and transactions	+	0	++ **(C)**
Smart tender of transportation	**0 (C)**	++ **(C)**	**0 (C)**
Improve product traceability	++ **(C)**	0	0
Monitor transport conditions	++ **(C)**	0	0
Reduce paperwork	++ **(C)**	0	0
Provide infrastructure for M2M-interaction	+ **(C)**	**0 (C)**	**0 (C)**
Increase Supply chain finance efficiency	+ **(C)**	0	**0 (C)**
Prove provenance	+ **(C)**	0	0
Verify supply chain activities	+ **(C)**	0	0
Provide infrastructure for C2M-interaction	**0 (C)**	**0 (C)**	**0 (C)**
Improve information sharing	**0 (C)**	0	0
Monitor assets at suppliers	0	0	**0 (C)**
Anti-counterfeiting	0	0	0
Issue targeted recalls	0	0	0
Sharing infrastructure using IoT	0	0	0
Provide secure communication for IoT-devices	0	**- (C)**	0

For four applications, all panels reached consensus around their individual ratings; *Smart tender of transportation*, *Create trusted marketplaces* and *Provide infrastructure for M2M- and C2M-interaction.* Disregarding consensus, the expert panels individually awarded the same rating on six different issues: *Provide infrastructure for C2M-interaction, Improve information sharing, Monitor assets at suppliers, Anti-counterfeiting, Issue targeted recalls, Sharing infrastructure using IoT* and *Provide secure communication for IoT-devices.* For all these issues, the panels awarded the rating of 0. It can further be noted that there was no issue were one panel gave a negative rating while the remaining panels gave a positive rating. Two issues, *Create trusted marketplaces* and *Automate payments and transactions,* saw two panels give a positive rating.

The results are discussed in the same manner as for the issues, using two characteristics to categorize the results.

Positive results

Clear results

Create trusted marketplaces was the application which could be deemed to have the most positive result of all with Blockchain experts being very positive, Academics more slightly so and Supply chain experts being neutral. Overall that means at the very least the Supply chain experts did not think it was a bad idea and the two other panels were positive. What seems to drive this positive view is the use of smart contracts but it is also worth noting that some experts expressed the view that the high rating should be reserved for on-chain assets. By utilizing atomic swaps the intermediary is cut out completely and no trust has to be put in anything else than the chain. As long as the data entered there is correct, or restricting the trade to on-chain assets, this is a good use case. The reason for not receiving strong positive results overall might be related to the issue of scalability and the risk that the blockchain will not be able to handle all needed transactions in reasonable time.

Another application that seems to be related to *Create trusted marketplaces* is *Automate payments and transactions*. This application also got strong positive results in the Delphi study. Blockchain experts agreed on that this was a very good use case with the supply chain panel concurring slightly but without any consensus. This application is close to the current use of BCT, which is mainly about paying and transacting. This is an area the Blockchain experts are familiar with and know how it works. They see solutions that will help this application in the near future, such as the Lightning network. The Supply chain experts seem carefully hopeful while the Academics are more skeptical. Objections against this application are related to which information should be publicly available and that a Pub-PL blockchain might not be the best alternative. Another strong objection is that processes need to be updated if this new technology is implemented. This is not an issue of the technology as such but a challenge in the implementation.

In some respect *Create trusted marketplaces* and *Automate payments and transactions* are closely linked. Both applications are focused on payment and the transfer of value. Perhaps it is not surprising that applications more similar to currently existing uses get higher ratings since it is a smaller step to take compared to more innovative concepts.

Less clear results

Supply chain experts were positive to the application of BCT to *Reduce paperwork*. The private blockchain application of Maersk and IBM, which has advertised a reduction of paperwork, has gained a lot of traction in the supply chain sphere. The Supply chain experts in this study seem to agree that this is a good application even for Pub-PL BCT. A lot of the less enthusiastic comments seem to be based on that BCT is not really necessary to digitize papers or digitalize the supply chain. Some experts were unsure on the legality of documents signed only on the blockchain and thought that perhaps when recognized by authorities such as customs blockchains might be applied to reduce paperwork.

Improve product traceability and *Monitor transport conditions* were very positively viewed by Supply chain experts and the trend in the other panels also seemed to be somewhat positive. The two applications could be seen as linked, both representing some control over where a product has been and in what way it has been treated. Regarding *Monitor transport conditions* there seemed to be mainly three beliefs; the Pub-PL blockchain had to be used in conjunction with a private chain, only a private blockchain would be suitable, or that BCT was not useful in this case at all. Going by some general comments, the view that BCT should not be used at all might be based in that there is no benefit to be gained if the IoT sensors providing the data cannot be secured. This conversion from physical to digital status was also cited as an issue with traceability. Another reason for experts not being more positive was that for such a traceability system to work every party in the supply chain has to participate. If not, the data for ownership would not always be correct.

Provenance was, as mentioned in the comments, often seen as a part of traceability. Hence, it is interesting to note that Supply chain experts thought this was a slightly worse application of BCT than traceability as a whole. Logically, events further upstream in the supply chain should be harder to trace and *Provenance* should therefore be harder to establish than downstream traceability from the point of provenance. *Verify supply chain activities* was, by many experts, also connected to traceability and Supply chain experts saw this as a good application. Smart contracts were envisioned to be used to achieve this, but as data is needed from outside the chain the verification is not trust-less and only as good as the actor verifying that the activity had taken place. As mentioned in the comments smart contracts are inflexible and supply chains often need flexibility. The same issue arises with the incorrect entry of data. Perhaps this would start out, as one expert suggested on private chains, and when the technology has matured, and it is possible to solve more eventualities, Pub-PL blockchains could be used.

Neutral results

Clear results

The suitability of two similar applications was decidedly neutral, *Provide infrastructure for M2M-interaction* and *Provide infrastructure for C2M-interaction.* M2M-interaction was however given a slight positive suitability by Supply chain experts but viewed together with the results from the other panels and the supposed similarities in a solution for C2M-interaction and M2M-interaction the total suitability of these applications is deemed as only being neutral. The comments seem to indicate that some experts can see some uses for Pub-PL BCT in this context. Others stated that there either already exists solutions that are as good as the possible benefit of using BCT, or that an application like this should be on a private blockchain. That Supply chain experts rated the prospects of Pub-PL applications for M2M applications higher than C2M applications could be because they believe that M2M-interactions are easier to control through pre-defined conditions stored in smart contracts while C2M-interactions demand a more flexible approach.

Less clear results

Monitor assets at suppliers was seen as neutral by Blockchain experts and the trend for the other panels was similar. The low amount of comments made it seem like this was something none of the panels felt strongly about. It seems like an implementable application based on the comments but also something that either might be too expensive or something that does not belong on a public blockchain.

Blockchain experts thought that *Increase Supply chain finance efficiency* was neither a good nor a bad application and the other panels did not reach consensus. For the Blockchain experts the difficulty of satisfactorily link data on the blockchain to the outside world seemed to be an issue. Some experts believed this to be a good use case for BCT, not just Pub-PL BCT, and stated that it would also be a good use of private blockchains.

Supply chain experts agreed on that *Improve information sharing* was neither an especially good or bad application of BCT. Experts saw both advantages and disadvantages with BCT in this application. The data on the blockchain is certainly almost immutable but not until after a certain time. This means that the latency of the blockchain might make data useful first after a certain time, which could disqualify the data structure from use in fast moving supply chains. There is also the issue that all data is not meant for totally public viewing and on a public chain some experts expressed doubt that it would be possible to only share the information you want with the parties you want to. Some experts suggested linking the blockchain to off-chain data through hashes, but in general comments made it seem like there could be issues with integrity of this off-chain data. However, that would depend on the way that data was stored.

For *Smart tender of transportation* all three panels reached internal consensus. Academics, who in general were quite restrained in their enthusiasm for the technology, were for this application very positive. This all while the two other panels reached consensus on a neutral suitability. Interestingly the Academics did not argue strongly in their comments for the application or give any specific reasons why this would be a suitable application. It might be that Academics believe in the use of trusted marketplaces where the asset traded in not an on-chain asset, in this case being transport, and hence view the *Smart tender of transportation* as being made on a trusted marketplace. The panels giving a neutral rating were, on the other hand, more vocal in their opinions. It seems like they consider the added value of the blockchain in this case would be minute and that there are other solutions, even current ones, having this functionality. It seems like the benefits of implementing a new solution does not outweigh the cost. Unwillingness by large actors to change systems and difficulty to get the whole supply chain into the same solution generated this lukewarm reaction. Because of the very positive view among Academics, this applications is classified as having positive results. They should however be considered weak, and in need of future validation.

Negative results

Less clear results

Only one application, *Provide secure communication for IoT-devices*, was deemed to be an unsuitable use of blockchain. Academics reached a negative consensus with Blockchain experts showing a slight trend towards also being negative. It seemed like some experts had hopes that this application would be possible in the future while others were completely against the idea, citing fundamental flaws of the technology for this application. They argued that in this case, the data would not benefit from being shared and that there was no guarantee that this data was authentic. This ties into the issue of garbage in, garbage out as the immutability of the data on the chain is to no benefit unless the quality of the data is good.

Unclear results

It was hard to deduce anything from the results on three of the applications. The applications of *Anti-counterfeiting*, *Issues targeted recalls* and *Sharing infrastructure using IoT* all had neutral results with no consensus. Comments suggested that *Anti-counterfeiting* and *Issue targeted recalls* suffered from the same issue, the challenge of identifying specific items and linking them to an identity on the blockchain. The comments regarding *Sharing infrastructure using IoT* were different in that they stated that the information generated from the IoT devices might be sensitive and that there are better data structures for this application.

6.1.3 Connection to SCOR framework

The SCOR framework was used in the literature review to link the identified issues and applications to a supply chain context (see Table 4.15 and Table 4.16). Now that expert views have been collected to judge the potential of BCT to solve these issues and the suitability of this application, it can be worth to revisit this connection to see whether any clear trends emerge.

The issues that had positive ratings were connected to five different Enable processes for managing data, managing agreements, managing compliance, managing risk and managing technology. That Pub-PL BCT, if possible to implement, would affect processes for managing data and managing technology is not surprising as it is a new technology for storing data. The other linked enabling process suggest that Pub-PL BCT will affect how agreements between supply chain partners are managed, how compliance to regulations is demonstrated and how supply chain risk is managed. Pub-PL BCT has an enabling potential to improve processes related to these issues.

The applications that had positive ratings were connected to four different Enable processes for managing performance, managing data, managing agreements and managing procurement. This further strengthens the view that BCT could be an enabling technology when applied in the supply chain, especially in contacts with supply chain partners as part of the procurement process and the processes for managing agreements. The other connected processes were Source or Deliver processes and at the third level they were generally to be found early in the Source process or late in the Deliver processes. BCT has the highest potential to affect processes in the linkages between supply chain actors, either information related to physical state and location of a product, as for verifying incoming goods or financially, as for paying invoices.

The studied system in this thesis, initially introduced in Chapter 3, is shown once again in Figure 6.1. Circles have been added to highlight the affected processes and connections, as discussed above. It should be stressed that the physical flow is not directly affected by the implementation of Pub-PL BCT, as it is an innovation mostly related to the flow of information. However, processes connected to the physical flow, such as verifying incoming goods, need to be changed as a result of the implementation. The need to change physical supply chain processes is something that many experts touched upon in their comments.

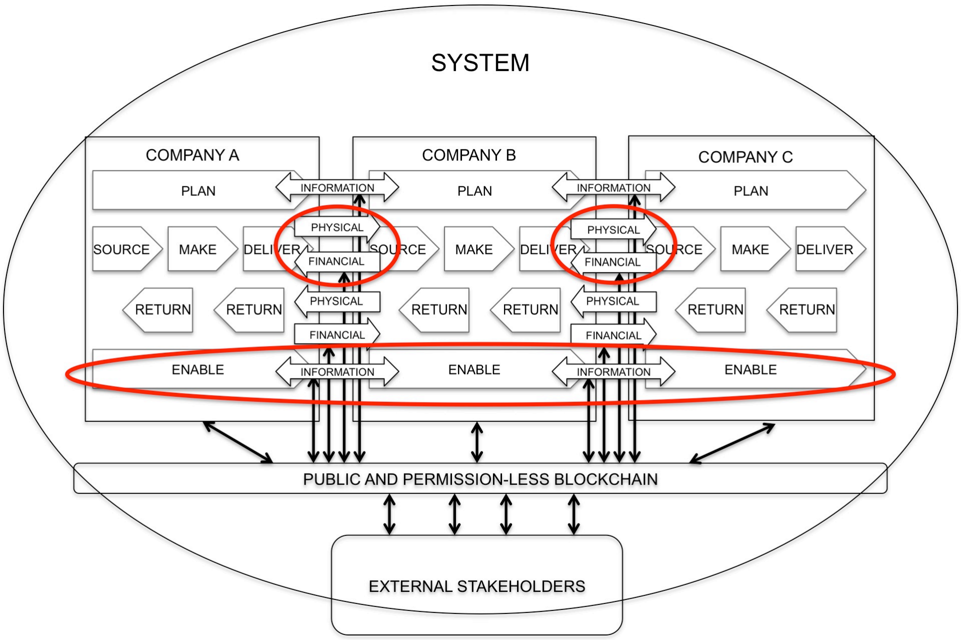

Figure 6.1: The system in this study. The processes and connections affected by those applications and issues that were given positive ratings are highlighted by circles.

6.1.4 Connections between issues and applications

Table 4.15 made an initial connection between the identified issues and applications. The results of the Delphi study could be compared, to see whether this connection holds up. A complete agreement between the ratings of issues and their connected applications should not be expected as a positive rating on a specific application not necessarily means that BCT could solve the, in most cases, broader issue it is connected to.

Applications such as *Improve product traceability, Increase Supply chain finance efficiency, Reduce paperwork, Provide security for IoT-devices* and *Anti-counterfeiting* should be closely linked to their respective issues. In general, the ratings of the issues and the connected applications correspond closely for the respective panels.

In a general comparison of the ratings, the potential of Pub-PL BCT to solve identified issues was rated lower, and with less consensus, than the suitability of identified Pub-PL BCT applications. This could be because issues are broader than specific applications and to state that Pub-PL BCT can solve a broad supply chain issue requires more conviction than to simply state that a certain application is suitable. Evaluating the possibility of Pub-PL BCT to solve an issue is also a more abstract task as no specific concept for how to solve this issue is provided. In that sense, the identified applications are more specific and probably easier to evaluate.

6.2 General themes

Some themes were identified on a more abstract level. These were overarching among the comments of the Delphi study, present for more than one issue or application.

6.2.1 Characteristics of different panels

It seemed like Blockchain experts in general assumed that as much as possible should be trust-less, just as they are used to in their field of work. Many of the Blockchain experts focused on Bitcoin, which might have made them even more prone to have opinions that rejected everything that required more than minimum trust. Supply chain experts on the other hand were more positive in general. It seems fair to assume that they would appreciate any solution that works better than current ones and therefore they are more willing to accept less-than-perfect solutions. It could also be that Supply chain experts are more open to concepts of collaboration and trusting other partners, whereas Blockchain experts want to create a system where trust is not necessary. Academics turned out to be a kind of their own. The result from the Academics panel seems a bit fragmented and so do the comments. This could be because they were recruited from different areas and had different specializations. Perhaps they were very knowledgeable in their own areas but less so in other areas making it difficult for them to evaluate the applications and issues from a common perspective. With different areas of expertise, they might not have been able to reach a higher level of consensus than they did since they held irreconcilable ideas. Another explanation could be that were just not pragmatic and unwilling to accept new facts in this way.

6.2.2 Garbage in, garbage out

This issue was prevalent throughout the questionnaires, with some experts using this exact phrase and others putting it in different words. Garbage in, garbage out refers to that if inaccurate data is entered into the blockchain, any conclusions or decisions made using this data will also be inaccurate. Inaccurate data could be posted by malicious actors, but also as a result of poor measurement systems. This is not a specific issue for BCT but the question is that if this is an issue, does BCT provide any additional benefits compared to existing systems? It would even be possible to argue that because of Pub-PL blockchains' immutability this type of blockchain is less functional compared to existing solutions, as inaccurate data could be posted on the blockchain and remain there in an unalterable state.

6.2.3 Digital representation of physical product

The question of how to connect a digital representation of a product to the characteristics of the actual physical product is related to the issue of garbage in, garbage out. Even if you scan a barcode on an item and receive a list of certain processes have taken place for this product, you cannot know that these in fact took place for that specific product. You still have to trust the actor posting this information on the blockchain.

This issue seemed to be the reason that many applications were disqualified by a lot of experts. Without being able to securely represent a physical product on the blockchain the main point of many applications fails. Many experts doubted that such a link would be possible to make, at least for now, but Supply chain experts seemed to accept a lower level of security than Academics and Blockchain experts.

6.2.4 Privacy of data

Many experts reasoned about the public characteristic of a Pub-PL blockchain. Most experts seemed to view this as a weakness of this particular type of blockchain. They worried that data currently not being shared, or only selectively so, would be available to anyone. This could either render it useless or even hurt the competitiveness of the company.

As a remedy it was suggested to encrypt the data on the chain and only make it available to those with the key to decrypt it. This approach seemed more positively viewed by experts focusing on usability than those that believed that data security should not be compromised. Another approach was to only include a link or some of the data on the blockchain and store the bulk of the data off-chain. Again, more security-minded experts objected to this since then trust would have to be put in the party providing the data storage if it would be alterable after writing. A hash of an individual document could however prove that a document stored off-chain has not been altered, according to the logic of timestamping.

Surprisingly few experts mentioned the positive aspects of having the data publicly available and how it could be applied for benefit, such as in the way Project Provenance Ltd. (2015) has.

As a transacting party in a physical supply chain there is no real possibility to be anonymous and probably it would not be desirable either. Anonymity is one of the main ideas behind Pub-PL blockchains and cryptocurrencies. It is interesting how none of the experts suggested any way to leverage anonymity to be used in any application or for solving any issue. This points towards some discord between SCM and BCT. If there are other benefits of using BCT in the supply chain it is a fair use of the technology but there is an issue regarding having a known identity on a Pub-PL blockchain. With a known identity, i.e. your public keys can be linked to the company making the transactions, miners can choose to discriminate against your transactions. This could mean that you will pay a higher price per transactions, validation of transactions could take longer time or your transaction might not be recorded at all.

6.2.5 Trust

Trust is in many ways related to the three previous themes. There are the questions of whether the data on the chain can be trusted and if the data linked from the chain but stored elsewhere can be trusted. It is clear that the data on the chain can be trusted in the sense that once it is posted on the blockchain it is immutable. Hence, what happens solely on the blockchain can be trusted. The issue is when data has to be submitted from the outside. You will have to trust the actor submitting the data in that it is correct. The data in a supply chain could for example be verifications that a particular task took place or that a certain number of items has been transferred.

The same trust is needed in current systems and the blockchain does not increase the level of trust needed. However, this again raises the question of what BCT then would add to current systems. Trustlessness is only possible for purely on-chain activities and as soon as other information is needed trust has to be invested in other actors. Most experts, however, agreed that once data is posted on the blockchain, it cannot be tampered with without it being discovered. This makes it impossible to cheat in an opportunistic manner, e.g. if a transporter notices that the transported goods have been exposed to too warm conditions he cannot alter the data provided by the IoT-devices if it has already been posted on the blockchain.

There seems to be some confusion or at least disagreement among the experts over the role of trust. *Lack of trust* seems to be something that is both a barrier to blockchain implementation and something that blockchain could potentially solve. This dual relationship could stem from that different types of trust exist in a supply chain. Trust as an antecedent relates to trust that supply chain actors enter accurate data on the blockchain while trust as an effect mainly relates to trust that data once entered has not been altered. Another effect of BCT is that any claims are directly traceable to the actor that made a claim and this traceability could increase honesty of supply chain actors and therefore increase trust. A visualization of this hypothesized relationship is provided in Figure 6.2.

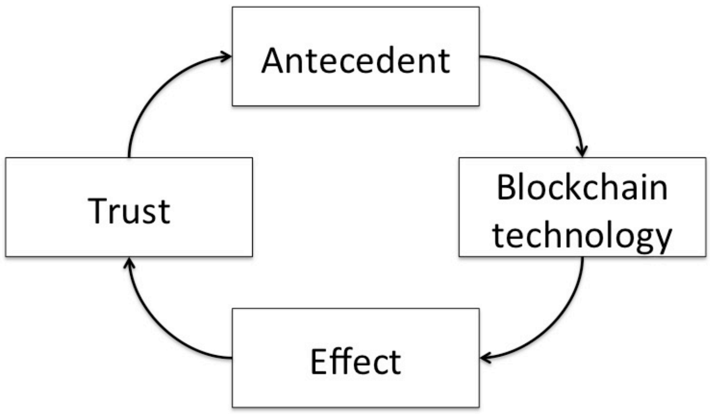

Figure 6.2: The hypothesized relationship between trust and BCT.

6.2.6 Scalability and throughput

For many applications the scalability and throughput of Pub-PL blockchains were questioned. Already in the frame of reference of this thesis, throughput was brought up as an issue of Pub-PL blockchains. In the cases where a Pub-PL blockchains such as Bitcoin would be used for supply chain issues, this problem would be aggravated and the blockchain would possibly be flooded with transactions. This would increase confirmation times of transactions, possibly over the limit of usability of the blockchain for the intended application. The seven transactions per second that the Bitcoin blockchain can offer at the moment seem to simply be too low for any useful application, especially since there are already issues with throughput. Scaling has to be achieved, but the inherent properties of the technology make this a challenge. However, some experts were hopeful that it, in time, this could be solved with some suggesting the Lightning network as a remedy. Currently, through the system being congested with many pending transactions, the transaction fees are also much higher compared to other ways of sending and storing data.

6.2.7 Adoption across supply chain

For many of the applications to be useful the whole supply chain would have to participate. This is clear since if any meaningful traceability is to be achieved no actor can remain outside the system. Making your whole supply chain adopt the BCT could prove incredibly difficult for a number of reasons. Every company has many supply chains and could end up with having to implement many different blockchain solution to be able to continue their business in each one. It creates unnecessary complexity and costs through the needed to implement more than one solution. Another reason would be that it is not certain every actor in the supply chain would benefit from these systems and hence it will be hard to convince them to implement them if they see no benefit. Yet another question is how to handle one-time purchases? You probably would not want to lose the opportunity to make such transactions but at the same time it is unreasonable for one-time suppliers to implement your blockchain solution solely for one transaction.

A possible solution to some of these issues could be standards and inter-blockchain functionality. In some sense a critical mass of users in a supply chain has to adopt a solution and at that point it will force the rest of the actors implement the solution as well, since it has become a prerequisite to do business. This could be the case in industries that are characterized by a few, large actors, who could push implementation across the industry. Large actors could also be an obstacle for adoption. Specifically, big actors in the transport industry were pointed out as possibly negative to implementation of blockchain solutions making smart tender of transportation possible. The reason being according to some experts that price would decrease and that they would lose their competitive advantage of having contracts covering large parts of the market.

6.2.8 Existing solutions

Many times, comments stated that blockchain could solve an issue or be used in an application but at the same time questioned if using blockchain really added any value. In many cases other existing solutions were said to be just as good. If no value is added there is no incentive to develop a new solution. Paperwork could for example be digitalized in other ways and does not necessarily have to be stored on a blockchain.

6.2.9 Comparison with private blockchains

In no question in the Delphi study were the experts asked to compare the Pub-PL BCT with the private one, yet it was commonly brought up in discussions. The experts bringing up the concept of private blockchains favored their implementation in supply chains as they are more scalable, have a higher throughput and can maintain data privacy. This is technically true, but it is also uncertain what then separates a private blockchain from a regular distributed database. It would have been interesting to receive more replies from other experts on the benefits of private blockchains. As this was not the case we provide our own comments here, based on the Frame of Reference in chapter 2 and our general knowledge on the subject. As mentioned in the previous theme there are exist solutions for many applications and issues. For any new technology to be useful it has to add some functionality that was previously not available. Since a private blockchain is controlled by one single entity it is not immutable or irreversible and neither is it trust-less. Even when blockchains are controlled by consortia it requires trust that the controlling parties do not manipulate or discriminate transactions. A private blockchain is, however, somewhat decentralized and perhaps there are gains to be made from storing your data in a decentralized manner. A possible benefit would be that you have no single point of failure should one node break down but in effect it is just a regular distributed database. For certain use-cases it is also unclear whether privacy of data can be upheld in an eco-system of private blockchain. If Company A holds a certification that it can produce 1000 tons of a certified product and has three customers that use three separate blockchain systems, each customer would want insight into its competitor's blockchain to see whether the total amount of certified product sold adds up to less than 1000 tons. This off-chain trading could occur without the presence of other blockchains as well but demonstrates some of the difficulties in navigating the question of private blockchains.

It is unclear what value could be added by implementing a private blockchain but the technology has its proponents and it will be interesting to see the results of highly anticipated projects such as the one of IBM and Maersk. It seems clear, however, that a certain level of trust between supply chain partners is necessary to implement such a blockchain. It seems to be important to really understand what you are aiming at gaining from implementing a blockchain in your choice between the two types.

6.2.10 Synthesis

Many of the identified themes discussed pose challenges in the implementation and use of Pub-PL BCT. These have been divided into two categories: technological challenges and organizational challenges. These categories are shown in Figure 6.3. Garbage in, garbage out features as both a technological and an organizational challenge as it can stem from both insufficient measurement device and insufficient processes.

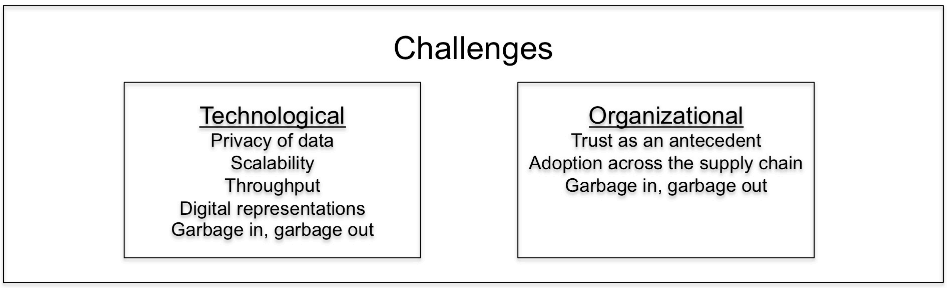

Figure 6.3: Challenges with Pub-PL BCT in supply chain, identified from expert comments in the Delphi study.

Apart from these challenges, the necessity to compare any application of Pub-PL BCT with existing technologies and private BCT was another important theme. This necessity will be expanded upon later in this chapter.

6.3 Comparison of Delphi study with literature review

In general, the Delphi study nuances the claims made in the review research articles and whitepapers. The whitepapers, often being a description of a sellable product, were obviously positive to the applications they suggested. The scientific articles might suffer from positive publication bias and it could also be the case that a new technology like BCT initially attracts academic interests from researchers who strongly believe in the potential of the technology. The Delphi experts in this study were in general more critical and nuanced.

Security for IoT-devices was positively viewed in the literature review, mainly by four scientific articles. In the Delphi study this application and issue was instead viewed with skepticism. It could be that this is so far mainly a concern in certain academic circles, since neither Blockchain experts or Supply chain experts seemed to find this as an interesting application of Pub-PL BCT. It could also be the case that this application is mainly meaningful on a private blockchain and it was therefore not rated highly by the experts. It might also be that the research articles that used Pub-PL blockchains to solve this issue did so simply out of convenience, as Pub-PL blockchains are open source.

Compliance with regulations was discussed by two whitepapers, and although the experts viewed this neutrally many seemed to express concern that regulatory compliance was hard to measure in a trust-less manner. It is for example true that fair trade compliance is difficult to quantify and rely on human inspections on-site. Trust in these inspectors would therefore still be required It could be the case that the companies behind these whitepapers identified BCT as a novel way of storing and sharing data on regulatory compliance but failed to take into account the processes that lead up to a certification of regulatory compliance. Both Kshetri (2018) and Abeyratne and Monfared (2016) also brought up compliance with regulations as a possible use-case. Neither of them discussed the potential data inaccuracy as an obstacle for this, although Kshetri (2018) did touch upon the issue of garbage in, garbage out. It should be noted that the claim that blockchain has "the potential to end unethical and illegal practices" (Kshetri, 2018) seems overoptimistic when compared to the results of this Delphi study. Blockchain does not make it impossible to act unethically or illegally in the supply chain, but it could reduce the incentives to do so.

Information sharing was an application that featured heavily in whitepapers and although the very nature of a distributed database is to share information, experts failed to reach a consensus on the suitability of Pub-PL BCT to improve supply chain information sharing. It can be concluded that Pub-PL BCT is not suitable for all types of information sharing, due to latency and the issue of garbage in, garbage out. The potential of BCT to improve information sharing in general has been overhyped by sellers of application and the results of the Delphi study points to a narrower suitability.

The issues of transparency and traceability, and applications to increase these, were featured in many of the reviewed articles and whitepapers. The results of the Delphi study support the claims that Pub-PL BCT can be applied to increase transparency and traceability of the blockchain, although it comes with the caveats that have previously been discussed in this chapter. In this sense, this study enforces, but also nuances, these themes in earlier work. The issues of transparency and traceability both featured in the review by Kshetri (2018). This study adds to his work by in greater detail describing the challenges and barriers that are necessary to overcome.

The issue of trust, touted in many scientific articles and whitepapers as something blockchain could bring to a supply chain, seems to be more complex than the initial literature review signaled. As mentioned in the general theme of trust, it seems to be both a barrier to blockchain implementation and a something that BCT could bring to a supply chain. Increasing trust seemed like a selling point of many of the whitepapers. Perhaps it was framed as such based on the relative little actual knowledge of the relationship between trust and BCT, making it a statement appealing to make and hard to debunk. The experts in the Delphi study were considerably more skeptical towards the idea that BCT in itself would provide any increase in trust between supply chain actors.

The broad, vague, claims that BCT could increase supply chain flexibility and reduce supply chain complexity could be debunked when looking at the results of this Delphi study. These were mainly brought forward by whitepapers for applications, and possibly only being used to market and hype the solution.

Blockchain interoperability was brought up by Kshetri (2018) and Shen et al. (2017). It was also featured in whitepapers, such as Banerjee (2017), Achain (2015) and Peck (2017).This is something that many experts also stressed and many seemed to envision a future ecosystem of interconnected public and private blockchains, where the advantages of each type are harnessed.

6.4 Technology adoption

We use the framework of Iacovou et al. (1995), initially used to evaluate the adoption of EDI technology, to study the adoption of Pub-PL blockchain in supply chains. It has later been used to evaluate Physical Internet (Sternberg and Norrman, 2017) and to evaluate e-business adoption in both Europe (Oliveira and Martins, 2010) and the United States (Hsu et al., 2006) . In Figure 6.2 the framework is visualized. It should be noted that it is somewhat simplified from Iacovou et al. (1995) by removing the Impact stage. The reason is because this stage implies real experienced impact, a stage that the technology in this study has not yet reached. In the initial work by Iacovou et al. (1995), the framework was used to classify the current adoption level of existing companies, whereas in this study it will be used to identify factors influencing the adoption of Pub-PL BCT in SCM. The expert comments, and the general themes derived from them, will form the basis of this analysis. It will therefore not be a complete mapping, but rather a selection of the most important factors influencing adoption.

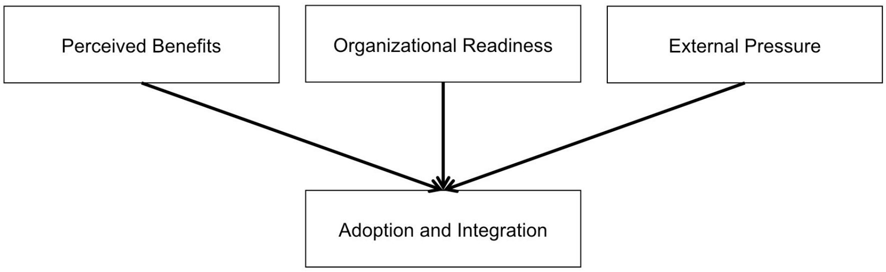

Figure 6.4: Model for technology adoption. Adapted from Iacovou et al. (1995).

Perceived benefits mean the perceived relative advantages of Pub-PL BCT compared to other technologies. Organizational readiness refers to the availability of the needed organizational resources for adoption while External pressure is the pressure from the environment of the firm to introduce BCT. The Adoption and Integration part contains the actual adoption, i.e. development of capability and changes needed to use the technology, but also the integration of the technology into the business. The integration takes the form of both integration of Pub-PL BCT with internal processes and external integration with other supply chain actors. The external integration includes the inter-organizational readiness in terms of, e.g. supply chain collaboration.

6.4.1 Perceived benefits

This study suggests that Pub-PL BCT can provide improved efficiency and improved traceability. The first can be provided through automation of transactions of digital assets, reduction of paperwork and removal of intermediaries when transacting digital assets. These improvements should lead to lower costs as they reduce the needed workforce and reduce costs from using intermediary partners. The benefits of increased traceability need to be quantified on a case-to-case basis. It is unclear whether supply chain partners are willing to pay for this increase and if the supply chain as a whole charge a higher price to end-customers as a result of this increase. This reveals the need for business models that incentivize supply chain partners to participate in blockchain solutions. For example, experts in the study expressed doubts that large transporters would adopt a solution that would cut prices and undermine their role as aggregators of demand. Suitable business models are crucial to realizing benefits of Pub-PL BCT.

Provided benefits also need to be judged against the costs incurred to create these benefits. Apart from a regular cost-benefit analysis of implementing Pub-PL BCT, comparisons with existing technologies and private blockchains need to be made. Expert comments suggested that, for certain applications, existing technologies could provide the same level of performance. The cost comparison between Pub-PL BCT and existing technologies then also has to be performed on a case-to-case basis. For traceability applications, expert comments suggested that Pub-PL BCT would be cheaper than existing technologies, whereas for reducing paperwork the opposite seemed to be true. As private blockchains have not been studied in this thesis, the benefits they could provide are difficult to judge. The cost reduction from implementing a private blockchain in comparison to a Pub-PL BCT would, depending on consensus protocol, come from reduced transaction costs. The implementation of private blockchains could also come with additional security and interoperability costs.

6.4.2 Organizational readiness

In order for a successful adoption of Pub-PL BCT several other puzzle pieces need to be in place within the organization. First, decisions regarding what data the organization is willing to share, and to whom it is willing to share this data, have to be made. An unwillingness to share the data suggests that BCT is not the right technology for storing this data. If the organization is only willing to share this data with selected partners, private and permissioned blockchains might be a more suitable technology.

When these decisions have been made, sufficient data accuracy needs to be ensured. BCT suffers from garbage in, garbage out, and successful adoption requires that data posted on the blockchain can be trusted. This requires investments in technology for collecting data. Establishing a trustworthy link between the physical state of a product and its digital representation is a barrier to blockchain adoption.

6.4.3 External pressure

Depending on the use-case, the attitudes of external stakeholders such as regulators, financial institutions and customers will influence adoption. Regulators and financial institutions could positively influence adoption through choosing to adopt BCT-based solutions, forcing organizations to also adopt these solutions. They could also negatively influence adoption through not accepting data provided by BCT applications as trustworthy or legally valid. This could for example happen in an application for customs clearance if the customs authority decided that signed and stamped paper documentation were still a necessity.

Customers demand will influence the adoption of BCT in customer-oriented use-cases. If customers were interested in trust-less product data, and willing to pay for it, it would have a positive influence on adoption. Many experts believed that customers were interested in knowing more about the origin of their products and the conditions under which they have been produced. There was however some doubt regarding whether they would be willing to pay for access to this information.

6.4.4 Adoption and integration

In order to successfully adopt Pub-PL BCT, the technology and business processes need to be aligned. As the technology is a new way to store and share data, radical changes to processes would be necessary where new data has to be collected or where new platforms, such as marketplaces, built on the technology emerge.

A key factor for a successful implementation of Pub-PL BCT is the integration with supply chain partners. Organizations should therefore focus on integrating a substantial number of upstream and downstream partners to be able to harness the benefits of the technology. Large actors were identified as playing an important role in driving adoption in a supply chain. This also relates to the introduction of business models that incentivize supply chain partners to participate. Interoperability between blockchains could become important for the adoption and integration. Many experts discussed the importance of interoperability between Pub-PL blockchains and private blockchains, as well as the interoperability between different Pub-PL blockchains. A possible situation where this is important is when a supplier serves different industries or different customers and needs to handle different blockchain solutions for each industry or customer.

Figure 6.5 illustrates the identified aspects for the different building blocks in the model proposed by Iacovou et al. (1995). Actors that can influence adoption are regulators, customers and large companies in a supply chain. Processes and technology for ensuring trustworthy data collection need to be in place. A sufficiently large part of the supply chain need to be integrated with the solution to fully realize the benefits. There must also exist a willingness to pay for improvements of, e.g. traceability, with suitable business models to capture provided benefits.

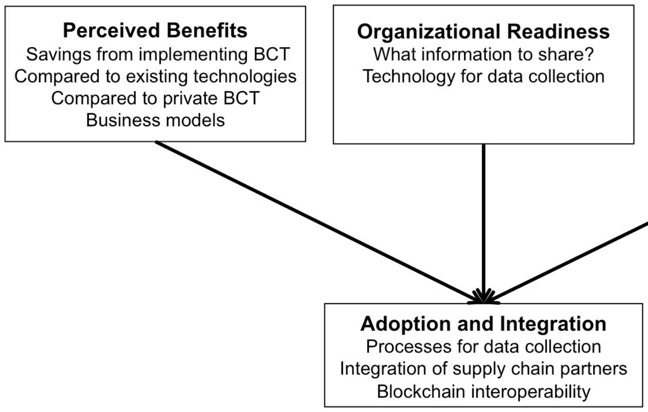

Figure 6.5: The same model as in Figure 6.4 but with identified aspects important for the different building blocks.

6.5 Propositions

Sanchez and Heene (2017) state that propositions can be used as basis for theory building. With this thesis being exploratory one of its main contributions are propositions on which to build further theory. A proposition is a prediction of an outcome in more abstract terms than a hypothesis that might not directly be testable without first being translated into a hypothesis. It can be said to be an assertion of cause and effect.

From the results of the Delphi study, six propositions on the potential of public and permission-less blockchain technology to solve supply chain issues can be stated:

P1. Public and permission-less blockchain technology can improve downstream and upstream product traceability in the supply chain.

P2. Public and permission-less blockchain technology can reduce the amount of paperwork in the supply chain.

P3. Public and permission-less blockchain technology can reduce the need for intermediaries in transactions of digital assets between supply chain partners.

P4. Public and permission-less blockchain technology cannot provide secure communication for IoT-devices in a supply chain environment.

P5. Public and permission-less blockchain technology cannot increase supply chain flexibility.

P6. Public and permission-less blockchain technology cannot decrease supply chain complexity.

Three, more general, propositions on challenges related to the adoption of Pub-PL BCT in the supply chain can also be stated:

P7. Trust in supply chain partners is both an antecedent to, and an effect of, the adoption of public and permission-less blockchain technology.

P8. The supply chain domain is more positive to the prospects of blockchain technology in supply chain management than the blockchain domain, due to different perspectives on trust.

P9. Business models with incentives for all involved supply chain partners need to be in place for adoption of blockchain technology in supply chain management.

Two propositions on the technological aspects of Pub-PL BCT in the supply chain can also be stated. Interdisciplinary research would be valuable for these propositions as they combine technological knowledge with knowledge of the supply chain domain.

P10. It is not possible to create a completely trust-less digital representation of a physical product.

P11. It is not possible to store data on a public blockchain, taking advantage of its characteristics, and keep that data completely private.

7. Conclusion

The purpose of this chapter is to provide answers to the initial purpose and research questions and point out the main contributions of this study. The limitations of the study are also presented and future research paths, as well as managerial implications today, are identified.

The purpose of this study was to evaluate the potential of public and permission--less blockchain technology to solve supply chain issues. This purpose was supported by three research questions:

RQ1: What are supply chain issues that public and permission-less blockchain technology can solve?

RQ2: How can public and permission-less blockchain technology be applied to solve these issues?

RQ3: What are challenges for successful implementation and use of public and permission-less blockchain technology in the supply chain?

The research questions were answered through a Delphi study, informed by an extensive literature review. The Delphi study included Supply chain experts, Academic experts and Blockchain experts. Each group of experts participated in three rounds where they were asked to rate whether Pub-PL BCT could solve identified issues and if identified applications of Pub-PL BCT were suitable for use in the supply chain. The experts were also asked to provide comments arguing for their answers, especially when they held extreme views. These comments were used as basis for the analysis providing the answer for research question 3. The issues and applications were identified in the literature review.

7.1 Findings answering the purpose

On one hand there is research question 1, which gives us a list of issues that can be solved by Pub-PL BCT, and on the other hand there is research question 2, which provides us with more concrete uses of this technology for alleviating the issues. Research question 3 adds another important aspect, the one of challenges related to the implementation and use of Pub-PL BCT in supply chains. Together, these three questions allowed an informed evaluation of the potential of Pub-PL BCT in the supply chain.

The findings of this study can in short be said to be that the potential of Pub-PL BCT to solve supply chain issues lies in providing the tools needed for making transactions and payments automatically and setting up marketplaces without the need for trusted intermediaries. Further it can be used to reducing paperwork and in providing and making traceability and, successively, transparency possible.

The potential seems currently to be the highest in applications which involve only digital assets that uses the inherent security of a blockchain and applications which make sure that the information in a document submitted to the blockchain has not been altered providing trust in the information on the paper. Being willing to trust other supply chain actors, or in the future being able to provide this trust in some technological way, opens up a wider potential. If this trust is present there is a higher potential to solve issues related to traceability and transparency. Trust among supply chain actors was deemed a challenge of implementing Pub-PL BCT in supply chains, along with the challenges to create a trusted digital representation of physical products and that many applications require widespread adoption within the supply chain. There are also challenges more specifically related to the characteristics of Pub-PL BCT, such as low throughput and lack of privacy.

7.2 Research question 1

This study strongly suggests that the amount of paperwork in the supply chain can be reduced using Pub-PL BCT. Large amounts of paperwork are still prevalent in certain industries, e.g. the shipping industry. It further suggests that the lack of upstream and downstream product traceability and the lack of transparency for customers, regulators and financial institutions could be solved using Pub-PL BCT. Lack of traceability relates to the capabilities of a company to know the location, conditions and characteristics of a product before it arrives at the company and after it leaves the company. Lack of transparency applies to information shared with external stakeholders, and if external stakeholders feel that they can trust this information.

The issues evaluated in this study tended to be wide and thus in needed of a combination of technology and processes to be solved in full. The full list of issues evaluated can be seen in Table 7.1. The judgments are based on the Delphi study, where experts were asked to rate the issues according to a five-point Likert scale. From the different ratings of the panels, a general judgment has been estimated. The general judgments take two aspects into accounts: whether there was a general positive or negative rating among the experts, and if there was a sufficiently strong consensus within and between the panels.

Table 7.1: The results of the Delphi study, when judging whether Pub-PL BCT can be used to solve specific supply chain issues. Judgments take into account both the general stance of panels and the levels of consensus.

Judgment	*Issue*
Clear positive	Paperwork
Less clear positive	Lack of transparency
	Lack of traceability
Less clear negative	Lack of flexibility
	High supply chain complexity
Unclear	Lack of security for IoT-devices
	Counterfeited products
	Lack of visibility

From this list it is clear that blockchain is not well suited to solve neither lack of flexibility nor high supply chain complexity. Blockchain is an inherently inflexible technology in that the data submitted to the chain is unchangeable and the rules according to which the blockchain functions are difficult to change. High supply chain complexity was through the Delphi study found to be related more to processes used in the supply chain rather than to which technology is used. Furthermore, the study did not achieve any clear results for the potential to solve the issue of lack of security for IoT-devices, the issue of counterfeited products and the issue of lack of visibility. In general the Supply chain experts reached higher degrees of consensus and were more positive in their ratings compared to the two other groups.

7.3 Research question 2

Based on the issues being wide, a clear link between identified issues and applications for solving them cannot be made. In fact, two applications, to create trusted marketplaces and to automate payments and transactions, had a favorable rating were not directly linked to any of the issues with a favorable rating. The conclusion drawn is that the technology only partly can solve the issues.

This study strongly suggests that Pub-PL BCT can be applied to automate transactions between supply chain partners and can be used to create marketplaces without trusted intermediaries. These applications could potentially use smart contracts to stipulate business rules and conditions. The applications would also use the existing infrastructure surrounding cryptocurrencies, such as Bitcoin. This will, however, only be possible if digital assets are traded. Smart contracts could also be inflexible in rapidly changing supply chain environment. The prospects of creating marketplaces without trusted intermediaries should generate cost savings but also open up for more direct contact between buyers and suppliers. The full list of applications evaluated can be seen in Table 7.2.

Table 7.2: The results of the Delphi study, when judging whether specific applications of Pub-PL BCT are suitable for use in the supply chain. Judgments take into account both the general stance of panels and the levels of consensus.

Judgment	*Application*
Clear positive	Create trusted marketplaces
	Automate payments and transactions
Less clear positive	Reduce paperwork
	Improve product traceability
	Monitor transport conditions
	Prove provenance
	Verify supply chain activities
	Smart tender of transportation
Less clear neutral	Monitor assets at suppliers
	Increase Supply chain finance efficiency
	Improve information sharing
Less clear negative	Provide secure communication for IoT-devices
Unclear	Anti-counterfeiting
	Issue targeted recalls
	Sharing infrastructure using IoT

If some level of trust is present between the supply chain actors the previously mentioned applications are appropriate also for physical assets. With this trust a few more applications can be discerned, specifically using Pub-PL to improve traceability through the whole supply chain and to reduce paperwork. Again, referring to Table 7.2 this corresponds to the applications listed as *Less clear positive.* The improvement in traceability includes proving the provenance of an asset, monitoring the conditions through its transport and verifying that certain supply chain activities has taken place. This would be achieved through creating an identity for the asset on the blockchain to which all information about that asset throughout its lifetime would be linked. The trust needed is in conversion of the physical state of the product to this digital representation, you have to assume that the data uploaded is correct. Once the data has been linked to the blockchain it is impossible to alter that data, making it more difficult to make false claims. It is still unclear whether tamper-proof IoT-devices in some cases can provide the trusted representations necessary, or if trust in the specific actor posting the data is necessary. Pub-PL BCT could also be applied to reduce paperwork through creating a trusted database of statements or verifications that would today be represented through a paper trail.

Less clearly distinguishable results involved some applications on which the judgment from the experts could be taken to mean that they were neither suitable nor unsuitable. In this category were applications meant to monitor assets at the suppliers' sites, increase supply chain efficiency and improve information sharing. The Academic experts were very positive to the smart tender of transportation while the other panels were neutral. According to the experts Pub-PL BCT does not have the potential to provide secure communication for IoT-devices. Unclear results were reached for anti-counterfeiting applications, using BCT for issuing targeted recalls and sharing infrastructure for IoT-devices.

In general, the three panels differed somewhat in their responses. Blockchain experts favored applications that were connected to the current use of BCT, such as automating transactions and creating trusted marketplaces. Supply chain experts were more excited about applications related to product traceability and the reduction of paperwork. The Academic experts were often too internally fragmented to reach a clear positive, or negative, verdict, but strongly favored an application for automating the tender process for transportation.

7.4 Research question 3

Challenges to successful implementation and use of public and permission-less blockchain technology were grouped into two groups, technological challenges and organisational challenges, which can be seen in Figure 7.1. These challenges were identified through the comments given by experts in the Delphi study. The technological challenges are those that are related to the characteristic challenges of Pub-PL BCT, such as the low throughput, low potential for scalability and lack of privacy of data. Throughput and scalability issues follows from the inflexibility of the rules implemented when first starting a public and permission-less blockchain. The throughput is determined by how often new blocks are created and with what intervals. Scalability is hampered by the fact that changing rules once the blockchain is live might lead to forks and disunity in the network. Privacy is by definition lacking in public and permission-less blockchains and if data not intended for everyone is to be stored on this type of blockchain it has to be protected and encrypted in some other way.

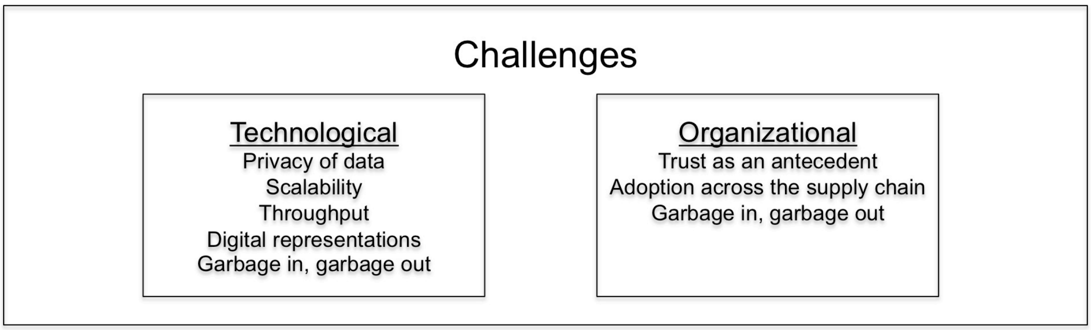

Figure 7.1: Challenges with Pub-PL BCT in supply chain, identified from expert comments in the Delphi study.

Technological issues also includes challenges of technologies for data collection. If the data posted on the blockchain cannot be trusted, the benefits of the technology are greatly reduced. Data entered on the blockchain has to be correct and it is a challenge to make sure that sensors and other sources of data input correct data. A great challenge found in the study was the linking of the digital world of data on the blockchain and the physical world in which the objects it describes exists. These representations were found to be challenging to achieve, and at this time requiring trust between actors to be possible. To eliminate this need for trust would pose a great challenge.

Among the organizational challenges there was a challenge of trust as well. It was found that trust had a two-fold role of both being an antecedent to the use of blockchain technology in all applications, not solely being related to transaction on-chain, and to be increased by the implementation of blockchain technology. For some applications such as traceability, adoption by the entire supply chain is necessary to create meaningful applications for. Garbage in, garbage out was found to be an organizational issue as well in that the quality and usability of the data entered is depending on the which processes are used.

When it came to challenges, the Blockchain experts saw lack of trust and difficulties in creating a trustless connection between the physical conditions of a product and its digital representation on the blockchain as main hinders for successful implementation. It could be said that blockchain experts were generally opposed to solutions where any amount of trust, however small it may be, has to be placed in another actor. The Supply chain experts were more pragmatic in their relationship to trust, seeing it as a challenge but also seeing Pub-PL BCT as potentially improving the existing situation. Once again, the Academic experts were fragmented, a fragmentation that could perhaps come from the fact that they represented different research backgrounds.

7.5 Contribution

As BCT is a rapidly developing field, one of the main contributions of this study has been to provide a snapshot of the field today and contrast it with earlier publications. The hype surrounding BCT and its implications on SCM has made it difficult to correctly evaluate its potential. This study unravels some of the hype; dismissing statements that BCT could increase supply chain flexibility and decrease supply chain complexity. It also enforces statements that BCT could reduce paperwork, increase product traceability, increase transparency in the supply chain, automate transactions and create new marketplaces without the need of intermediaries. The traceability can specifically be improved through monitoring transport conditions, possibility to prove provenance and verification of supply chain activities. The study, however, nuances earlier literature by bringing up, in more detail, the potential challenges that could hinder adoption. These include lack of business models, difficulties in creating digital representations of physical products and lack of trust between supply chain partners. This last caveat opened up a discussion on the duality of trust, as both an antecedent for and a benefit of implementing Pub-PL BCT. This discussion has not been found in previous research.

A summary of which issues and applications that received a positive rating, and where therefore deemed solvable and suitable for Pub-PL BCT, can be seen in Table 7.3.

Table 7.3: The issues and applications that received a positive rating by the Delphi panels.

Judgment	*Issues*
Clear positive	Paperwork
Less clear positive	Lack of transparency Lack of traceability
	Applications
Clear positive	Create trusted marketplaces Automate payments and transactions
Less clear positive	Reduce paperwork Improve product traceability Monitor transport conditions Prove provenance Verify supply chain activities

The Delphi study resulted in ratings of the potential of BCT to solve identified issues and the suitability of identified applications of BCT. These ratings, although not always unambiguous, provide a quantitative view of the opinions of experts within the field. This result can provide a baseline from which to further evaluate the potential of BCT in connection to these issues and applications. By having three different panels current experts' opinions could be probed and contrasted, highlighting the expectations and focus of various groups of professionals relating to the technology. The expertise of the groups was focused on different parts of the concept of BCT in the supply chain and made a critical examination possible.

A qualitative view was provided by the expert comments, which were analyzed and grouped into themes. Many of the themes related to challenges with successful implementation and use of Pub-PL BCT in supply chains. These themes were divided into two categories, technological challenges and organizational challenges.

The identified themes were also used together with the technology adoption framework, proposed by (Iacovou et al., 1995) and seen in Figure 7.2. This analysis provides a view of which factors influence the adoption of Pub-PL BCT in the supply chain. It shows that benefits need to be supported by suitable business models that incentivize all supply chain partners. Data accuracy needs to be improved through technology development. Adoption across the entire supply chain determines adoption and customers, regulators and large supply chain actors play an important role in driving adoption.

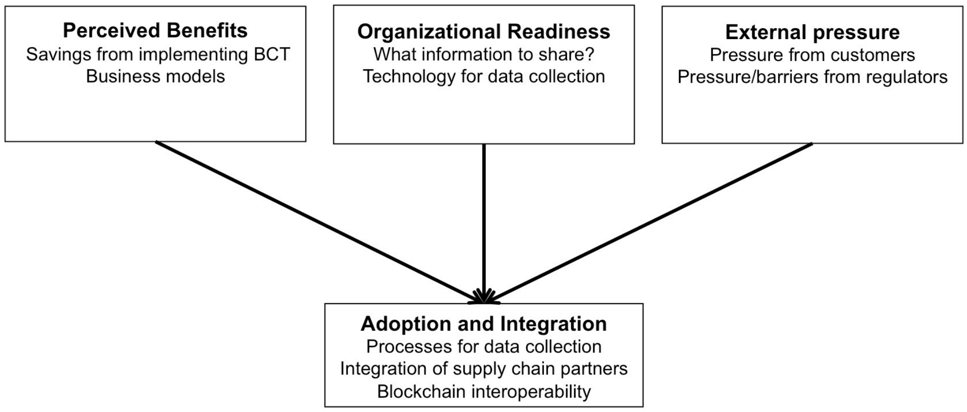

Figure 7.2 Technology adoption model of Iacovou et al. (1995), with relevant aspects for the adoption of Pub-PL BCT in supply chains.

To our knowing, this is the first study to focus on Pub-PL blockchains in supply chain and as such it provides a novel angle from which to view BCT in a supply chain environment. Many of the reviewed articles have been ambiguous on what type of blockchain was studied or studied different types without diving deeper into the differences. In order for the research surrounding BCT in SCM to evolve, the abstraction level of the technology must be reduced so that differences between different types of blockchains are taken into account. The focus of this study allows it to present an evaluation of the potential of Pub-PL blockchains, individually from private and permissioned blockchains. It shows that Pub-PL blockchains have the potential to be implemented in supply chains, but also concludes that more work on the different characteristics and benefits of Pub-PL BCT and private and permissionless BCT needs to be carried out.

7.6 Limitations

Apart from the general limitations of the Delphi study, such as limited generalizability and the risk for compromise rather than consensus, some limitations stem from the way this particular study was conducted. Three main points could be improved: The number of rounds, the number of experts and the choice of experts. All these limitations have their origin in the limited time available through this being a master thesis.

By not having more rounds in the Delphi study it was not ensured that the ratings of the experts reached stability. One of the points of a Delphi study is to let experts influence each other and change opinion, and this should continue until stable results have been achieved. This means that we could have got different results if more rounds had been carried out. More rounds would give a more trustworthy result. An improvement possible with more rounds would have been to spend some time making sure that the experts agreed on common definitions to ensure that they were evaluating the same things. It should also be noted that research participant fatigue could hinder further rounds even if there was time for them.

The number of experts were as explained in the methodology sufficient but the recommendations were to have more experts than this study had. Through not having more experts, important views might have been left out.

The choice of experts could have been more thorough. This follows both from the limited time available but also from the fact that this is a new field where our own networks are limited and there are no appropriate search terms for finding the correct people. Finding people who are knowledgeable about both BCT and SCM is not easy and perhaps not all our experts had an appropriate level of knowledge of both areas. Most experts were found and contacted by us, the only indicator of their expertise being what was found online and their self-assessment in connection to our first Delphi questionnaire.

7.7 Managerial implications

For a supply chain manager this study provides an overview of the proposed applications of Pub-PL BCT in the supply chain and the supply chain issues they claim to solve. The technology has a strong potential to automate payments and transactions in the supply chain and create new marketplaces without the need for trusted intermediaries. Given a supply chain with pre-existing trust among actors, or in a future where technologies for trust-less data collection have been developed, it also has the potential to increase supply chain traceability and transparency.

These findings indicate for managers where among their supply chain processes to begin implementing Pub-PL BCT. The identified issues and the use of the adoption framework also allows for managers to judge whether the pre-conditions and capabilities of their specific supply chain are suitable for implementation of Pub-PL blockchain applications. An important pre-condition is the level of trust among supply chain actors, as a low level of trust in supply chain partners could mean a low level of trust in the data provided to blockchain applications. This would reduce the usefulness of any application as blockchain suffers from the same garbage in, garbage out issues as existing information sharing systems in the supply chain. The introduction of a blockchain application could however reduce the possibilities of opportunistic cheating, adding trust to a supply chain where this is deemed to be an issue. Implementation of certain applications would also require good supply chain cooperation, as many different actors would need to integrate into the application. An important capability to assess before implementing a blockchain solution is the technology and processes for data collection in the supply chain. If accurate data is difficult to collect, the benefits of an application would be reduced due to aforementioned issues of garbage in, garbage out.

7.8 Future research

7.8.1 Academic research

In the SCM field, focus should be on the propositions stated in chapter 6.5 (shown in Table 7.4.)

Table 7.4: Propositions for future research.

Number	*Proposition*
	Potential of Pub-PL BCT
1	Pub-PL BCT can improve downstream and upstream product traceability in the supply chain
2	Pub-PL BCT can reduce the amount of paperwork in the supply chain
3	Pub-PL BCT can reduce the need for intermediaries in transactions of digital assets between supply chain partners
4	Pub-PL BCT cannot provide secure communication for IoT-devices in a supply chain environment
5	Pub-PL BCT cannot increase supply chain flexibility
6	Pub-PL BCT cannot decrease supply chain complexity
	Adoption of Pub-PL BCT
7	Trust in supply chain partners is both an antecedent to, and an effect of, the adoption of Pub-PL BCT.
8	The supply chain domain is more positive to the prospects of BCT in SCM than the blockchain domain, due to different perspectives on trust.
9	Business models with incentives for all involved supply chain partners need to be in place for adoption of BCT in SCM.
	Technology development of Pub-PL BCT
10	It is not possible to create a completely trust-less digital representation of a physical product
11	It is not possible to store data on a public blockchain, taking advantage of its characteristics, and keep that data completely private.

For propositions 1-6, the future research should focus on trying to validate the results of this study. This could be done through detailed case studies as larger pilot projects are being launched. When possible, quantifiable measurements of the effects of Pub-PL BCT in the supply chain should be made.

For propositions 7-9, further studies need to be undertaken to investigate these issues in a more focused manner. The duality of trust was only brought up as a by-product of the Delphi discussion, but could easily be the subject of a study on its own. A lot of the discussion surrounding BCT revolves around the concept of trust and to clarify the different types of trust in a supply chain and what trust BCT can improve would be an important step. This question also relates to how different experts view trust, and the view of trust that is prevalent in the supply chain. Potential research questions could be "When is supply chain trust play a necessary pre-requisite for implementation of Pub-PL BCT?" and "How can Pub-PL BCT increase supply chain trust?”

The two final propositions need to be looked upon from a technological perspective, focusing on whether current or, potentially future, technologies could be used to discard these propositions. This requires interdisciplinary research as computer scientists and supply chain management academics need to cooperate in order to reach answers that are relevant for the use of Pub-PL BCT in the supply chain.

For a number of the identified issues and applications, results were unclear and no conclusions could be made. These include the issues of *Lack of trust*, *Counterfeited products* and *Lack of visibility*, and the applications for *Anti-counterfeiting, Issuing targeted recalls* and *Sharing infrastructure using IoT.* Future research should set out to clarify the potential of Pub-PL BCT for these issues and applications.

7.8.2 Technology development

In terms of technology development, both in terms of the BCT and other, enabling technologies there are gaps to be filled. Critical challenges for Pub-PL BCT are throughput, scalability and privacy, and the work that is being done on these issues at the moment has to be continued and expanded to develop the technology in the future. Enabling technologies that increase trust in the data posted on the blockchain need to be developed to stimulate the adoption of the technology. These include tamper-free IoT-devices for measuring product characteristics and hindering counterfeiting, as well as tamper-proof GPS signals to give trusted locations of products.

The different capabilities of Pub-PL blockchains and private blockchains also need to be examined in more detail. As Pub-PL blockchains have a proven functionality, through the widespread use of Bitcoin, it would be important to understand whether private blockchains can improve this functionality without sacrificing other important characteristics such as security and trustlessness. This question should be easier to answer once private blockchain solutions have been launched for more widespread use.

The business models surrounding the technology also need to be developed, especially to incentivize all partners of the supply chain to adopt the technology. Successful and suitable business models, built on the specific characteristics of Pub-PL BCT, need to be developed in order for mainstream adoption to occur. Research questions here are related to the mapping of costs and benefits across the supply chain. The design of profit- and cost-sharing models could be important to demonstrate that adoption can generate cross-chain benefits.

8. References

ABEYRATNE, S. A. & MONFARED, R. P. 2016. Blockchain ready manufacturing supply chain using distributed ledger.

ACHAIN. 2015. *Achain Blockchain Whitepaper* [Online]. Achain,. Available: https://www.achain.com/Achain Whitepaper 2.0_EN.pdf [Accessed February 21 2018].

ADAMS, R. J., SMART, P. & HUFF, A. S. 2017. Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies. *International Journal of Management Reviews,* 19**,** 432-454.

AKERLOF, G. A. 1970. The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics,* 84**,** 488-500.

AMBROSUS. 2017. *Ambrosus: White Paper* [Online]. Ambrosus. Available: https://ambrosus.com/assets/Ambrosus-White-Paper-V8-1.pdf [Accessed February 21 2018].

AMETRANO, F. M. 2016. About Bitcoin And Blockchain: A Cultural Paradigm Shift. Bank of Italy, Rome.

ANAND, S. 2018. *A Pioneer in Real Estate Blockchain Emerges in Europe* [Online]. Wall Street Journal. Available: https://www.wsj.com/articles/a-pioneer-in-real-estate-blockchain-emerges-in-europe-1520337601 [Accessed April 9 2018].

APICS 2017. SCOR: Supply Chain Operations Reference Model 12.0. APICS.

APODACA, R. 2017. *Six Things Bitcoin Users Should Know about Private Keys* [Online]. Rich Apodaca. Available: https://bitzuma.com/posts/six-things-bitcoin-users-should-know-about-private-keys/ [Accessed May 28 2018].

ARBNOR, I. & BJERKE, B. 2009. Methodology for Creating Business Knowledge. 3rd ed ed. London: SAGE Publications Ltd.

BAHGA, A. & MADISETTI, V. K. 2016. Blockchain platform for industrial Internet of Things. *Journal of Software Engineering and Applications,* 9**,** 533-546.

BANERJEE, A. 2017. *Integrating Blockchain with ERP for a Transparent Supply Chain* [Online]. Infosys. Available: https://www.infosys.com/Oracle/white-papers/Documents/integrating-blockchain-erp.pdf [Accessed February 21 2018].

BANKER, S. 2017. *Blockchain In The Supply Chain: Too Much Hype* [Online]. Forbes. Available: https://www.forbes.com/sites/stevebanker/2017/09/01/blockchain-in-the-supply-chain-too-much-hype/ [Accessed February 21 2018].

BIRKO, S., DOVE, E. S. & ÖZDEMIR, V. 2015. Evaluation of Nine Consensus Indices in Delphi Foresight Research and Their Dependency on Delphi Survey Characteristics: A Simulation Study and Debate on Delphi Design and Interpretation. *PLoS ONE,* 10**,** 1-14.

BLECHSCHMIDT, B. & STÖCKER, C. 2016. *How Blockchain Can Slash the Manufacturing "Trust Tax"* [Online]. Genesis of Things. Available: http://www.genesisofthings.com/pdf/whitepaper.pdf [Accessed February 21 2018].

BOOTH, A., SUTTON, A. & PAPAIOANNOU, D. 2016. *Systematic Approaches to a Successful Literature Review*, SAGE Publications.

BROCKHOFF, K. 1975. The performance of forecasting groups in computer dialogue and face-to-face discussion. *In:* LINSTONE, H. A. & TUROFF, M. (eds.) *The Delphi method: Techniques and applications.* Reading, Massachusetts: Addison-Wesley Educational Publishers Inc.

BROWN, B. B. 1968. Delphi process: A methodology used for the elicitation of opinions of experts. Santa Monica: RAND Corp Santa Monica CA.

BUCK, J. 2017. *Blockchain Oracles, Explained* [Online]. Cointelegraph. Available: https://cointelegraph.com/explained/blockchain-oracles-explained [Accessed April 10 2018].

BUTERIN, V. 2015. *On Public and Private Blockchains* [Online]. Ethereum Blog. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ [Accessed February 21 2018].

CASTOR, A. 2017. *A Short Guide To Bitcoin Forks* [Online]. CoinDesk Inc. Available: https://www.coindesk.com/short-guide-bitcoin-forks-explained/ [Accessed April 10 2018].

CHAKRABARTI, A. & CHAUDHURI, A. K. 2017. Blockchain and its Scope in Retail. *International Research Journal of Engineering and Technology,* 4**,** 3053-3056.

CHEN, Y. Forthcoming 2018. Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Business Horizons*.

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

CHYUNG, S. Y., ROBERTS, K., SWANSON, I. & HANKINSON, A. 2017. Evidence-Based Survey Design: The Use of a Midpoint on the Likert Scale. *Performance Improvement,* 56**,** 15-23.

CLOSS, D. J. & MCGARRELL, E. F. 2004. Enhancing security throughout the supply chain. Washington DC: IBM Center for the Business of Government Washington, DC.

COGNIZANT. 2016. *Blockchain's Smart Contracts: Driving the Next Wave of Innovation Across Manufacturing Value Chains* [Online]. Cognizant. Available: https://www.cognizant.com/whitepapers/blockchains-smart-contracts-driving-the-next-wave-of-innovation-across-manufacturing-value-chains-codex2113.pdf [Accessed February 21 2018].

COINMARKETCAP. 2018. *Cryptocurrency Market Capitalizations* [Online]. CoinMarketCap. Available: https://coinmarketcap.com/all/views/all/ [Accessed February 21 2018].

COLE, Z. D., DONOHOE, H. M. & STELLEFSON, M. L. 2013. Internet-Based Delphi Research: Case Based Discussion. *Environmental Management,* 51**,** 511-523.

COPPOLA, F. 2016. *A Painful Lesson For The Ethereum Community* [Online]. Forbes. Available: https://www.forbes.com/sites/francescoppola/2016/07/21/a-painful-lesson-for-the-ethereum-community/ - 62273e38bb24 [Accessed April 10 2018].

COTTON, M. 2014. *Ethics and Technology Assessment: A Participatory Approach,* Berlin Heidelberg, Springer.

CROSBY, M., NACHIAPPAN, PATTANAYAK, P., VERMA, S. & KALYANARAMAN, V. 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, 6-10.

DALKEY, N. & HELMER, O. 1963. An experimental application of the Delphi method to the use of experts. *Management Science,* 9**,** 458-467.

DELBECQ, A. L., VAN DE VEN, A. H. & GUSTAFSON, D. H. 1975. *Group techniques for program planning: A guide to nominal group and Delphi processes,* Glenview, Illinois, Scott Foresman.

DELOITTE. 2017. *Using blockchain to drive supply chain innovation* [Online]. Deloitte Development LLC. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-blockchain-to-drive-supply-chain-innovation.pdf [Accessed March 28 2018].

DENG, A. & CHEN, Z. 2017. Managing Online Supply Chain finance Credit Risk of "Asymmetric Information". *World Journal of Research and Review,* 4**,** 29-32.

DENYER, D. & TRANFIELD, D. 2006. Using qualitative research synthesis to build an actionable knowledge base. *Management Decision,* 44**,** 213-227.

DIGICONOMIST. 2018. *Bitcoin Energy Consumption Index* [Online]. Digiconomist. Available: https://digiconomist.net/bitcoin-energy-consumption [Accessed March 12 2018].

DROST, E. 2011. Validity and Reliability in Social Science Research. *International Perspectives on Higher Education Research* 38**,** 105-124.

DURACH, C. F., KEMBRO, J. & WIELAND, A. 2017. A New Paradigm for Systematic Literature Reviews in Supply Chain Management. *Journal of Supply Chain Management,* 53**,** 67-85.

ELLRAM, L. M. & COOPER, M. C. 2014. Supply Chain Management: It's All About the Journey, Not the Destination. *Journal of Supply Chain Management,* 50**,** 8-20.

ETHEREUM COMMUNITY. 2016. *Frequently Asked Questions* [Online]. Ethereum Community. Available: http://ethdocs.org/en/latest/frequently-asked-questions/frequently-asked-questions.html - where-do-the-contracts-reside [Accessed February 21 2018].

EVERLEDGER. 2017. *Our technology* [Online]. Everledger. Available: https://www.everledger.io/ [Accessed March 4 2018].

EVRY. 2015. *Blockchain: Powering the Internet of Value* [Online]. Evry. Available: https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf [Accessed February 21 2018].

FEARNLEY, B. 2017. *The Emergence of Blockchain: Seizing Opportunity* [Online]. IDC. Available: https://www.oracle.com/webfolder/s/delivery_production/docs/FY16h1/doc39/IDCTheEmergenceofBlockchain.pdf [Accessed].

FELSON, D. T. 1992. Bias in meta-analytic research. *Journal of Clinical Epidemiology,* 45**,** 885-892.

GALLIVAN, M. Value in triangulation: a comparison of two approaches for combining qualitative and quantitative methods. *In:* LEE, A., LIEBENAU, J. & DEGROSSE, J., eds. International Conference on Information Systems and Qualitative Research, 1997 Philadelphia, Pennsylvania. Springer, 417-443.

GAMMELGAARD, B. 2004. Schools in logistics research?: A methodological framework for analysis of the discipline. *International Journal of Physical Distribution & Logistics Management,* 34**,** 479-491.

GARTNER. 2018. *Gartner Hype Cycle* [Online]. Gartner. Available: https://www.gartner.com/technology/research/methodologies/hype-cycle.jsp [Accessed February 21 2018].

GLOBAL SUPPLY CHAIN FINANCE FORUM 2016. Standard Definition For Techniques of Supply Chain Finance. *Part 3: The standard definitions of SCF Techniques.* Global Supply Chain Finance Forum.

GOLAFSHANI, N. 2003. Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report,* 8**,** 597-607.

GRATZKE, P., SCHATSKY, D. & PISCINI, E. 2017. *Banding together for blockchain* [Online]. Deloitte. Available: https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/emergence-of-blockchain-consortia.html [Accessed February 21 2018].

GROENFELDT, T. 2018. *IBM And Maersk Apply Blockchain To Container Shipping* [Online]. Forbes. Available: https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/ [Accessed February 21 2018].

GUPTA, U. G. & CLARKE, R. E. 1996. Theory and applications of the Delphi technique: A bibliography (1975–1994). *Technological Forecasting and Social Change,* 53**,** 185-211.

HABER, S. & STORNETTA, W. S. 1991. How to time-stamp a digital document. *Journal of Cryptology,* 3**,** 99-111.

HASSON, F. & KEENEY, S. 2011. Enhancing rigour in the Delphi technique research. *Technological Forecasting and Social Change,* 78**,** 1695-1704.

HEISKANEN, A. 2017. The technology of trust: How the Internet of Things and blockchain could usher in a new era of construction productivity. *Construction Research and Innovation,* 8**,** 66-70.

HOFMANN, E. & RÜSCH, M. 2017. Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry,* 89**,** 23-34.

HSU, C. C. & SANDFORD, B. A. 2007a. The Delphi technique: Making sense of consensus. *Practical Assessment, Research and Evaluation,* 12.

HSU, C. C. & SANDFORD, B. A. 2007b. Minimizing NonResponse in The Delphi Process: How to Respond to NonResponse. *Practical Assessment, Research and Evaluation,* 12.

HSU, P.-F., KRAEMER, K. L. & DUNKLE, D. 2006. Determinants of E-Business Use in U.S. Firms. *International Journal of Electronic Commerce,* 10**,** 9-45.

IACOVOU, C. L., BENBASAT, I. & DEXTER, A. S. 1995. Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology. *MIS Quarterly,* 19**,** 465-485.

IANSITI, M. & LAKHANI, K. R. 2017. *The Truth About Blockchain* [Online]. Harvard Business Review. Available: https://hbr.org/2017/01/the-truth-about-blockchain [Accessed February 21 2018].

IBM. 2017. *IBM Announces Major Blockchain Collaboration with Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever and Walmart to Address Food Safety Worldwide* [Online]. Armonk, N.Y: IBM. Available: http://www-03.ibm.com/press/us/en/pressrelease/53013.wss? [Accessed].

IBM. 2018. *IBM Blockchain based on Hyperledger Fabric from the Linux Foundation* [Online]. https://www.ibm.com/blockchain/hyperledger.html. Available: https://www.ibm.com/blockchain/hyperledger.html [Accessed February 21 2018].

INBOUND LOGISTICS. 2017. *GOOD QUESTION. What's the difference between supply chain visibility and transparency?* [Online]. Inbound Logistics. Available: http://www.inboundlogistics.com/cms/article/good-question-whats-the-difference-between-supply-chain-visibility-and-transparency/ [Accessed 25 April 2018].

ITO, J., NARULA, N. & ALI, R. 2017. *The Blockchain Will Do to the Financial System What the Internet Did to Media* [Online]. Harvard Business Review. Available: https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media [Accessed March 28 2018].

JABBAR, K. & MACDONALD, D. 2016. *Container Streams: A DLT-based system for the shipping industry fostering complete interoperability through customizable adapters* [Online]. Blockchain Labs for Open Collaboration. Available: https://www.un-bloc.com/wp-content/uploads/MTI-White-Paper-Container-Streams1.pdf [Accessed February 21 2018].

JAFFE, J. 2018. *Initial coin offerings, explained* [Online]. cnet. Available: https://www.cnet.com/how-to/initial-coin-offerings-explained/ [Accessed May 29 2018].

JARADAT, R., ADAMS, F., ABUTABENJEH, S. & KEATING, C. 2017. The Complementary Perspective of System of Systems in Collaboration, Integration, and Logistics: A Value-Chain Based Paradigm of Supply Chain Management. *Systems,* 5**,** 50.

KACINA, J., HARLER, M. C. & RAJNIC, M. 2017. *SophiaTX Whitepaper: The Blockchain for Business* [Online]. SophiaTX. Available: https://www.sophiatx.com/_data/_custom/SophiaTX_Whitepaper_v1.9.pdf [Accessed February 21 2017].

KEENEY, S., HASSON, F. & MCKENNA, H. P. 2001. A critical review of the Delphi technique as a research methodology for nursing. *International Journal of Nursing Studies,* 38**,** 195-200.

KENNEDY, Z. C., STEPHENSON, D. E., CHRIST, J. F., POPE, T. R., AREY, B. W., BARRETT, C. A. & WARNER, M. G. 2017. Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology. *Journal of Materials Chemistry C,* 5**,** 9570-9578.

KHAN, M. A. & SALAH, K. 2018. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems,* 82**,** 395-411.

KRUGMAN, P. 2009. *The Return of Depression Economics and the Crisis of 2008,* New York, W. W. Norton.

KSHETRI, N. 2017. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy,* 41**,** 1027-1038.

KSHETRI, N. 2018. 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management,* 39**,** 80-89.

KUSRINI, E., SUBAGYO & MASRUROH, N. A. 2014. Good criteria for supply chain performance measurement. *International Journal of Engineering Business Management,* 6.

LA ROSA, M., LOOS, P. & PASTOR, O. 2016. *Business Process Management. 14th International Conference, BPM 2016, Rio de Janeiro, Brazil, September 18-22, 2016. Proceedings*, Cham : Springer International Publishing : Imprint: Springer, 2016.

LEDGER. 2018. *Check the list of cryptocurrencies and tokens supported by Ledger here* [Online]. Ledger. Available: https://support.ledgerwallet.com/hc/en-us/articles/115005304449-Check-the-list-of-cryptocurrencies-and-tokens-supported-by-Ledger-here [Accessed April 10 2018].

LEE, J.-H. & PILKINGTON, M. 2017. How the Blockchain Revolution Will Reshape the Consumer Electronics Industry [Future Directions]. *IEEE Consumer Electronics Magazine,* 6**,** 19-23.

LEFKOTHEA, G. & EFTHIMIOS, Z. 2014. Using Delphi technique to build consensus in practice. *Int. Journal of Business Science and Applied Management,* 9**,** 66-82.

LEMAY, S., HELMS, M. M., KIMBALL, B. & MCMAHON, D. 2017. Supply chain management: the elusive concept and definition. *International Journal of Logistics Management,* 28**,** 1425-1453.

LI, Z., WANG, W., LIU, G., LIU, L., HE, J. & HUANG, G. 2018. Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing. *Industrial Management & Data Systems,* 118**,** 303-320.

LINCOLN, Y. S. & GUBA, E. G. 1985. *Naturalistic Inquiry,* Newbury Park, California, SAGE Publications.

LINSTONE, H. A. 1978. The Delphi Technique. *In:* FOWLES, J. (ed.) *Handbook of futures research.* Westport, Connecticut: Greenwood Publishing.

LUDLOW, J. D. 1970. The Delphi method: a systems approach to the utilization of experts in technological and environmental forecasting. Ann Arbor, Michigan: Bureau of Business Research, Graduate School of Business Administration, University of Michigan.

MADEIRA, A. 2018. *What Are Atomic Swaps?* [Online]. Available: https://www.cryptocompare.com/coins/guides/what-are-atomic-swaps/ [Accessed April 24 2018].

MAX, K. 2017. Cryptocurrency Secrets. Lulu

MCCONAGHY, M., MCMULLEN, G., PARRY, G., MCCONAGHY, T. & HOLTZMAN, D. 2017. Visibility and digital art: Blockchain as an ownership layer on the Internet. *Strategic Change-Briefings in Entrepreneurial Finance,* 26**,** 461-470.

MELANIE, A. R., WILLEM, E. S. & JON, A. K. 2013. Choosing the Number of Categories in Agree–Disagree Scales. *Sociological Methods & Research,* 43**,** 73-97.

MENTZER, J. T., DEWITT, W., KEEBLER, J. S., MIN, S., NIX, N. W., SMITH, C. D. & ZACHARIA, Z. G. 2001. Defining Supply Chain Management. *Journal of Business Logistics,* 22**,** 1-25.

MICROSOFT. 2018. *Blockchain technology | Microsoft Azure* [Online]. Microsoft. Available: https://azure.microsoft.com/en-us/solutions/blockchain/ [Accessed February 21 2018].

MODUM. 2017. *Data Integrity for Supply Chain Operations, powered by blockchain technology* [Online]. Available: https://modum.io/wp-content/uploads/2017/08/modum-whitepaper-v.-1.0.pdf [Accessed February 21 2018].

MORABITO, V. 2017. Business Innovation Through Blockchain. Springer International Publishing.

MORSE, J. M. 1991. Approaches to Qualitative-Quantitative Methodological Triangulation. *Nursing Research,* 40**,** 120-123.

NAKAMOTO, S. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System* [Online]. www.bitcoin.org. Available: https://bitcoin.org/bitcoin.pdf [Accessed February 21 2018].

NAKAMOTO, S. 2009. *Bitcoin v0.1 released* [Online]. The Mail Archive. Available: https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html [Accessed February 21 2018].

NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A. & GOLDFEDER, S. 2016. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University.

NATARAJAN, H., KRAUSE, S. K. & GRADSTEIN, H. L. 2017. Distributed Ledger Technology (DLT) and blockchain. *Fintech note.* Washington DC: World Bank Group.

NDRAHA, N., HSIAO, H.-I., VLAJIC, J., YANG, M.-F. & LIN, H.-T. V. 2018. Time-temperature abuse in the food cold chain: Review of issues, challenges, and recommendations. *Food Control,* 89**,** 12-21.

NELSON, J. S., HENDERSON, D., JONES, G., ROON, M., ZARGHAM, M., BULKIN, A., BRUKHMAN, J. & ROWE, K. 2017. *A blockchain-based protocol stack for global commerce and supply chains* [Online]. Sweetbridge. Available: https://sweetbridge.com/public/docs/Sweetbridge-Whitepaper.pdf [Accessed February 21 2018].

NOTANI, R. 2017. *Can Blockchain Revolutionize the Supply Chain?* [Online]. OneNetwork. Available: http://www.supplychain247.com/paper/can_blockchain_revolutionize_the_supply_chain [Accessed].

NOTHEISEN, B., CHOLEWA, J. B. & SHANMUGAM, A. P. 2017. Trading Real-World Assets on Blockchain An Application of Trust-Free Transaction Systems in the Market for Lemons. *Business & Information Systems Engineering,* 59**,** 425-440.

O'LEARY, D. E. 2017. Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. *Intelligent Systems in Accounting Finance & Management,* 24**,** 138-147.

OKOLI, C. & PAWLOWSKI, S. D. 2004. The Delphi method as a research tool: an example, design considerations and applications. *Information & Management,* 42**,** 15-29.

OLIVEIRA, T. & MARTINS, M. F. 2010. Understanding e-business adoption across industries in European countries. *Industrial Management & Data Systems,* 110**,** 1337-1354.

OUDE WEERNINK, M., VAN DEN ENGH, W., FRANCISCONI, M. & THORBORG, F. 2017. *The blockchain potential for port logistics* [Online]. SmartPort. Available: http://smart-port.nl/wp-content/uploads/2017/06/Bijlage-6_White-Paper-Blockchain.pdf [Accessed February 21 2018].

OXFORD DICTIONARIES 2018. *expert | Definition of expert in English by Oxford Dictionaries,* Oxford, Oxford University Press.

PANETTA, K. 2017. *Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017* [Online]. Gartner. Available: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/ [Accessed February 21 2018].

PECK, M. 2017. *Reinforcing the links of the blockchain* [Online]. IEEE. Available: https://blockchainincubator.ieee.org/images/files/pdf/ieee-future-directions-blockchain-white-paper.pdf [Accessed February 21 2018].

POPAY, J., ROGERS, A. & WILLIAMS, G. 1998. Rationale and Standards for the Systematic Review of Qualitative Literature in Health Services Research. *Qualitative Health Research,* 8**,** 341-351.

POPPER, N. 2017a. *Move Over, Bitcoin. Ether Is the Digital Currency of the Moment* [Online]. The New York Times. Available: https://www.nytimes.com/2017/06/19/business/dealbook/ethereum-bitcoin-digital-currency.html [Accessed February 21 2018].

POPPER, N. 2017b. *Understanding Ethereum, Bitcoin's Virtual Cousin* [Online]. The New York Times. Available: https://www.nytimes.com/2017/10/01/technology/what-is-ethereum.html [Accessed February 21 2018].

PREUVENEERS, D., JOOSEN, W. & ILIE-ZUDOR, E. 2017. Trustworthy data-driven networked production for customer-centric plants. *Industrial Management & Data Systems,* 117**,** 2305-2324.

PROJECT PROVENANCE LTD. 2015. *Blockchain: the solution for transparency in product supply chains* [Online]. Project Provenance Ltd.,. Available: https://www.provenance.org/whitepaper [Accessed February 21 2018].

PROJECT PROVENANCE LTD. 2016. *From shore to plate: Tracking tuna on the blockchain* [Online]. Project Provenance Ltd.,. Available: https://www.provenance.org/tracking-tuna-on-the-blockchain [Accessed April 18 2018].

PROTOCOL LABS. 2018. *IPFS is the distributed web* [Online]. IPFS. Available: https://ipfs.io/ - how [Accessed April 9 2018].

PRYBILA, C., SCHULTE, S., HOCHREINER, C. & WEBER, I. Forthcoming 2018. Runtime verification for business processes utilizing the Bitcoin blockchain. *Future Generation Computer Systems*.

RABAH, K. 2017. Challenges & Opportunities for Blockchain Powered Healthcare Systems: A Review. *Mara Research Journal of Medicine & Health Sciences* 1**,** 45-52.

RAKIC, B., LEVAK, T., DREV, Z., SAVIC, S. & VELJKOVIC, A. 2017. *First purpose built protocol for supply chains based on blockchain* [Online]. OriginTrail. Available: https://origintrail.io/storage/documents/OriginTrail-White-Paper.pdf [Accessed February 21 2018].

RAVAL, S. 2016. *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology,* Sebastopol, California, O'Reilly Media.

RIPPLE. 2018. *rippled Setup* [Online]. Ripple. Available: https://ripple.com/build/rippled-setup/ [Accessed April 8 2018].

ROBERTSON, J. 2018. *Digital Revolution Demands Changes To Education* [Online]. Forbes. Available: https://www.forbes.com/sites/gradsoflife/2018/03/06/digital-revolution-demands-changes-to-education/ - 286f99ee589c [Accessed April 10 2018].

ROSENBAUM, R. & BOLSTORFF, P. 2003. *Supply Chain Excellence: A Handbook for Dramatic Improvement Using the SCOR Model,* New York American Management Association International.

ROSIC, A. 2017. *What is hashing? Under the hood of the blockchain* [Online]. Blockgeeks. Available: https://blockgeeks.com/guides/what-is-hashing/ [Accessed February 21 2018].

ROWE, G., WRIGHT, G. & BOLGER, F. 1991. Delphi: A reevaluation of research and theory. *Technological Forecasting and Social Change,* 39**,** 235-251.

ROWLEY, J. & HARTLEY, R. 2008. *Organizing Knowledge: An Introduction to Managing Access to Information,* Ashgate, Ashgate Publishing Ltd.

ROWLEY, J. & SLACK, F. 2004. Conducting a literature review. *Management Research News,* 27**,** 31-39.

ROWLISON, S. & HOLMAN, G. K. 2018. *A De-centralised Accounting System for Commerce and Industry: 06th February 2018. 12:00 UTC.* [Online]. BBiller. Available: https://bbiller.com/wp-content/uploads/2018/02/bBiller-Whitepaper-February-2018.V1.1.pdf [Accessed February 21 2018].

RUMRILL, P. D., JR. & FITZGERALD, S. M. 2001. Using narrative literature reviews to build a scientific knowledge base...this is the first in a series of three articles. *Work,* 16**,** 165-170.

SABERI, S., KOUHIZADEH, M. & SARKIS, J. 2018. Blockchain technology: A panacea or pariah for resources conservation and recycling? *Resources, Conservation and Recycling,* 130**,** 80-81.

SAMUEL, H. H., SUNIL, K. S. & GE, W. 2004. A review and analysis of supply chain operations reference (SCOR) model. *Supply Chain Management: An International Journal,* 9**,** 23-29.

SANCHEZ, R. & HEENE, A. 2017. Building Theory for Management Science and Practice: An Epistemological Perspective from Competence-Based Management Theory. *In:* SANCHEZ, R., HEENE, A., POLAT, S. & ASAN, U. (eds.) *Mid-Range Management*

Theory: Competence Perspectives on Modularity and Dynamic Capabilities. Emerald Publishing Limited.

SCHATSKY, D. & MURASKIN, C. 2015. *Beyond Bitcoin* [Online]. Deloitte Insights: Deloitte. Available: https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/trends-blockchain-bitcoin-security-transparency.html [Accessed February 21 2018].

SHAPIRA, A. & LEINZ, K. 2017. *Long Island Iced Tea Soars After Changing Its Name to Long Blockchain* [Online]. Bloomberg. Available: https://www.bloomberg.com/news/articles/2017-12-21/crypto-craze-sees-long-island-iced-tea-rename-as-long-blockchain [Accessed February 2018 2018].

SHARMA, S. R. 2017. Blockchain Technology Review and Its Scope. *International Research Journal of Engineering and Technology,* 4**,** 1070-1073.

SHEN, J., HUANG, Y. & CHAI, Y. 2017. A cyber-anima-based model of material conscious information network. *International Journal of Crowd Science,* 1**,** 9-25.

SHIPCHAIN. 2017. *Shipchain: The Whitepaper* [Online]. Shipchain. Available: https://shipchain.io/shipchain-whitepaper.pdf [Accessed February 21 2018].

SHIRRIFF, K. 2014. *Bitcoins the hard way: Using the raw Bitcoin protocol* [Online]. Ken Shirriff. Available: http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html [Accessed May 28 2018].

SIKORSKI, J. J., HAUGHTON, J. & KRAFT, M. 2017. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy,* 195**,** 234-246.

SINHA, I. P., SMYTH, R. L. & WILLIAMSON, P. R. 2011. Using the Delphi Technique to Determine Which Outcomes to Measure in Clinical Trials: Recommendations for the Future Based on a Systematic Review of Existing Studies. *PLoS Medicine,* 8**,** e1000393.

SKWAREK, V. 2017. Blockchains as security-enabler for industrial IoT-applications. *Asia Pacific Journal of Innovation and Entrepreneurship,* 11**,** 301-311.

SMART CONTRACTS ALLIANCE & DELOITTE. 2016. *Smart Contracts: 12 Use Cases for Business & Beyond* [Online]. Chamber of Digital Commerce. Available: https://bloq.com/assets/smart-contracts-white-paper.pdf [Accessed February 21 2018].

SMITH, J. 2016. *Blockfreight™ the blockchain for*

global freight [Online]. Blockfreight. Available: https://bravenewcoin.com/assets/Whitepapers/BlockfreightWhitepaperFinalDraft.pdf [Accessed February 21 2018].

STAFFORD, P. & MURPHY, H. 2016. *Has the blockchain hype finally peaked?* [Online]. The Financial Times. Available: https://www.ft.com/content/5e48f9ec-b651-11e6-ba85-95d1533d9a62 [Accessed February 21 2018].

STAKE, R. E. 2010. *Qualitative Research: Studying How Things Work,* New York, Guilford Publications.

STERNBERG, H. & NORRMAN, A. 2017. The Physical Internet – review, analysis and future research agenda. *International Journal of Physical Distribution and Logistics Management,* 47**,** 736-762.

STEWART, T. R. 1987. The Delphi technique and judgmental forecasting. *Climatic Change,* 11**,** 97-113.

SWAN, M. 2015. *Blockchain: Blueprint for a New Economy,* Sebastopol, California, O'Reilly Media, Inc.

SWAN, M. 2017. Anticipating the Economic Benefits of Blockchain. *Technology Innovation Management Review,* 7**,** 6-13.

SWANSON, E. 2014. Validity, Reliability, and the Questionable Role of Psychometrics in Plastic Surgery. *Plastic and reconstructive surgery. Global open,* 2**,** e161.

SYNCFAB. 2018. *Decentralized Manufacturing: Creating the world's first peer-to-peer manufacturing supply chain and incentivized token system adapted for public and private blockchains* [Online]. Available: https://blockchain.syncfab.com/SyncFab_MFG_WP.pdf [Accessed February 21 2018].

SZABO, N. 1996. Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought,* 16.

THE ECONOMIST. 2015. *Who is Satoshi Nakamoto?* [Online]. Available: https://www.economist.com/blogs/economist-explains/2015/11/economist-explains-1 [Accessed April 24 2018].

THE ECONOMIST. 2016. *The DAO of accrue* [Online]. The Economist. Available: https://www.economist.com/news/finance-and-economics/21699159-new-automated-investment-fund-has-attracted-stacks-digital-money-dao [Accessed April 10 2018].

THE LINUX FOUNDATION. 2018. *About Hyperledger* [Online]. The Linux Foundation. Available: https://www.hyperledger.org/about [Accessed May 28 2018].

TORPEY, K. 2017. *Will Bitcoin's Lightning Network Kill Off Altcoins Focused On Cheap Transactions?* [Online]. Forbes. Available: https://www.forbes.com/sites/ktorpey/2017/12/28/will-bitcoins-lightning-network-kill-off-altcoins-focused-on-cheap-transactions/ - 694d6b347dab [Accessed May 10 2018].

TRANFIELD, D., DENYER, D. & SMART, P. 2003. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management,* 14**,** 207-222.

TRÜEB, H. R. 2018. Smart Contracts. *In:* GROLIMUND, P., KOLLER, A., LOACKER, L. D. & PORTMANN, W. (eds.) *Festschrift für Anton K. Schnyder.* Zürich: Schulthess Juristische Medien AG, Zürich.

VAN DER MEULEN, R. & PETTEY, C. 2017. *Gartner's Hype Cycle Reveals the Digitalization of the Supply Chain* [Online]. Gartner. Available: https://www.gartner.com/newsroom/id/3798863 [Accessed 24 April 2018].

VERNON, W. 2009. The Delphi technique: A review. *International Journal of Therapy & Rehabilitation,* 16**,** 69-76.

VON DER GRACHT, H. 2008. *The Future of Logistics – Scenarios for 2025,* Wiesebaden, Betriebswirtschaftlicher Verlag Dr. Th. Gabler.

WHITE, G. R. T. 2017. Future applications of blockchain in business and management: A Delphi study. *Strategic Change-Briefings in Entrepreneurial Finance,* 26**,** 439-451.

WHITE, M. 2018. *Digitizing Global Trade with Maersk and IBM* [Online]. IBM. Available: https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/ [Accessed February 21 2018].

WINKLER, J. & MOSER, R. 2016. Biases in future-oriented Delphi studies: A cognitive perspective. *Technological Forecasting and Social Change,* 105**,** 63-76.

WOODSIDE, J. M., AUGUSTINE JR, F. K. & GIBERSON, W. 2017. Blockchain Technology Adoption Status and Strategies. *Journal of International Technology and Information Management,* 26**,** 65-93.

XU, X., WEBER, I., STAPLES, M., ZHU, L., BOSCH, J., BASS, L., PAUTASSO, C. & RIMBA, P. A Taxonomy of Blockchain-Based Systems for Architecture Design. 2017 IEEE International Conference on Software Architecture (ICSA), 3-7 April 2017 2017 Gothenburg. IEEE, 243-252.

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.

ZAMFIR, V. 2015. *Introducing Casper "the Friendly Ghost" - Ethereum Blog* [Online]. Available: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/ [Accessed February 21 2018].

ZHENG, Z., XIE, S., DAI, H., CHEN, X. & WANG, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *In:* KARYPIS, G. & ZHANG, J., eds. 2017 IEEE International Congress on Big Data (BigData Congress), 25-30 June 2017 2017 Honolulu, HI. IEEE, 557-564.

Appendices

Appendix A. SCOR framework

There are five first-level processes in the SCOR framework. Each one is described in detail below.

Plan

The planning process in the SCOR model is an overarching process, vital for the successful execution of the other processes (Rosenbaum and Bolstorff, 2003, p. 7). On the first level, planning can be considered as the practice of balancing supply and demand and developing a plan to meet the requirements on sourcing, manufacturing, delivery and returns (Rosenbaum and Bolstorff, 2003, p. 7). On the second level, when broken down using APICS (2017), five separate planning processes are presented: planning the supply chain, planning sourcing, planning manufacturing, planning delivery and planning returns. Each of these processes can, in turn, be broken down into similar sets of sub-processes. The main steps of the processes are to identify and aggregate the specific requirements, identify and aggregate the resources available and to balance resources with requirements. From this, a plan is devised and communicated. When broken down further, specific activities associated with each planning process are required. The planning process also requires input from the processes to be planned, creating a closed loop feedback system.

Enable

The enabling process was upgraded to a level one process with the release of SCOR 11.0 in 2012 (APICS, 2017). This process acts as a supporting process for the other five level one processes. On level two, a wide number of enabling processes exists: managing business rules, managing performance, managing human resources, managing assets, managing contracts, managing the supply chain network, managing compliance, managing risk, managing procurement and managing technology (APICS, 2017). Each of these processes has sub-processes that are specific to their field and purpose.

Source

The source process procures and sources goods and services necessary to meet planned demand (Rosenbaum and Bolstorff, 2003, p. 7). More specifically, according to APICS (2017), the processes are associated with ordering, delivery, receipt and transfer of goods and services. The SCOR 12.0 model makes a difference between the processes associated with three different types of products: stocked products, make-to-order products and engineer-to-order products. Stocked products are products for which a pre-determined inventory level exists. They are not linked to a specific customer order. Make-to-order products are instead sourced for a specific customer order, while engineer-to-order products are designed to specific specifications in the customer order. For stocked and make-to-order products, the SCOR model does not include identifying supply, sending out requests for proposals or quotations and negotiating the final deal. Instead, these activities are carried out in one of the enabling processes. For engineer-to-order products identification of supply, selection of suppliers and negotiation are included as sub-processes as they are connected to a specific customer order. Apart from this, the sub-processes for each type of product are similar on level three. They include scheduling product deliveries, receiving product, verifying product, transferring product to appropriate location and authorizing payment to the supplier.

Make

The make process includes all things related to the actual manufacturing and production such as scheduling production activities, producing, testing, packaging and finally releasing the product for delivery (Rosenbaum and Bolstorff, 2003, p. 7). In APICS (2017) the meaning of the make process on the first level is to add value to a deliverable through manufacturing or creation. In the SCOR 12.0 model there are three different kinds of products: Make-to-stock, Make-to-order and Engineer-to-order. This is in line with how the different products were categorized in the sourcing activity. For make-to-order products the sub-processes are scheduling of production activities, issue material, produce and test, package, stage product, release product to deliver and finally waste disposal. Make-to-order sub-activities are similar but not exactly the same, the main point of the differences being that the product is not meant to be put in stock but is manufactured for a specific customer order. Engineer-to-order products are perhaps the kind of products that stand out the most. Here the product is not fully defined from the start but its definition is part of the manufacturing process that hence also becomes a creation process. The steps in this process are similar to the two other make processes with the exception of an additional first step, which is to finalize production engineering.

Deliver

APICS (2017) defines the deliver process as comprising all processes associated with order management in relation to customers and order fulfilment activities. Just as in previous steps SCOR 12.0 differentiates between stocked products, make-to-order products and engineer-to-order products, but adds the additional sub-activity deliver retail product. The set of activities given for stocked products only apply for non-configurable, i.e. standard, products. Make-to-order products are already when kept in stock associated with a customer order. The same goes for engineer-to-order products with the additional fact that the engineering process will not start until a firm order has been received. All three prior set of sub-activities are relatively similar in that they have tasks related to receiving customer orders, picking, packing and shipping and invoicing. Deliver retail products on the other hand can be explained as the situation in a typical retail store. The tasks involved are generate a stocking schedule, receive product at store, pick product from backroom, stock shelf, fill shopping cart, checkout and deliver and/or install.

Return

The return process is concerned with all tasks needed in the return flow of products upstream in the supply chain (Rosenbaum and Bolstorff, 2003, p. 7). According to APICS (2017), this process can be used to deal with defects in ordering, manufacturing or in the product itself as well as to perform upkeep activities. The process deals with both product returns from deliveries made as well as returns in sourcing. The process for returns varies slightly depending on the type of the return and the source of the return. This is because in different cases different entities have to take action and certain parties have to make decisions. For both returns from deliveries and to source there are three different types of returns: Return defective product, return MRO product and return excessive product.

Appendix B. Review protocol

Table B1: Review protocol for literature review.

Review Protocol	
Review Question	Which activities in the supply chain of an organization could BCT have an impact on?
Criteria for inclusion (White Literature)	*Reasoning*
Paper published in a scientific journal	Allows for a clear distinction between white and grey literature
Paper written in English	English is understood by both researchers and for transparency; English sources are easier to review for readers.
Paper written between 2008 and present time	The Bitcoin whitepaper (2008) marks the first application of BCT
Paper treats interaction between BCT and supply chain	Papers should treat the subject of this study.
Criteria for inclusion (Grey Literature)	*Reasoning*
Written in English	English is understood by both researchers and for transparency; English sources are easier to review for readers.
Paper written between 2008 and present time	The Bitcoin whitepaper (2008) marks the first application of BCT
Whitepaper describing a blockchain application	The whitepaper should propose to solve the identified problem using BCT
The application uses a public and/or permission-less blockchain	This study focuses on Pub-PL blockchains
Connection to supply chain	The application should have a clear connection to an activity carried out in the supply chain of an organization

Application not ONLY related to an ICO	The application should not simply use cryptocurrency or tokens as means of raising funds for projects not related to BCT
Data search	
White literature is searched for according to a hierarchy of databases; first Web of Science Core Collection is searched, then Business Source Complete (EBSCOhost), followed by Elsevier, Emerald and finally Google Scholar	
A scoping study is conducted using the briefsearch strategy. If central papers are discovered the strategy is switched to citation pearl growing. If no central papers exist, the search continues using the building blocks strategy.	
Grey literature is searched for using the Google search engine. Results on the first 2 or 5 pages (20 or 50 top results) are considered for inclusion.	
Total articles	385
After removing duplicates	195
After screening based on inclusion/exclusion criteria	50

Appendix C. Data extraction forms

Table C1: Data extraction form for white literature.

1. Bibliographic information
Title
Year
Publication
Link
Keywords
Relevant references

2. Researcher details
Authors and affiliations
Academic discipline of authors

3. Aims and methods
Study aims
Research Questions
Method used
Definition of BCT
Distinction between public and private blockchains?
Definition of supply chain

4. Findings
Themes
Presented initiatives (companies/organizations/consortia)
Applications of BCT, from secondary sources
Applications of BCT, from primary sources
Connections between SCM and BCT
Connected SCOR processes
Identified barriers for adoption
Suggested future research

5. Quality
Has the research design been adapted to the real-life settings encountered?
Is the sample adequate for producing knowledge?
Is the description detailed enough to allow the reader to make own interpretations of context, methods and meaning?
Are different sources compared and contrasted?
Does the research move from data to analysis and interpretation in a transparent and coherent manner?
Are claims for generalizability supported by valid argumentation?
Citations per year
Journal Impact Factor

Table C2: Data extraction form for grey literature.

1. Bibliographic information
Title
Year
Publisher
Publishing date
Link
2. Author details
Authors and affiliations
Industry of authors
3. Purpose
Identified Problem
Definition of BCT
Definition of supply chain
Connected SCOR processes
Connected SCOR practices
Connections between SCM and BCT/ Why a blockchain?
Identified barriers for adoption
Suggested future improvements
In what phase is the project?
Solution for minimizing data on chain
Blockchain used
4. Quality
Level of description

Appendix D. Panel results from Delphi round 1

Total

Table D1: Total responses for issues in Delphi round 1.

Issue	*Yes*	*Don't know*	*No*
Paperwork	83.3 %	6.7 %	10 %
Lack of trust	80 %	0 %	20 %
Lack of transparency for customers	73.3 %	6.7 %	20 %
Lack of downstream traceability	73.3 %	3.3 %	23.3 %
Lack of upstream visibility	70 %	10 %	20 %
Lack of upstream traceability	70 %	20 %	10 %
Lack of downstream visibility	63.3 %	10 %	26.7 %
High supply chain complexity	53.3 %	16.7 %	30 %
Lack of transparency for regulators	50 %	26.7 %	23.3 %
Lack of flexibility	46.7 %	23.3 %	30 %
Lack of security for IoT-devices	50 %	30 %	20 %
Counterfeited products	46.7 %	20 %	33.3 %
Lack of transparency for financial institutions	36.7 %	30 %	33.3 %

Table D2: Total responses for applications in Delphi round 1.

Application	*Yes*	*Don't know*	*No*
Automate payments and transactions	90 %	3.3 %	6.7 %
Reduce paperwork	83.3 %	3.3 %	13.3 %
Improve information sharing	73.3 %	20 %	6.7 %
Improve product traceability	76.7 %	3.3 %	20 %
Monitor transport conditions	76.7 %	3.4 %	20.7 %
Prove provenance	73.3 %	10 %	16.7 %
Verify supply chain activities	66.7 %	16.7 %	16.7 %
Provide infrastructure for M2M-interaction	66.7 %	6.7 %	26.7 %
Create trusted marketplaces without intermediaries	66.7 %	16.7 %	16.7 %
Anti-counterfeiting	66.7 %	13.3 %	20 %
Issue targeted recalls	63.3 %	13.3 %	23.3 %
Provide secure communication for IoT-devices	60 %	23.3 %	16.7 %
Increase Supply chain finance efficiency	60 %	23.3 %	16.7 %
Smart tender of transportation	53.3 %	23.3 %	23.3 %
Provide infrastructure for C2M- interaction	53.3 %	26.7 %	20 %

Supply Chain Experts

Table D3: Supply chain expert responses for issues in Delphi round 1.

Issue	*Yes*	*Don't know*	*No*
Paperwork	90 %	10 %	0 %
Lack of trust	90 %	0 %	10 %
Lack of downstream traceability	80 %	10 %	10 %
Lack of upstream traceability	80 %	0 %	20 %
Lack of upstream visibility	80%	0 %	20 %
Lack of downstream visibility	70 %	10 %	20 %
Lack of flexibility	70 %	10 %	20 %
Lack of transparency for customers	60 %	20 %	20 %
High supply chain complexity	60 %	0 %	40 %
Lack of security for IoT-devices	50 %	40 %	10 %
Lack of transparency for regulators	40 %	40 %	20 %
Lack of transparency for financial institutions	30 %	40 %	30 %
Counterfeited products	20 %	40 %	40 %

Table D4: Supply chain expert responses for applications in Delphi round 1.

Application	*Yes*	*Don't know*	*No*
Monitor transport conditions	100 %	0 %	0 %
Automate payments and transactions	90 %	10 %	0 %
Reduce paperwork	90 %	0 %	10 %
Improve product traceability	90 %	10 %	0 %
Verify supply chain activities	80 %	20 %	0 %
Provide secure communication for IoT-devices	80 %	20%	0 %
Improve information sharing	80 %	20 %	0 %
Provide infrastructure for M2M-interaction	80 %	0%	20 %
Prove provenance	70 %	20%	10 %
Increase Supply chain finance efficiency	60%	40 %	0 %
Smart tender of transportation	60%	40%	0 %
Issue targeted recalls	60 %	30%	10 %
Anti-counterfeiting	60 %	30 %	10 %
Provide infrastructure for C2M- interaction	50 %	40%	10 %
Create trusted marketplaces without intermediaries	50 %	30%	20 %

Academics

Table D5: Academic expert responses for issues in Delphi round 1.

Issue	*Yes*	*Don't know*	*No*
Lack of upstream visibility	90.9 %	0 %	9.1 %
Lack of transparency for customers	90.9 %	0 %	9.1 %
Lack of downstream visibility	81.8 %	9.1 %	9.1 %
Lack of upstream traceability	81.8 %	0 %	18.2 %
Paperwork	81.8 %	0 %	18.2 %
Lack of trust	81.8 %	0 %	18.2 %
Counterfeited products	72.7 %	9.1 %	18.2 %
Lack of downstream traceability	72.7 %	0 %	27.3 %
High supply chain complexity	54.5 %	18.2 %	27.3 %
Lack of transparency for regulators	54.5 %	18.2 %	27.3 %
Lack of security for IoT-devices	45.5 %	27.3 %	27.3 %
Lack of transparency for financial institutions	45.5 %	18.2 %	36.3 %
Lack of flexibility	36.4 %	27.2 %	36.4 %

Table D6: Academic expert responses for applications in Delphi round 1.

Application	*Yes*	*Don't know*	*No*
Automate payments and transactions	90.9 %	0 %	9.1 %
Improve product traceability	90.9 %	0 %	9.1 %
Prove provenance	90.9 %	0%	9.1 %
Anti-counterfeiting	90.9 %	0 %	9.1 %
Improve information sharing	81.8 %	9.1 %	9.1 %
Reduce paperwork	81.8 %	0 %	18.2 %
Issue targeted recalls	81.8 %	0 %	18.2 %
Increase Supply chain finance efficiency	72.7 %	18.2 %	9.1 %
Verify supply chain activities	72.7 %	9.1 %	18.2 %
Monitor transport conditions	72.7 %	0 %	27.3 %
Smart tender of transportation	63.6 %	18.2%	18.2 %
Provide secure communication for IoT-devices	63.6 %	18.2 %	18.2 %
Create trusted marketplaces without intermediaries	63.6 %	9.1 %	27.3 %
Provide infrastructure for C2M- interaction	54.5 %	27.3 %	18.2 %
Provide infrastructure for M2M-interaction	54.5 %	9.1 %	36.4 %

Blockchain experts

Table D7: Blockchain expert responses for issues in Delphi round 1.

Issue	*Yes*	*Don't know*	*No*
Paperwork	77.8 %	11.1 %	11.1 %
Lack of trust	66.7 %	0 %	33.3 %
Lack of transparency for customers	66.7 %	0 %	33.3 %
Lack of downstream traceability	66.7 %	0 %	33.3 %
Lack of transparency for regulators	55.6 %	22.2 %	22.2 %
Lack of security for IoT-devices	55.6 %	22.2 %	22.2 %
Lack of upstream visibility	44.4 %	33.3 %	22.2 %
Lack of upstream traceability	44.4 %	33.3 %	22.2 %
High supply chain complexity	44.4 %	33.3 %	22.2 %
Counterfeited products	44.4 %	11.1 %	44.4 %
Lack of flexibility	33.3 %	33.3 %	33.3 %
Lack of transparency for financial institutions	33.3 %	22.2 %	44.4 %
Lack of downstream visibility	33.3 %	11.1 %	55.6 %

Table D8: Blockchain expert responses for applications in Delphi round 1.

Application	*Yes*	*Don't know*	*No*
Create trusted marketplaces without intermediaries	88.9 %	11.1%	0 %
Automate payments and transactions	88.9 %	0 %	11.1 %
Reduce paperwork	77.8 %	11.1 %	11.1 %
Provide infrastructure for M2M-interaction	66.7 %	11.1 %	22.2 %
Improve information sharing	55.6 %	33.3 %	11.1 %
Monitor transport conditions	55.6 %	11.1 %	33.3 %
Prove provenance	55.6 %	11.1 %	33.3 %
Provide infrastructure for C2M- interaction	55.6 %	11.1 %	33.3 %
Verify supply chain activities	44.4 %	22.2 %	33.3 %
Anti-counterfeiting	44.4 %	11.1 %	44.4 %
Issue targeted recalls	44.4 %	11.1 %	44.4 %
Increase Supply chain finance efficiency	44.4 %	11.1 %	44.4 %
Improve product traceability	44.4 %	0 %	55.6 %
Provide secure communication for IoT-devices	33.3 %	33.3 %	33.3 %
Smart tender of transportation	33.3 %	11.1 %	55.6 %