Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments

Completed Research Paper

Kristoffer Nærland
brainbot technologies
Mainz, Germany
kristoffer@brainbot.com

Christoph Müller-Bloch
IT University of Copenhagen
Copenhagen, Denmark
chmy@itu.dk

Roman Beck
IT University of Copenhagen
Copenhagen, Denmark
beck@itu.dk

Søren Palmund
IT University of Copenhagen
Copenhagen, Denmark
spal@itu.dk

Abstract

Many decentralized, inter-organizational environments such as supply chains are characterized by high transactional uncertainty and risk. At the same time, blockchain technology promises to mitigate these issues by introducing certainty into economic transactions. This paper discusses the findings of a Design Science Research project involving the construction and evaluation of an information technology artifact in collaboration with Maersk, a leading international shipping company, where central documents in shipping, such as the Bill of Lading, are turned into a smart contract on blockchain. Based on our insights from the project, we provide first evidence for preliminary design principles for applications that aim to mitigate the transactional risk and uncertainty in decentralized environments using blockchain. Both the artifact and the first evidence for emerging design principles are novel, contributing to the discourse on the implications that the advent of blockchain technology poses for governing economic activity.

Keywords: Blockchain, Bill of Lading, international trade, decentralized environments

Introduction

The management of key documents in international trade is a vulnerable process that is error-prone and threatened by fraud (Jensen et al., 2014). A central document in international trade is the Bill of Lading, a physical document that does not only serve as a contract of carriage and as a receipt that the goods have been loaded, but also as a title to the cargo. Hence, possession of the Bill of Lading is equivalent to the ownership of the cargo it represents (Schmitz, 2011). The Bill of Lading and several other documents need to be physically presented to authorities on request. Given that many dozen actors (i.e., authorities, service providers, etc.) can be involved in a single trade (Jensen et al., 2014) and several of these actors may possess the Bill of Lading at some point, the process is failure-prone and risk-laden: the document might get lost, destroyed, stolen, or a fraudulent Bill of Lading might be forged (Bassindale, 1996; Jensen et al., 2014). Given the vulnerability of the process, cooperative behavior of all actors involved is indispensable. According to Maersk, the largest container shipping company in the world, managing the

trade documentation can be more costly than the actual transport of the container (World Economic Forum, 2017). Thus, the centrality of the Bill of Lading in international trade and the challenges of managing the physical document across the different stakeholders in the supply chain urges the logistics industry to look for more secure, more efficient, and more trustworthy ways of information management in international trade. The example of international trade is just one of many cases of decentralized, inter-organizational environments, which are characterized by high transactional risk and uncertainty, governed by bilateral agreements, and lack central authorities.

A potential solution to mitigate the transactional risk and uncertainty in such decentralized environments is offered by blockchain. Blockchain technology has garnered a lot of attention in both mainstream media and business (Avital et al., 2016), in particular in the financial services industry (Walsh et al., 2016). The technology is perceived as groundbreaking (e.g., Niederman et al., 2017), and several companies and organizations are already working on implementing blockchain-based solutions (e.g., Beck & Müller-Bloch, 2017; Hyvärinen et al., forthcoming). Blockchain can be described as a distributed, transactional database technology that provides validated, immutable transactions that are consistent between a large number of network participants (Glaser, 2017). One of the most salient features of blockchain technology are smart contracts: software code that runs exactly as programmed without any risk of downtime, censorship, or fraud (Buterin, 2014). Smart contracts encode the rules of contracts in software code (Szabo, 1997) and enforce these contracts by making contract breaches prohibitively expensive. They give rise to a new kind of economic systems, which organize "transactions completely reliable, without any human interaction, following intractable rules set in the computer protocol" (Beck et al., 2016, p. 2). So far, most research on blockchain has focused on technological issues (e.g., Tschorsch & Scheuermann, 2016) as well as Bitcoin (e.g., Böhme, 2016; Böhme et al., 2015; Li & Wang, 2016). However, blockchain research is still in its infancy when it comes to applications beyond Bitcoin as well as more theory-driven considerations (Lindman et al., 2017; Yli-Huumo et al., 2016). This paper addresses these two shortcomings in the literature by building an IT artifact that is based on a blockchain application and by presenting first evidence for emerging design principles (Gregor & Hevner, 2013) for applications that aim to mitigate the transactional risk and uncertainty in decentralized environments using blockchain.

Following a Design Science Research (DSR) approach (Beck et al., 2013; Iivari, 2015), we (1) present a prototype that was constructed and evaluated in cooperation with Maersk, one of the leading container shipping companies in the world. The prototype illustrates how blockchain can help to address the deficits in international trade, thereby illustrating what has been proposed in the literature (Korpela et al., 2017). Abstracting from our insights gained during problem-solving to the level of design knowledge (Gregor & Hevner, 2013), we (2) provide first evidence for nascent design principles that could potentially serve to design applications that aim to mitigate the transactional risk and uncertainty in decentralized environments using blockchain.

The remainder of this paper is structured as follows. Section 2 explores the foundational literature on both blockchain and informational flows in international trade. Section 3 describes our research process and methodology. Section 4 contains the development, description, and evaluation of the prototype. Section 5 discusses the emerging design principles. Section 6 presents implications, limitations, and concludes.

Literature Background

Blockchain

Blockchain has been referred to as a groundbreaking technology, potentially having a comprehensive impact on business and society (e.g., Niederman et al., 2017). The advent of blockchain has the capacity to revolutionize established economic systems by increasing the transparency and security of transaction-based processes (Beck et al., 2016). Blockchain has come a long way since the invention of Bitcoin, a decentralized virtual currency constituting the first application of blockchain technology in 2009

(Nakamoto, 2008). Leading technology firms such as IBM and Microsoft currently have their own blockchain projects underway[1], and the amount of research on the topic is picking up swiftly.

While there are different incarnations of blockchains (also referred to as distributed ledger technology), in this paper we focus on public permissionless blockchains. In essence, a public permissionless blockchain is a database that is characterized by being open source, decentralization, consensus, tamper-proofness, and validity (see Table 1). Blockchain refers to a chain of blocks, each containing a number of transactions. The transaction data is secured by cryptographic hash functions. Each block is linked to the previous block in that it contains the hash of the previous block in addition to the actual hashed transaction data. The blockchain protocols are *open source*, meaning anyone can use the entire history of the blockchain and set up an identical or slightly modified version, legally and free of charge (this is called forking). The blockchain is shared in a *decentralized* fashion among a network of computers—so-called nodes. Every node has a copy of the blockchain. The nodes are incentivized to reach *consensus* on the state of the blockchain. Hence, all nodes share identical versions of the blockchain. If one node fraudulently alters its version of the blockchain, that version of the blockchain would be rejected by the other nodes, making the blockchain *tamper-proof*. New entries can only be accepted if they are *valid*, meaning that they need to adhere to a predefined protocol.

Table 1. Characteristics of Public Permissionless Blockchains

Characteristic	**Meaning**
Open source	Anyone can set up an identical or slightly modified version of the blockchain.
Decentralization	It operates without a central decision maker or hierarchy.
Consensus	All transactions in a blockchain are agreed upon through consensus. There is only one version of the truth in a blockchain.
Tamper-proofness	It accepts new entries only if they build on unmodified previous entries.
Validity	It accepts new entries only if they adhere to a predefined protocol.

Table 1. Characteristics of Public Permissionless Blockchains

In the case of the Bitcoin blockchain, nodes validate blocks by running an algorithm called proof-of-work. Transactions are bundled into blocks and must be validated to be added to the blockchain. To validate a block, nodes compete to discover the nonce of a new block, which remains unknown until a node has mined the block. A nonce is a unique identifier assigned to blocks. By combining the nonce of the previous block and an unknown nonce, a complex mathematical puzzle is presented. The challenge nodes have is to discover the unknown nonce while proving they also found the known previous nonce. This puzzle serves two purposes. First, it makes validating a block a computationally expensive task. Second, it makes proving that the nonce was found according to the protocol easy to verify for all other nodes in the network. Since all nodes know the hash, they only need to use a hash function of the new nonce and the nonce of the previous block. If the new nonce is correct, it will always produce an identical hash. When a node has successfully discovered the hash of a new block, it creates and adds the block and therefore also the bundled transactions to the existing blockchain. The Bitcoin protocol awards this node with Bitcoins for its work, whereas all other nodes that competed do not receive remuneration. Nodes that wish to mine Bitcoins can spend more energy and increase their computation power. The waste and expense of this energy also makes Bitcoin very secure. An attacker who wishes to subvert the network must be able to spend more than 51% of the network's combined energy to do so, which has not been possible so far.

Using Bitcoin transactions for other applications apart from payments is possible, but difficult. One of the reasons why it is difficult to write applications on top of Bitcoin is that Bitcoin does not come with a

[1] http://www.computerworld.com/article/3088705/cloud-computing/microsoft-and-ibm-want-to-own-your-blockchain.html

Turing-complete programming language. Turing completeness expanded the functionality of blockchain from a protocol to enable cryptocurrencies such as Bitcoin into a distributed computer that can run programs through a decentralized network. In other words, Turing-complete blockchains such as Ethereum enable a wider range of applications to be built while inheriting the properties listed in Table 1. Turing-complete blockchains might enable many kinds of innovations, such as applications for the Internet-of-Things (Christidis & Devetsikiotis, 2016) or decentralized marketplaces (Wörner et al., 2016).

The primary component introduced to handle Turing-complete language in blockchains is called smart contracts (Szabo 1997). In Ethereum, smart contracts are programs that can run in a decentralized environment. This means that it is possible to read and verify the code written in the program and to know that it will execute exactly as stated in the program. Based on smart contracts that are stored on a blockchain, decentralized autonomous organizations (DAOs), which solely exist on the blockchain, can be established. Within those organizations, governance rules are formalized, automated, and enforced according to the business logic encoded in the software. DAOs are written with the same code as smart contracts and therefore include built-in voting methods for participants. Hence, participants can exercise direct real-time control over management decisions. This represents a paradigmatic shift from traditional organizations, which are governed by a combination of private contracts between owners, legal prescriptions, and rules that are not explicitly specified (Jentzsch, n.d.).

Other transaction validation algorithms beyond proof-of-work also exist. In particular, proof-of-stake has gained a lot of attention recently. The underlying idea is to disincentive malicious actions. Network participants provide a stake of their cryptocurrency as collateral. The collateral is burned if the network participant acts maliciously. The algorithm does not require vast amounts of energy as in the proof-of-work, thereby addressing concerns about the ecological and economical sustainability of proof-of-work algorithms (see also Spasovski & Eklund, 2017; Tschorsch & Scheuermann, 2016).

Besides public permissionless blockchains, other types of blockchains also exist. In essence, blockchains can be classified along two dimensions (see Table 2): (1) access to transactions—that is, the ability to read and to submit transactions. In public blockchains, all nodes can read and submit transactions. In private blockchains, only nodes that have been predefined by a central authority can read and submit transactions. The other dimension is (2) access to transaction validation—that is, the ability to participate in the creation of new blocks, for instance through proof-of-work or proof-of-stake algorithms. In permissionless blockchains, all nodes can validate transactions. In permissioned blockchains, only nodes that have been predefined by a central authority can validate transactions. A permissioned blockchain can be public and private (Peters & Panayi, 2016).

Table 2. Different Types of Blockchains (based on Peters & Panayi, 2016)

By access to transactions	**By access to transaction validation**	
	Permissioned	Permissionless
Public	All nodes can read blockchain data and submit transactions. Only predefined nodes can validate transactions.	All nodes can read blockchain data and submit transactions. All nodes can validate transactions.
Private	Only predefined nodes can read blockchain data and submit transactions. Only predefined nodes can validate transactions.	Not applicable

Table 2. Different Types of Blockchains

Informational Flows in International Trade

Informational flows in international trade are characterized by fragmented systems that are used to serve the needs of each of the many actors that are part of the supply chains. Even though inter-organizational systems exist, they are often only used for exchanging information bilaterally (Jensen et al., 2014). Güven-Koçak (2015, p. 9) points out the ineffectiveness of these local solutions, given that "all stakeholders are

inter-related in such a complex ecosystem and interact with each other on a day-to-day basis". Unsurprisingly, poor data quality is a common problem in international trade (Jensen & Vatrapu, 2015). Large efficiency gains seem possible if a global information infrastructure would be adopted, thereby facilitating more effective information exchange (Jensen et al., 2014). Betz and Henningsson (2016) argue that network effects (i.e., increasing economies of return), which characterize many innovative technologies (Katz & Shapiro, 1994), could potentially create a lot of value if such a global information infrastructure for international trade would be introduced.

The actors in international trade act out of self-interest, pursuing their own agenda (Güven-Koçak, 2015), and even fraud is not uncommon (Jensen et al., 2014). Due to its function as a title to the cargo (Schmitz, 2011), the Bill of Lading may be the most salient target of misconduct. In the case of the Bill of Lading, different types of fraud can be distinguished (Bassindale, 1996). For instance, some information on a genuine Bill of Lading may be fabricated. In this case, a seller might try to produce a Bill of Lading that suggests he or she complied with the contractual obligations. The incentive to create such a Bill of Lading is considerable, as the buyer may reject the goods if the seller fails to comply with the contract. In another example, a wholly false Bill of Lading may be forged. In this case, the fraudsters identify genuine cargo, which is loaded on board a genuine vessel. Then they pretend to sell the cargo and cheat on the buyer.

The potential of information technology to improve operational processes in supply chains has been widely recognized (Gunasekaran & Ngai, 2004). The World Economic Forum (2013) estimates that the introduction of modern information technologies in conjunction with reengineered information management processes could reduce the cost of international trade by 15 percent, thereby boosting the global gross domestic product by five percent. However, the adoption of state-of-the-art information technologies in international trade remains slow due to manifold issues (Betz & Henningsson, 2016; Jensen & Tan, 2015). A reluctance in the shipping industry to embrace more radical innovations has been diagnosed (Jensen et al., 2014). Moreover, it has been noted that those who would reap the most benefits from innovations may not necessarily be the ones who would invest, which might further deter investment (Hedman & Henningsson, 2012).

To counter the inefficiency of informational flows in international trade, a shared information infrastructure has been proposed (Jensen & Vatrapu, 2015b). The proposed system is meant to facilitate information exchange among an indefinite number of supply chain participants (Jensen & Tan, 2015; Jensen & Vatrapu, 2015a). Jensen and Tan (2015, p. 499) argue that it "will provide higher quality and up to date information compared to today where information often is missing, out of date and of poor quality". However, some of the transactional risk that manifests itself in the informational flows in international trade would remain even after the introduction of the proposed solution. Cooperative behavior of the involved stakeholders would still be necessary to facilitate frictionless transactions, given that it would still be possible to forge key documents such as the Bill of Lading.

Methodology

In this paper, we follow a DSR approach, which originates from areas such as engineering and computer science, which essentially focus on problem-solving (Simon, 1996). Informed by a problem with practical relevance (Hevner et al., 2004), we design a new and innovative IT artifact (March & Smith, 1995; Orlikowski & Iacono, 2001) while simultaneously abstracting design knowledge to guide future artifact design in problem areas that are similar to the one at hand (Gregor & Hevner, 2013; Gregor & Jones, 2007). Our rationale for choosing a DSR approach was twofold. First, our research project aimed for building and evaluating an IT artifact. Second, our literature review indicated a lack of design knowledge in the area of blockchain, which we address by presenting first evidence for emerging design principles (Gregor & Hevner, 2013) for applications that aim to mitigate the transactional risk and uncertainty in decentralized environments using blockchain. We followed the guidelines for theory-generating design science research by Beck et al. (2013). The remainder of this chapter describes the key steps of our research project. The steps are (1) creating awareness of the problem and suggesting an approach to solve it, (2) developing the artifact, (3) evaluating the artifact, and (4) abstracting design knowledge. However, these steps are not as linear as implied, the process can be highly iterative (Beck et al., 2013).

In the first step, we became aware of the problem and devised an approach to solve it. The research project was initiated in an informative meeting of two of the authors and a C-level manager at Maersk. The initial hunch was that blockchain technology might have the potential to mitigate some of the uncertainty and risk that is inherent to supply chains in international trade. Between April and August 2016, several workshops attended by both executive management and subject matter experts were held to create an understanding of the problem domain. Together with the subject matter experts at Maersk, a use case was designed to use blockchain to improve the informational flows and to reduce the inherent uncertainty and risk in international trade. Based on the use case, tentative design requirements were derived, which were refined over time. The subject matter experts were also available once the research process entered its next stages (development, evaluation, theory-generation), to clarify open questions regarding the use case and design requirements, and to provide their feedback and insights.

Next, we started to develop the prototype. Most of the development took place in August 2016 in a workshop held at a university. The session spanned several days, in which both developers and industry experts were present. The development and evaluation of the artifact proceeded concurrently. Maersk's subject matter experts were available during the development session to provide guidance and feedback. After the workshop, some additional development took place to refine the solution. The development ended once the feedback provided by the subject matter experts indicated a satisfactory problem solution.

The primary goal of the evaluation was to analyze whether the prototype represents a feasible alternative to the current information management processes in international trade. The evaluation therefore focuses on how the application reduces transactional risk and uncertainty (Sein et al., 2011). Naturalistic evaluation with real users in a real world environment would not have been possible, since the artifact only represents a first step towards understanding how blockchain can improve current processes in international trade. Therefore, we chose an evaluation approach with a focus on formative and artificial evaluation methods (Venable et al., 2016). The criteria our evaluation focuses on are actual effectiveness, actual efficiency, perceived usefulness, and perceived ease of use (Moody, 2003). The evaluation process spanned three episodes (see Table 3), each of which concentrated on two criteria. These were evaluated using the most appropriate methods available, informed by method types proposed in the literature (Peffers et al., 2012). The three episodes were linked to evaluating the suggested approach to (1) solving the problem, (2) evaluating the prototype under development, and (3) evaluating the final artifact.

Table 3. Evaluation Episodes

Episode	Evaluation method	Evaluation criteria
Episode 1	Logical argument Expert evaluation	Actual Effectiveness Perceived Usefulness
Episode 2	Prototype Illustrative scenario	Actual Efficiency Actual Effectiveness
Episode 3	Expert evaluation	Perceived Usefulness Perceived Easy of Use

Table 3. Evaluation Episodes

The first episode started with getting familiar with the problem and the solution requirements. The main issue we identified was the transactional risk and uncertainty of information management processes in international trade. Thus, our aim became to build an artifact that mitigated these issues. We proposed to design a prototype based on blockchain technology, since the technology's inherent characteristics address the problems explicated above at least to some extent. The industry experts also perceived the proposed solution as useful.

During the second episode, we built a prototype and devised an illustrative scenario to demonstrate how documents such as the Bill of Lading could be put onto a blockchain and to assess the technical feasibility. The results of the second evaluation episode are reported in the *demonstration* section of the next chapter.

During the third and final evaluation episode, we held two focus group sessions with three experienced industry experts, who were also familiar with the technology. Hence, they were qualified to assess how well the artifact addressed the problem. Two of the experts were senior IT executives at Maersk and one of them was a former IT executive at the same company. In the sessions, the experts were shown a test run of the prototype and given a presentation on the issues it tried to address. Subsequently, all experts were asked for their opinions on the final prototype, with respect to how they perceived usefulness and ease of use. The results of the third and final evaluation episode are reported in the *final evaluation* section of the next chapter.

Our final step comprised theory-generation. For the empirical grounding of our nascent design principles, we relied on several sources. In addition to the findings from the evaluation of the IT artifact, the design principles were also informed by applicable knowledge, that is, data from the existing knowledge base. Moreover, we triangulated our findings with insights we gained from participating in several dozen blockchain workshops, panels, and events.

Blockchain Prototype

Development

The prototype was implemented by writing a smart contract, which was deployed in the Ethereum blockchain with a static HTML page serving as the user interface and IPFS, a distributed system for storing files[2], serving as the data layer. The smart contract itself, written in Solidity[3], embodies the concept of a shipment. A shipment has an owner (referred to as shipment owner) and contains a list of stakeholders as well as attached documents. The shipment owner is always the entity that created the shipment in the blockchain. Each stakeholder is identified by their address on the network. The shipment owner holds the sole authority to whitelist stakeholders. That is, an address can only become a stakeholder if the shipment owner whitelists it.

The documents attached to a shipment represent the legal paperwork, which normally follows a shipment in physical form, and they may take many forms, for instance, the Bill of Lading or the form of import or export declaration from a specific port. While the documents for this use case are shipping documents, in reality the documents could be anything—even photos or audio files.

In the prototype, the concept of a document is represented by just two fields: Author and fingerprint. The author holds the address of the last stakeholder to upload/amend the document and the fingerprint is the ID, uniquely identifying the document in the data layer. Logically, initially the author of any document is the shipment owner. As the shipment progresses through the system, authorities at the receiving ports sign the documents, thus allowing the shipment to continue its journey to its destination. When a document is signed, its new state is written to the blockchain, with the signee taking over as the author of the document. This is done to allow for an easy way to track who last modified a document.

While the signing of a document is stored on the Ethereum Blockchain, the document itself is not. Since a document might be arbitrarily large, and the Ethereum Blockchain is not well-suited for storing arbitrarily large binary files, the choice was made to store the documents on IPFS instead. Upon storing a document, IPFS returns a unique fingerprint, which uniquely identifies the uploaded document on the IPFS network. This fingerprint can be used to retrieve the document in the future. Furthermore, if a completely identical file is later uploaded to the network, the very same unique fingerprint is returned—as the files are identical. This can be seen in Figure 1, in which a stakeholder has uploaded a document, which had already been uploaded to the IPFS network.

[2] https://ipfs.io

[3] http://solidity.readthedocs.io/en/develop

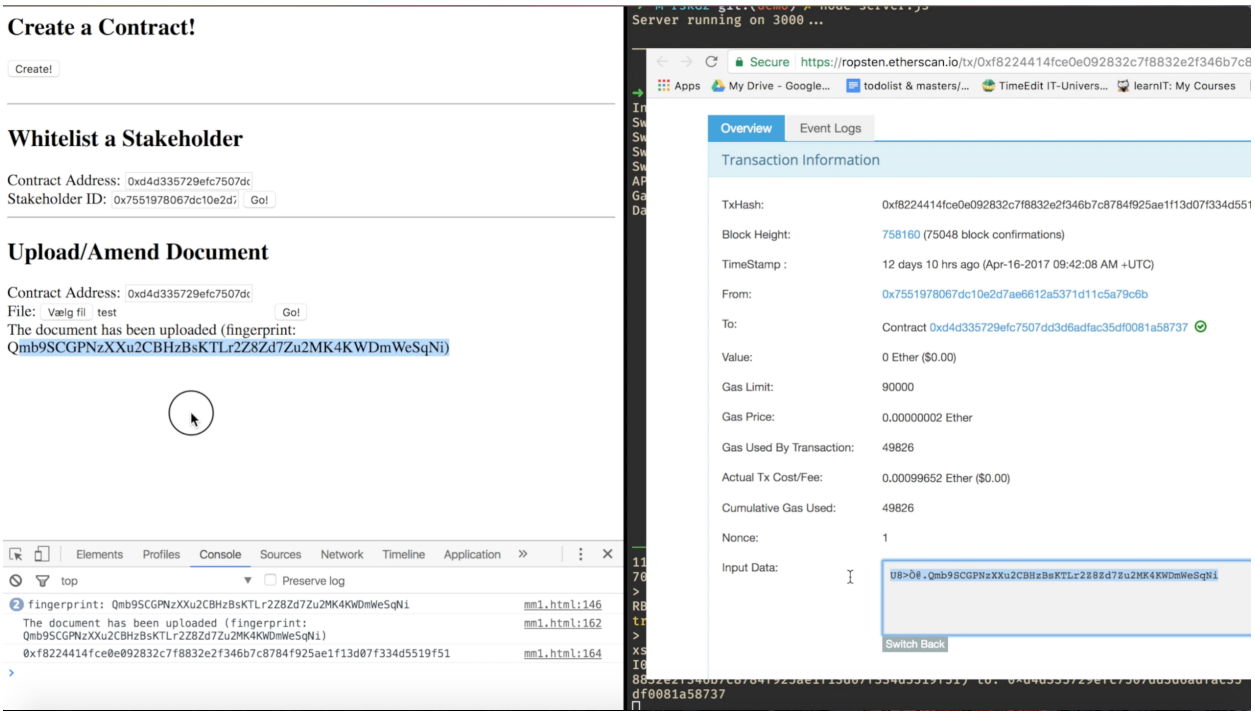


Figure 1. Document Upload

The user interface for the prototype was built using HTML and JavaScript, using Web3JS[4] connecting to a local geth[5] client.

Demonstration

In addition to the description in this paper, we also provide a video demonstration online[6] as well as process flow diagram in Appendix A.

Shipment Owner Perspective

In its current design, the shipment owner has the ability to create a shipment, whitelist stakeholders (e.g. authorities, shipping agents, etc.), and to upload/amend a document. The shipment needs to be created first so that stakeholder and document can be associated with it. Apart from that, the order of events as described here is arbitrary. One need not whitelist stakeholders first and upload documents second. It can be done in reverse order.

The creation of a shipment is handled by creating a new instance of the shipment smart contract. This instance is then written to the blockchain with the current user as the shipment owner. Figure 2 shows the contract being written from the point of view of the prototype and Figure 3 from the point of view of Etherscan. Once a shipment has been created and successfully mined, the shipment owner begins the process of uploading documents and whitelisting stakeholders.

---

[4] https://github.com/ethereum/web3.js

[5] https://github.com/ethereum/go-ethereum

[6] http://bit.ly/2p1N1zh

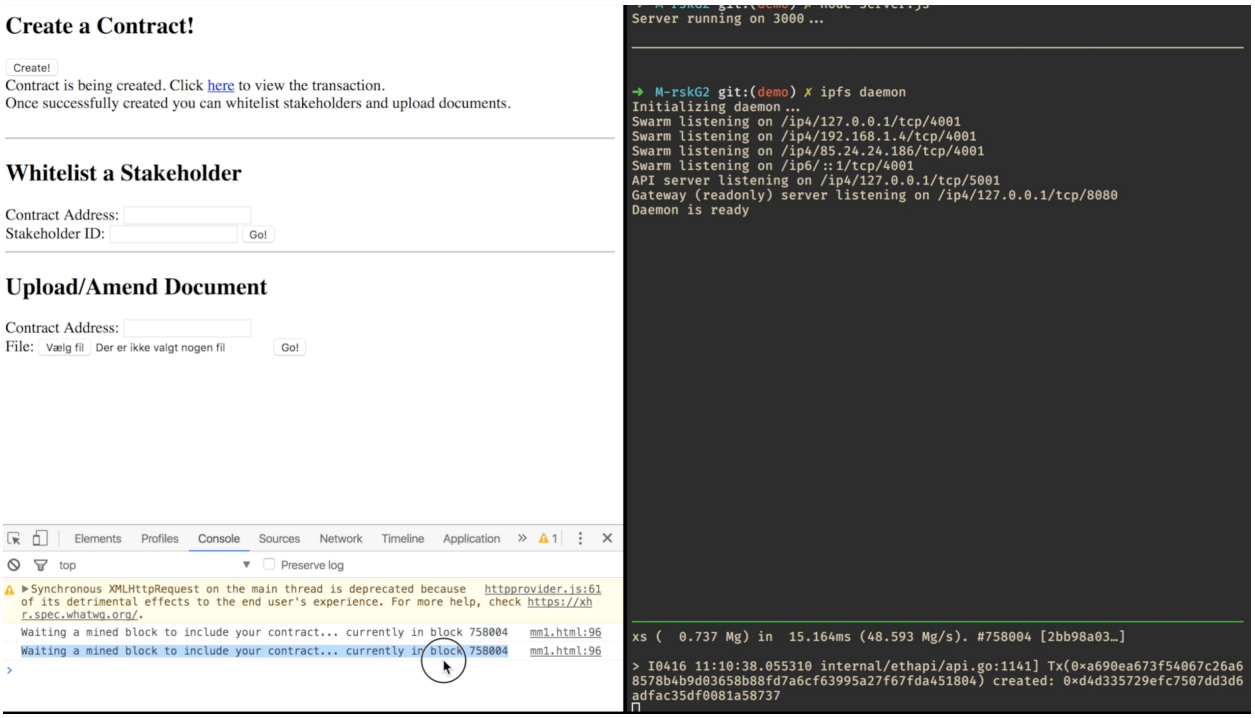


Figure 2. Prototype View of Contract Written to Blockchain

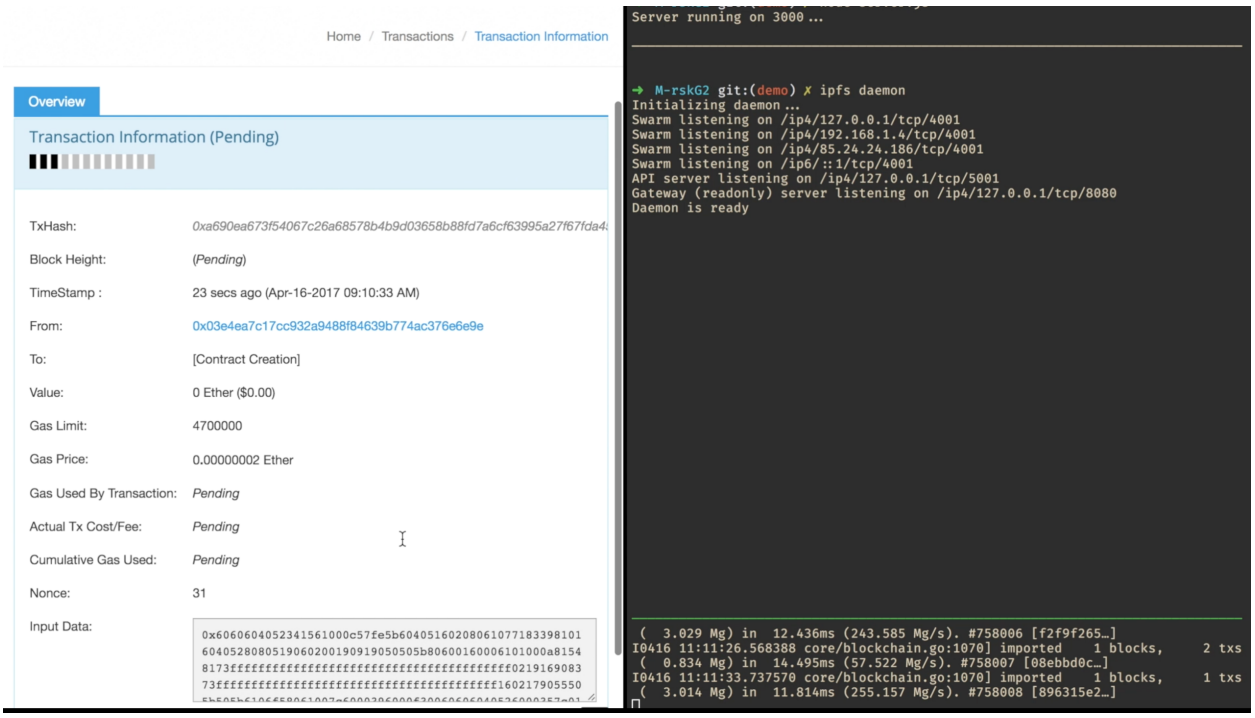


Figure 3. Etherscan View of Contract Written to Blockchain

Whitelisting a stakeholder requires knowing the address of the stakeholder and the address of the contract (see Figure 4 where contract address and stakeholder ID have already been filled out). Having just created a contract, its address is already on hand. We assume that the address of the stakeholder has been exchanged beforehand. When the shipment owner whitelists a stakeholder, the address is permanently added to the shipment, allowing the stakeholder to amend existing documents and upload new documents - should the need arise.

Figure 4. Whitelisting a Stakeholder

Next, the shipment owner uploads the paperwork that is to be signed by the stakeholders. IPFS provides a JavaScript API[7], which handles transferring the documents to the IPFS network, returning a unique fingerprint. For every document uploaded, IPFS will return a fingerprint, which is then attached to the shipment. Attaching the document to the shipment takes place in separate transactions, one for each document.

Stakeholder Perspective

The stakeholder only has the option to amend/upload a document. There are multiple potential ways in which a stakeholder can sign a document. In its current design, however, the prototype only allows for signing a document "manually". That is, by uploading a changed copy of the document. The stakeholder will download and sign the document. This can be done digitally or by printing, signing it by hand, and scanning it. Ideally, more and more stakeholders would be signing the documents digitally.

Once the documents have been uploaded and stakeholders whitelisted, the next phase takes place, in which the documents are signed by the appropriate stakeholders. By signing a document, the stakeholder takes ownership of the document, hereby indicating that they have seen it and changed it. Also by design, documents belonging to a shipment can only be changed by stakeholders whitelisted for that shipment.

Final Evaluation

The final evaluation episode commenced once the final development iteration had been conducted. We held two final evaluation sessions with experts. In essence, the experts did not expect that the prototyping would produce results that had tangible implications for their operational processes. They got so used to the Bill of Lading and the problems to improve information flows in shipping that they did not expect that blockchain could be a solution. However, they pointed out that adopting blockchain technology to improve their information management processes seemed feasible. One of the experts noted:

"The prototype shows that the technology is far more promising than expected. This is something we could embrace now if we're bold enough." [Expert #1]

[7] https://github.com/ipfs/js-ipfs

Another expert underlined the potential value that many shipping companies might capture by switching to blockchain-based solutions, in particular given the many problems in current informational flows.

"Undoubtedly, Maersk would benefit from introducing a blockchain solution [to improve their informational flows]. I think this would be the case for most shipping companies. Current documentation systems are extremely cumbersome, complicated, and error-prone." [Expert #2]

Although the potential of public blockchain technology surprised all experts, they also met the technology with some skepticism. Implementing such a technology in the current state of the industry did not seem feasible for the experts. The primary issue they identified for this was the conservatism of the industry which previously has offset other major technologies such as cloud computing. One of the interviewees pointed out:

"[Introducing a blockchain-based solution would be] valuable for international trade as a whole – although I could imagine this would be offset by conservatism in the industry." [Expert #3]

The experts noted that preserving privacy is a crucial issue that needs to be resolved before using a public blockchain for the handling of shipping documents. While most documents do not need to be kept in private, certain documents are sensitive and require privacy. Even though this is possible on a public blockchain, the interviewees pointed out that the transaction history is still public and could therefore still be a risk to clients who were particularly sensitive about their shipments.

Overall, the expert feedback revealed an interest in embracing blockchain technology to solve the complexity of informational flows in international trade. However, issues of conservatism in the industry as well as privacy were perceived as hindrances. One of the interviewees summed up as follows:

"The prototype helped us to learn a lot about the capabilities of the technology, but I am still undecided if we should pursue the technology." [Expert #1]

Discussion and Nascent Design Principles

From our prototype and the evaluation episodes, we gather first evidence for nascent principles to design applications that mitigate the transactional risk and uncertainty in decentralized, inter-organizational environments using blockchain. These are (1) digitization, (2) tamper-proof storage of documents, (3) accessibility of the application, and (4) user authentication. Table 4 defines all four nascent design principles. In the following, we discuss how these nascent design principles address transactional risk and uncertainty in decentralized environments. Moreover, we de-abstract and elaborate how these design principles were technically embedded in our artifact.

Table 4. Nascent Design Principles

Design Principle	Description
Digitization	All data is stored and exchanged digitally.
Tamper-proof storage	All changes made to the data that are stored in the system can be retraced.
Accessibility	The system can be accessed easily even by technically non-sophisticated stakeholders.
User authentication	All activities in the system can be traced back to certain users.

Table 4. Nascent Design Principles

Digitization means that all data is stored and exchanged digitally. The reason we included digitization as a design principle is that even though it may seem commonplace, our case illustrates that physical (e.g., paper-based) information storage and exchange processes are still widespread. Digitization means that the loss or destruction of data becomes less likely, since the marginal cost of creating copies of data is basically zero, allowing for storing several copies. Moreover, it implies that information exchange becomes faster and more cost-effective. In addition, digitization is indispensable to enable the use of

blockchain technology to manage information, and thus to facilitate tamper-proof storage of information. Technically, digitization means that information is represented by binary code.

Tamper-proof storage means that all changes made to the data that is stored in the system can be retraced. For decentralized environments, this implies that information cannot get lost. Together with another design principle, user authentication, tamper-proof storage allows for tracing back all changes that have been made to identifiable users. Technically, tamper-proof storage is guaranteed by the versioned and hashed IPFS addresses stored in the smart contract. These are linked to the actual documents, which are stored in IPFS. While the IPFS addresses are self-authenticated as the link and the files root hash are interchangeable, privacy is more difficult to ensure. Given the sheer volume of documents needed for blockchain technology to serve the shipping industry, the current proof-of work-algorithm *Ethash* would certainly not be feasible. We are therefore presented with two conflicting interests in the current prototype. On the one hand, there is a need for a hashed, versioned and tamperproof state of document amendments, stored as separate transactions on the blockchain. On the other hand, the speed and privacy of transactions that centralized databases offer are desirable as well.

Further development of the prototype could be an implementation of state channel technology existing on the open protocol *Raiden* network. The *Raiden* network lets users conduct asset transfers at high speeds (1.000.000+ transactions per second are technically possible). Transfers are done via state channels. When two parties open a state channel to conduct transfers, they submit a deposit of tokens onto the blockchain that are held in a smart contract as escrow. State channels are always backed by a deposit on the chain and users can therefore rely on immediately owning the value transferred off-chain. In the state channel, users pay no transfer fees, have private transfers, and near-instantaneous transfer execution. In case of a dispute, any party can submit the state on-chain because they have cryptographic proof of being owed a certain amount of tokens in the deposit on-chain. Transfers can also happen between state channels. This is called a multihop transfer and happens without settling transfer on-chain while a small fee is paid to those that help forward the transfer. Using the Raiden Network, participants who hold many contracts and need to sign large quantities could do so by making Raiden token transfers between participating stakeholders. The two main advantages of such a setup would be that they happen privately between stakeholders and nearly instantaneously, as they do not need to get validated by the blockchain.

Accessibility means that the system can be accessed easily even by technically non-sophisticated stakeholders. For decentralized environments, accessibility is crucial, since systems need to be shared within a network of participants, while technological capabilities can be diverse at the same time. Technically, accessibility is realized in a public and permissionless blockchain, where every participant can read transaction data and submit transactions. Moreover, every participant can validate transactions. The infrastructure that is required is non-sophisticated: a dial-up Internet connection is sufficient to be able to read and inspect transactions.

User authentication means that all activities in the system can be traced back to certain users. In connection with tamper-proof storage, user authentication allows for tracing back all changes made to the data that is stored in the system to authenticated users. While data can still be forged, these activities can be traced back to users, thereby discouraging malicious behavior. Technically, user authentication works as follows: The application is associated with a public Ethereum key. This key must be unlocked with the shipment owner's private key. Once authenticated, the shipment owner can operate the application. The application only checks for an unlocked Ethereum account, it does not store the password locally.

Conclusion

In this paper, we report on a DSR project that we conducted in collaboration with Maersk, one of the leading shipping companies in the world. The paper addresses two research gaps in the blockchain literature. First, blockchain applications beyond Bitcoin are only rarely discussed, and second, the absence of more theory-driven consideration. To address these concerns, we present a prototype that illustrates how blockchain can help to make information management processes in international trade more secure, more efficient, and more trustworthy. Abstracting from problem-solving to the level of design knowledge, we provide first evidence and insights regarding nascent design principles for applications that aim to mitigate the transactional risk and uncertainty that is inherent to decentralized,

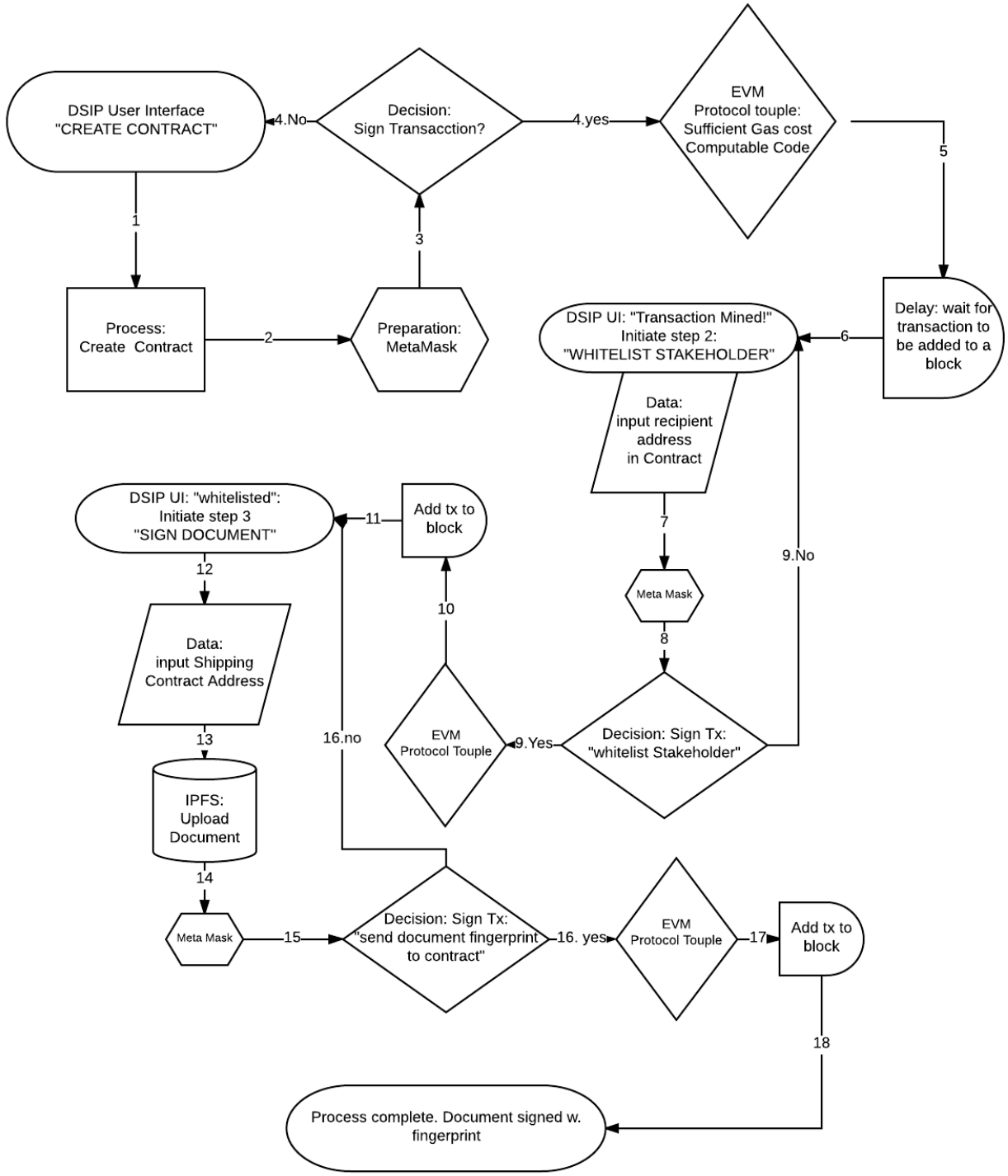
inter-organizational environments, thereby extending and complementing existing studies in the literature on blockchain technology.

This paper has several limitations. We identify the need to investigate blockchain applications for decentralized, inter-organizational environments that have already been implemented. To address this deficit, we plan to further develop our findings into more mature design principles as part of an ongoing collaboration with Maersk. Moreover, we recognize the need to move beyond looking at only one domain and one company, which imposes certain limitations in terms of the generalizability of our study. In addition, while a blockchain solution as any other software is designed locally, it has to be adopted and used globally to unfold its potentials. Thus, we are interested in design principles for network effect solutions such as public permissionless blockchains to understand better what needs to be considered in the design and creation phase, so that it provides its full potential in the later adoption and implementation phase. Nevertheless, our research can be seen as a foundation for future research to produce design theory for applications that aim to mitigate the transactional risk and uncertainty in decentralized environments using blockchain. Moreover, we acknowledge that blockchain technology as a nascent technology is still under development itself. Hence, our findings should be perceived as preliminary step towards a more holistic understanding of design principles and design theories in this area.

Acknowledgements

The research was supported by the European Blockchain Center (http://ebcc.eu).

Appendix A – Process Flow Diagram



References

Avital, M., King, J. L., Beck, R., Rossi, M., and Teigland, R. 2016. "Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future Panel," in *Thirty-Seventh International Conference on Information Systems (ICIS)*. Dublin, Ireland.

Bassindale, J. 1996. "Fraud and Bills of Lading," *Journal of Financial Crime* (4:1), pp. 33–36.

Beck, R., Czepluch, J. S., Lollike, N., and Malone, S. O. 2016. "Blockchain - The Gateway to Trust-free Cryptographic Transactions," in *24th European Conference on Information Systems (ECIS)*. Istanbul, Turkey.

Beck, R., and Müller-Bloch, C. 2017. "Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers," in *50th Hawaii International Conference on System Sciences (HICSS 2017)*. Waikoloa, Hawaii, USA, pp. 5390–5399.

Beck, R., Weber, S., and Gregory, R. W. 2013. "Theory-generating design science research," *Information Systems Frontiers* (15:4), pp. 637–651.

Betz, M., and Henningsson, S. 2016. "An Approach for Assessing the Benefits of IT Investments in Global Supply Chains," in *24th European Conference on Information Systems (ECIS)*. Istanbul, Turkey.

Böhme, R. 2016. "Perceived Benefit and Risk as Multidimensional Determinants of Bitcoin Use: A Quantitative Exploratory Study," in *Thirty-Seventh International Conference on Information Systems (ICIS)*. Dublin, Ireland.

Böhme, R., Christin, N., Edelman, B., and Moore, T. 2015. "Bitcoin: Economics, Technology, and Governance," *The Journal of Economic Perspectives* (29:2), pp. 213–238.

Buterin, V. 2014. *Ethereum White Paper*. Retrieved May 25, 2017, from http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Christidis, K., and Devetsikiotis, M. 2016. "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access* (4), pp. 2292–2303.

Glaser, F. 2017. "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis," in *50th Hawaii International Conference on System Sciences (HICSS 2017)*. Waikoloa, Hawaii, USA.

Gregor, S., and Hevner, A. R. 2013. "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Quarterly* (37:2), pp. 337–355.

Gregor, S., and Jones, D. 2007. "The Anatomy of a Design Theory," *Journal of the Association for Information Systems* (8:5), pp. 312–335.

Gunasekaran, A., and Ngai, E. W. T. 2004. "Information systems in supply chain integration and management," *European Journal of Operational Research* (159), pp. 269–295.

Güven-Koçak, S. 2015. "Maritime Informatics Framework and Literature Survey - Ecosystem Perspective," in *AMCIS 2015 Proceedings*. Puerto Rico, USA.

Hedman, J., and Henningsson, S. 2012. "Information Systems Integration in the Food Industry," in *Nordic Contributions in IS Research,* C. Keller, M. Wiberg, P. Ågerfalk, and J. S. Z. Eriksson Lundström (eds.), Heidelberg et al.: Springer, pp. 145–160.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75–105.

Hyvärinen, H., Risius, M., and Friis, G. 2017. "A Blockchain Based Approach Towards Overcoming Financial Fraud in Public Sector Services," *Business & Information Systems Engineering*, forthcoming.

Iivari, J. (2015). "Distinguishing and Contrasting two Strategies for Design Science Research," *European Journal of Information Systems* (24:1), pp. 107–115.

Jensen, T., Bjørn-Andersen, N., and Vatrapu, R. 2014. "Avocados Crossing Borders: The Missing Common Information Infrastructure for International Trade," in *Proceedings of the 5th ACM International Conference on Collaboration Across Boundaries: Culture, Distance & Technology - CABS '14*. Kyoto, Japan.

Jensen, T., and Tan, Y. 2015. "Key Design Properties for Shipping Information Pipeline," in *Open and Big Data Management and Innovation: 14th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society*. Delft, The Netherlands.

Jensen, T., and Vatrapu, R. 2015a. "Shipping Information Pipeline: Initial Design Principles," in *DESRIST 2015*. Dublin, Ireland.

Jensen, T., and Vatrapu, R. 2015b. "Ships & Roses: A Revelatory Case Study of Affordances in International Trade," in *ECIS 2015 Completed Research Papers*. Münster, Germany.

Jentzsch, C. n.d. *Decentralized Autonomous Organization to Automate Governance.* Retrieved May 25, 2017, from https://download.slock.it/public/DAO/WhitePaper.pdf

Katz, M. L., and Shapiro, C. 1994. "Systems Competition and Network Effects," *Journal of Economic Perspectives* (8:2), pp. 93–115.

Korpela, K., Hallikas, J., and Dahlberg, T. 2017. "Digital Supply Chain Transformation toward Blockchain

Integration," in *50th Hawaii International Conference on System Sciences (HICSS 2017)*. Waikoloa, Hawaii, USA, pp. 4182–4191.

Kosba, A., Miller, A., Shi, E., Wen, Z., and Papamanthou, C. 2015. *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*. Retrieved May 25, 2017, from https://eprint.iacr.org/2015/675.pdf

Li, X., and Wang, C. A. 2017. "The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin," *Decision Support Systems* (95) pp. 49–60.

Lindman, J., Rossi, M., and Tuunainen, V. K. 2017. "Opportunities and risks of Blockchain Technologies – a research agenda," in *50th Hawaii International Conference on System Sciences (HICSS 2017)*. Waikoloa, Hawaii, USA, pp. 1533–1542

March, S. T., and Smith, G. F. 1995. "Design and Natural Science Research on Information Technology," *Decision Support Systems* (15:4), pp. 251–266.

Moody, D. L. 2003. "The method evaluation model: a theoretical model for validating information systems design methods," in *Proceedings of the 11th European Conference on Information Systems (ECIS 2003)*, Naples, Italy.

Nakamoto, S. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved May 25, 2017, from http://s.kwma.kr/pdf/Bitcoin/bitcoin.pdf

Niederman, F., Clarke, R., Applegate, L., King, J. L., and Beck, R. 2017. "IS Research and Policy: Notes From the 2015 ICIS Senior Scholar's Forum," *Communications of the Association for Information Systems*, (40:1*)*, Article 5.

Orlikowski, W. J., and Iacono, C. S. 2001. "Research Commentary: Desperately Seeking the "IT" in IT Research - A Call to Theorizing the IT Artifact," *Information Systems Research* (12:2), pp. 121–134.

Peffers, K., Rothenberger, M., Tuunanen, T., and Vaezi, R. 2012. "Design science research evaluation," in *International Conference on Design Science Research in Information Systems*. Las Vegas, USA.

Peters, G. W., and Panayi, E. 2016. "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," in *Banking Beyond Banks and Money*, P. Tasca, T. Aste, L. Pelizzon, and N. Perony (eds.), Heidelberg et al.: Springer International Publishing, pp. 239–278.

Schmitz, T. 2011. "The bill of lading as a document of title," *Journal of International Trade Law and Policy* (10:3), pp. 255–280.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. 2011. "Action Design Research," *MIS Quarterly* (35:1), pp. 37–56.

Simon, H. A. 1996. *The Sciences of the Artificial* (3rd ed.), Cambridge, Massachusetts: MIT Press.

Spasovski, J., and Eklund, P. 2017. "Proof of stake Blockchain: performance and scalability for groupware communications," in *Proceedings of the International Conference on Management of Emergent Digital EcoSystems*. Bangkok, Thailand, forthcoming.

Szabo, N. 1997. *Smart Contracts*. Retrieved May 25, 2017, from http://szabo.best.vwh.net/smart.contracts.html

Tschorsch, F., and Scheuermann, B. 2016. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications Surveys & Tutorials* (18:3), pp. 2084–2123.

Venable, J., Pries-Heje, J., and Baskerville, R. 2016. "FEDS: a Framework for Evaluation in Design Science Research," *European Journal of Information Systems* (25:1), pp. 77-89.

Walsh, C., O'Reilly, P., Gleasure, R., Feller, J., Shanping, L., and Cristoforo, J. 2016. "New kid on the block: a strategic archetypes approach to understanding the Blockchain," in *37th International Conference on Information Systems (ICIS)*. Dublin, Ireland.

World Economic Forum. 2013. *Enabling Trade – Valuing Growth Opportunities*. Retrieved May 25, 2017, from http://www3.weforum.org/docs/WEF_SCT_EnablingTrade_Report_2013.pdf

World Economic Forum. 2017. *How blockchain can restore trust in trade*. Retrieved May 25, 2017, from https://www.weforum.org/agenda/2017/02/blockchain-trade-trust-transparency

Wörner, D., Von Bomhard, T., Schreier, Y.-P., and Bilgeri, D. 2016. "The Bitcoin Ecosystem: Disruption beyond financial Services?," in *Twenty-Fourth European Conference on Information Systems (ECIS 2016)*. Istanbul, Turkey.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K. 2016. "Where is current research on Blockchain technology? - A systematic review," *PLoS ONE* (11:10), pp. 1–27.