Towards an Implementation of Blockchain-based Collaboration Platforms in Supply Chain Networks: A Requirements Analysis

Lukas-Valentin Herm
University of Würzburg
lukas-valentin.herm@uni-wuerzburg.de

Christian Janiesch
University of Würzburg
christian.janiesch@uni-wuerzburg.de

Abstract

The competitiveness and speed of international markets have created significant pressure from competitors, forcing companies to collaborate with foreign companies. To address this situation, companies use supply chain networks (SCN) to concentrate on their core competencies while sourcing the remainder of (pre-)products or services. This situation often causes a lack of trust as the application of hard-to-trace illegal practices through complex SCN is a threat. The blockchain provides a solution for chaining data, enabling trust in its tamper-proof storage, even if there is no trust between business parties. Using blockchain also provides the opportunity to automate and monitor processes within digital SCNs in real-time. This paper aims to identify requirements for a blockchain-based collaboration platform in SCNs. We define the requirements based on a literature review and expert interviews. We use an additional survey to validate and prioritizes these 45 requirements.

1. Introduction

Introduced in 2008, blockchain technology, as well as the resulting cryptocurrency Bitcoin have created a fundamentally new approach in electronic payment systems [1]. Furthermore, blockchain provides secure exchange of data between users without any trustworthy intermediaries. Blockchain is a shared ledger, structured as a peer-to-peer network, with the ability for immutable and therefore tamper-proof storage for any kind of data [2]. Meanwhile, there is a lack of trust in many supply chain networks (SCN) due to competitive pressure and the resulting cooperation of many companies with new and unknown partners or even competitors. Thus, the blockchain, the so-called "trust machine", seems to be the perfect fit [3].

Restoring trust through a blockchain platform can enable the dissolution of silo-like data repositories within systems and consequently allows for (real-time) monitoring, control, and ultimately the improvement of SCNs [4].

Nevertheless, the amount of scientific publications in this field is very limited. As a result, authors such as [5] have already mentioned this lack of knowledge and the demand for further research on blockchain platforms in SCNs. In response, [6-8] discuss initial requirements for the implementation of a blockchain platform. However, these requirements only rely on a literature review and are not evaluated by practitioners, which are the primary stakeholders. Likewise, [9] show an evaluation of the postulated requirements by prototypical realization. However, their requirements primarily describe the storage and handling of transactions. On the other hand, [7] discusses findings from interviews on applying a company blockchain. However, a presentation of the resulting requirements for their prototype is missing. Beyond the primary consideration of scientific publications, it is evident that in practice, blockchain-based collaboration platforms already exist through platforms such as originChain, AgriDigital, or TradeLens [2]. Therefore, it seems necessary to gather knowledge from practitioners using scientific methods [10]. Consequently, this paper focuses on the transparent collection of requirements from literature and practice, which are necessary to implement such a blockchain-based platform. Our research question reads as follows:

RQ: What are the requirements for a blockchain-based supply chain network and how should these requirements be prioritized?

Our contribution is structured as follows: In Section 2, we present the theoretical background. In Section 3, we describe our methodology. In Section 4, we illustrate the scope of the data collection using a literature review, an interview study, and an additional survey. Summarizing in Section 5, we describe the prioritized and validated requirements derived from the data collection and analysis of Section 4. In Section 6, we conclude with a look at limitations and an outlook.

URI: https://hdl.handle.net/10125/71444
978-0-9981331-4-0

2. Theoretical background

2.1 Digital supply chain networks

Globalization entails that companies have to compete in an international and competitive market, because consumers or manufacturers are no longer bound to local companies, productions, or suppliers. Therefore, they can source in a global market [11]. This cooperation can create competitive advantages for all parties [12].

As a result, companies no longer have to perform all processes and build all components themselves, but instead can outsource them to external companies acting as service providers. Consequently, a company can focus on its core competencies and, thus on specific sections within a heterogeneous supply chain across different companies [13].

A supply chain represents a flow of materials and information between several parties that participate in creating a product from the company to the customer. These complex supply chains are also called SCN and are coordinated by supply chain management (SCM) [12].

Compared to SCN, digital supply chain networks (DSCN) represent an extension through the integration and networking of information systems. This extension allows to overcome the silo-type data storage of different companies and systems within an SCN. The result is a transparent and monitorable ecosystem [10]. The DSCN can benefit from the use of technologies such as the Internet of Things (IoT) as well as intelligent machines and infrastructures, generating real-time communication and monitoring as well as support for decision making. All heterogeneous data resulting from the processes are processed and prepared by a shared service platform. This platform enables the management of operations within the SCN, and enables creating new types of services for customers and participants [14]. However, there is usually no trust in other DSCN partners. Companies are afraid of making their knowledge available to potential competitors or becoming victims of fraud due to the increasing complexity and the resulting intransparency in supply networks. On this basis of mistrust, long-term partnerships, which are necessary for successful SCM, cannot develop [15].

Research has pointed out that trust between cooperation partners is one of SCM's most critical factors, along with factors such as commitment and interrelationships. This results in a lack of willingness to exchange information and knowledge, which complicates the use of DSCNs and the development of a service platform [14].

2.2 Blockchain

A blockchain represents a distributed and therefore, decentralized ledger containing all transactions. The structure corresponds to a concatenated chronological list of blocks, where each block contains a list of transactions. In this decentralized approach, each participant, also called a node, has an identical ledger. The distributed general ledger is characterized by its persistence, redundancy, and tamper resistance since each node can check for subsequent changes [2, 16]. The use of the blockchain divides into three different areas of application. Blockchain 1.0 defines the application in cryptocurrencies, while blockchain 2.0 focuses on the use of smart contracts for applications in business environments, such as SCM. It enables the monitoring and automation of processes using the data stored on the blockchain [2]. The blockchain application in the public sector is referred to as blockchain 3.0 [16].

Three major types of blockchains are used for these applications: public blockchain, consortium blockchain, and private blockchain. All types differ in their accessibility for participants and the resulting degree of decentralization. So, if the degree of centrality increases and the degree of anonymity decreases, the performance of block generation and the resistance to manipulation improves [17]. The procedure for creating a new block can also vary. Adding new blocks (mining) within a blockchain is done by solving mathematical calculations based on the registered nodes. Frequently used methods are proof-of-work, proof-of-stake, or byzantine fault tolerance [18]. The blockchain implementation Hyperledger Fabric, Ethereum, or VeChain use variations of these procedures [2].

2.3 Blockchain for DSCNs

Currently, DSCNs often use certified audit institutions as trusted intermediaries. These check new cooperation partners based on quality requirements. However, such central authorities represent a single point of failure [19]. Blockchain technology can create change in the consciousness of the cooperation partners and counter this deficiency [1].

Instead of building trust between the different cooperation partners, the partners instead develop confidence in blockchain technology and the resulting technically immutable and transparent storage of data [20]. This immutable basis of trust can lead to an exchange of information through the blockchain and, thus, also leads to the use of the potential of DSCN based on blockchain technology [10].

However, this leads to several challenges. Each transaction has to be validated by each node, which requires high computing power for all involved nodes

[21]. Additionally, there is no standardized blockchain architecture or blockchain implementation. As current research contributions show, blockchain projects use different implementations such as Ethereum, VeChain, or Hyperledger Fabric [20]. In addition, blockchains can store data on- or off-chain. Simultaneously, conceptual decisions must be made on the procedure for (automated) payments [17].

Furthermore, in the course of digitization, many companies have invested massively in business software such as enterprise software, which are usually not compatible with blockchain implementations [22]. Current uncertainties of announced regulatory decisions by several governments intensify this issue [21]. Since these solutions are consortium blockchains, the applications and thus the service platform as well as the necessary infrastructure, should be developed for the specific context first. Likewise, according to the current state-of-the-art, only a few practical experience reports on the blockchain's long-term use in DSCN justify investments and developments [22].

3. Methodology

For our research, we follow the Design Science Research (DSR) approach by Peffers et al. [23]. The application of DSR allows an iterative and problem-centered procedure to develop information technology-based artifacts such as implementation requirements. Simultaneously, it ensures the quality of the artifact [24]. We implement their approach using a structured literature review and an expert study for data collection from (see Figure 1 and Section 4).

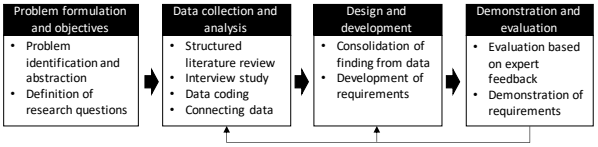

Figure 1. Research methodology according to Peffers et al. [23]

First, we determine the research artifact in the *problem formulation and objectives*: that is the definition of requirements for a blockchain-based platform in SCN to provide companies and SCNs with implementation guidance. In the *data collection and analysis*, we map the current state-of-the-art and evaluate it using a systematic literature review [25]. In addition, we conduct an interview study with practitioners as a practical comparison. In the third phase, *design and development*, we translate the collected data into requirements. We create a multi-perspective view from several information sources to allow for an objective requirements analysis. We follow the guidelines of [26] for requirements formulation and design. To ensure the collected artifact's quality, we carry out an evaluation and prioritization in the *demonstration and evaluation* phase by an additional expert survey. Lastly, we present the requirements.

4. Data collection & analysis

4.1. Literature review

We aimed to identify research papers dealing with blockchains in SCNs. In doing so, we applied a structured literature review, according to Webster and Watson [25]. We analyzed the databases Taylor & Francis Online, ScienceDirect, EmeraldInsight, Web of Science as well as Business Source Premier (ESCBOhost) to find economics-related contributions. Simultaneously, we examined IEEE Xplore and ACM Digital Library for computer science-related contributions. We also included AISeL for an information systems perspective. First, we considered limiting the results based on (journal) rankings. However, considering the novelty of the subject, we abstained from this limitation.

We used the following search term pseudocode: *((supply chain* | supply network* | value chain* | value web*) AND (blockchain | distributed ledger) AND (platform* | eco system | ecosystem | platform as a service | paas | blockchain as a service | baas))*. By performing a forward and backward search, we were able to identify a total of 618 contributions. Thereby, we classified 103 contributions as relevant through a full-text analysis. As criteria for full-text analysis, we only included contributions focusing on the theoretical and practical use of blockchain platforms applicable within SCNs, related (technical) components within these blockchains as well as related systems and users.

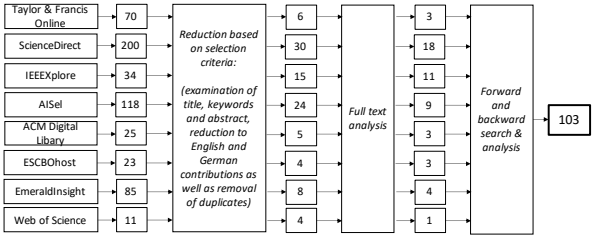

Figure 2. Result of literature review according to Webster and Watson [25]

During the literature review, we analyzed the content of these 103 contributions for the occurrence of aspects mentioned for using a blockchain platform in DSCN. We summarized similar aspects and subsequently transferred them into 10 different dimensions. Afterwards, we rechecked all contributions for the

occurrence of these dimensions. To ensure the quality of the classification, we applied an inter-rater reliability test with Fleiss' Kappa statistic [27] resulting in a so-called 'Excellent' score. We introduce the dimensions, and their frequency in the literature in Table 1.

Table 1. Extracted dimensions from the literature review

Dimension	QTY	Description
Platform implementation	72	Technical implementation of a blockchain platform
Data storage	25	Size and type of data stored on the blockchain
Data exchange	48	Data exchange between user and platform
Data privacy	21	Data privacy aspects within the platform
Administration	40	Required tasks and specifications for the management of the platform
Application	38	Potential application scenarios for users
Crypto-currencies	9	Use of cryptocurrency according to blockchain 1.0
Third parties	23	Intermediaries and their functions and responsibilities
User interfaces	16	Interfaces to manage and use the platform
Further aspects	5	Aspects in the literature, but which only occur rarely

4.2. Expert interviews

We used semi-structured interviews to allow for emerging ideas from the interviewed experts [28]. The formal design of the expert interviews is based on [29]. Therefore, the interviews are separated into three parts. First, we presented the aim of the study. Second, we asked about the experts' demographics and present a general introduction of blockchain in DSCN to ensure a shared understanding. Third, we asked the experts about the requirements of blockchain in DSCNs. In order to do so, we developed the questions based on preliminary considerations that emerged in the course of the literature review and, thus, the survey is aligned with the dimensions identified in the literature review. Also, we offered the experts the possibility to include additional dimensions. The identification of causalities and, thus, the reduction to core aspects of the interviews took place during data evaluation [30].

Following the recommendations of [31], we conducted ten interviews with experts to collect sufficient findings. Using a preliminary study based on the literature review, we identified four different stakeholder groups (SG). *Users* (U) using the platform, *platform providers* (PP) developing the infrastructure, *service providers* (SP) performing the administration, for example in smart contracts, as well as *certification providers* (CP), enabling the certification of physical components for the validation of specifications for process steps. The experts were selected according to these SGs. Due to company policies, no CP was willing to provide insights. As experts, we defined practitioners who are involved in the implementation of blockchain within SCNs. In total, our audio recordings have a length of 744 minutes (see also Table 2). The interviews were conducted in German.

Table 2. Scope of expert interviews

ID	SG	Job title	Job tenure (years)	Survey duration
I1	U	Head of Research	5-10	35min
I2	U	Junior Developer	< 2	53min
I3	U	Managing Director	> 10	1h 08min
I4	U	Chief Information Officer	< 2	1h 10min
I5	PP	Business Developer	2-5	1h 33min
I6	PP	Business Developer Manager	< 2	1h 38min
I7	PP	Product Analyst	5-10	2h 02min
I8	SP	Junior Developer	< 2	41min
I9	SP	Business Developer	2-5	1h 14min
I10	SP	Business Developer Manager	< 2	1h 30min

We transcribed the content of all recorded interviews and subsequently classified those using codes. The codes are based on the dimensions introduced in Table 1 as well as additional sub-dimensions developed in this context. The differentiation into (sub)-dimensions is detailed in Section 5. In order to analyze the interviews, we conducted a qualitative cross-sectional analysis according to [32]. Using this approach allows us to comprehensively overview the similarities and differences in the experts' perception.

4.3. Additional expert survey

To ensure the artifact's quality, we conduct an additional survey with 12 experts [23]. Using this survey, experts can validate and correct the collected requirements. Furthermore, the experts were invited to prioritize the requirements. Following [33], we classified requirements in three stages:

1. *Mandatory (MA)*: The requirement must be integrated for the operation of the platform.
2. *Optional (OP)*: The requirement should be integrated to increase the effectiveness as well as the efficiency of the platform.
3. *Not necessary (NN)*: The requirement is not relevant for the platform.

In order to enable an objective prioritization, we converted the results into numerical values and transformed the resulting averages back into the three stages introduced above [34].

5. Requirements derivation

In the following, we show the synthesis of the literature review as well as the expert interviews according to the identified dimensions above. For a better overview, we display the dimensions with additional subdimensions. Furthermore, we integrated the validation and prioritization from the additional expert survey. The full research data is available at [35].

Dimension: platform implementation

Blockchain type. Several authors describe the use of a consortium blockchain due to legal requirements as well as the higher processing speed compared to public platforms (cf. for example [36]). The interviewees I5 to I7 confirmed this. Nevertheless, some authors such as [37] consider the possibility of a hybrid double chain architecture.

REQ1 (MA): For the collaboration platform, the implementation must use a consortium blockchain.

Blockchain implementation. According to contributions such as [6], Hyperledger Fabric, which is most frequently mentioned in literature reviews, is characterized by its low latency, validation time, multi-level read/write permissions as well as high scalability of transactions. I7 sees the development primarily through popular programming languages as the main reason for its application. I5 and I6 mention the additional trust of users in the company IBM, which is co-developing Hyperledger Fabric. Following I5 and I7, the Ethereum platform's use is not an option for smart contracts due to gas costs.

REQ2 (MA): The software implementation of the blockchain must be based on Hyperledger Fabric.

Consensus algorithm. In the literature review, we identified various consensus-building procedures. According to [38], it is essential to use a lightweight but still secure consensus algorithm in SCM. I5 and I7 confirm and consider that the consensus algorithm does not offer any monetary incentives for the validation of blocks but provides a fair and equally distributed procedure. All companies should participate in this process with equal shares.

I4 and I5 point out within the requirement validation that in REQ4 the number of parties necessary for consensus building must be integrated, otherwise the requirement can be misunderstood. In literature, contributions such as [39] have shown that procedures like proof-of-work or proof-of-stake are not suitable in a consortium blockchain. Several contributions, such as [40] propose the practical Byzantine fault tolerance procedure.

REQ3 (OP): The consensus algorithm must allow for an equal distribution of consensus-building among all users of the collaboration platform.

REQ4 (OP): All users must participate in the block validation process as required by the consensus algorithm. The consensus algorithm determines the number of parties required for consensus-building.

Node structure. [41] describe that all platform participants should be able to participate in the block mining process. According to [41], I5, and I6, the validation of blocks should be carried out by the participating companies. According to I6, it should be possible for companies to purchase this process as a service. The SP carries out the generation and validation on behalf of the users of the platform [42].

REQ5 (MA): Participating companies must be able to outsource the mining process on the blockchain in the form of a continuous service.

Dimension: data storage

On- and off-chain. Both, in literature as well as the experts mentioned that not all data should be stored on the blockchain due to scalability issues. I5 describes the necessity of storing all relevant information for direct traceability on the blockchain. According to [36] as well as I5 and I6, necessary on-chain data has to be determined based on the application scenario. The remaining data should be stored off-chain. However, the checksums of this data are stored on the blockchain and should use cryptographic hash functions (I9).

REQ6 (OP): Only data necessary for traceability should be stored on the blockchain. The definition is determined by the application scenario.

REQ7 (MA): Data not stored on the blockchain must be checked for unchangeability using checksums based on cryptographic hash functions. The checksum is stored on the blockchain.

Cloud storage. Process data or transactions, which are not to be saved on the blockchain, must be accessible through cloud solutions [43], I6. I7 mention that cloud services like Amazon Web Service do not meet all requirements, such as data security. I3 confirms this problem. I10 further clarifies in our validation interviews that these cloud solutions must also be decentralized. I7 and I9 also define the necessity of on-premise solutions for internal company data, which should not be stored on the blockchain.

REQ8 (OP): Decentralized cloud solutions must be used for storing data outside the blockchain, which enable the permanent availability of the data. On-premise solutions can be used for internal company data.

REQ9 (MA): Decentralized cloud solutions must be used to satisfy the users' data protection requirements.

Dimension: data exchange

Enterprise systems. For the automated exchange of transactions between enterprise systems, a standard has to be created according to [10], I5, and I7. Only I7 provides an example of the exchange of metadata using lightweight standards such as JSON or XML. The interview study revealed that all interviewees would adopt a proposed standard.

REQ10 (MA): A standardized data format must be defined to exchange transaction data between ERP systems.

REQ11 (MA): The data format must be adapted to exchange transactions via the blockchain.

Sensor technology. To perform a standardized and automated evaluation of sensor data, a data structure must be defined for the used sensors. Several authors introduce JSON as well as XML [44]. I1 and I4 also mention these formats. I7 additionally proposes the consideration of the IoT standard O-MI/O-DF.

REQ12 (MA): For the exchange of data, the platform must support the data structure of JSON as well as XML.

Similarly, according to I5 as well as I6, an automated and standardized retrieval of data from production facilities is required. An OPC-UA interface is usually applied for this purpose.

REQ13 (OP): For the storage of production data on the blockchain, the platform must provide an interface that supports the OPC-UA data exchange standard.

Dimension: data privacy

Legal handling. In a consortium, companies are not allowed to interact anonymously [5]. However, no personal data is allowed to be stored in the blockchain, for example to comply with the GDPR. This applies not only to nodes that are active in Europe, but to all personal data of EU citizens [45]. This fact is also confirmed by I1 and I4, which additionally classify the storage of checksums of personal data as legally problematic due to the lack of legislation.

REQ14 (MA): No personal data as well as the checksums of this personal data must be stored on the blockchain.

Data privacy. Concerning data privacy, various authors indicate the need to set up different access levels [6]. All interviewees agree with this fact. I1 also describes that competing companies cannot see any transaction history with customers of other companies.

REQ15 (OP): A multi-level permission system must be implemented on the platform. This defines the read and write permissions. The number of levels as well as their differentiation must be decided per use case.

REQ16 (MA): The permissions system must allow data to be visible only to specific participants.

State organizations. According to [5], I5, and I7, no data should be hidden from governmental organizations due to the required checks to detect manipulations. In the requirement validation phase, I4 and I5 state that this should only be done in suspicious cases.

REQ17 (OP): The platform must offer governmental organizations read access to all stored data for suspicious cases.

Dimension: administration

Integration of users. According to [46], the management of a user should be done by a superuser. I5 and I7 confirm this. Also, I7 sees the requirement to integrate several of these super users into the platform. A majority vote ensures objectivity as well as prevents a single point of failure. This administration role is performed by an SP (I7).

REQ18 (OP): Administrators must perform the management of users. Service providers perform this task.

REQ19 (MA): Multiple administrators must perform the management. All administrators must agree to the process by a majority vote.

The admission of companies may not be unrestricted but must be checked against various criteria such as the business license or the liquidity of companies [41]. I9 and I10 recommend the adaptation of the "know-your-customer" principle. Likewise, I8 and I10 describe the review of technical requirements for the company to operate a node.

REQ20 (MA): Before a user is allowed to join the platform, a check must be performed. This must be based on business factors according to the "know-your-

customer" principle on the one hand and the fulfillment of technical requirements on the other hand.

Management of the public/private keypair. If a user loses his public/private keypair, the user will be excluded from the platform. I5, I6, and I9 suggest developing guidelines for users to counteract the loss of keypairs. According to I8, the storage of keypairs by SPs is not a solution due to the potential for abuse.

REQ21 (MA): In order to counteract the loss of public/private keypairs by users, guidelines for keypair handling must be developed.

Development support for smart contracts. The survey revealed the need to offer the possibility of having smart contracts developed by users themselves (I1), but also to be able to develop them in collaboration with an SP (I2 and I4).

REQ22 (MA): The development of smart contracts must be possible by users as well as by service providers.
REQ23 (MA): Service providers can offer the development of smart contracts for users as a service.

Industry-specific and configurable templates should be developed to support this. These templates should be addressable through a Web interface and guide the developer through a tutorial [42]. Also, the program code should also be readable by non-technical users. This can be achieved by providing pseudocode (I5, I6, I9, and I10). In addition, smart contracts should be modularizable by graphical modeling tools using modeling standards such as BPMN (I7 and I9).

REQ24 (OP): For the development of smart contracts, configurable and industry-specific templates must be offered. These templates should support the developer with hints and instructions.
REQ25 (OP): It must be possible to develop smart contracts modularly and sequentially using graphical modeling tools.
REQ26 (MA): Smart contracts templates must meet regulatory and industry-specific requirements.
REQ27 (OP): Smart contracts templates must be addressable through Web interfaces on the platform.
REQ28 (MA): Each smart contract must be traceable by displaying the source code as well as the associated pseudo code.

Due to the autonomous execution of smart contracts on the blockchain, validity periods must be defined by specifying timestamps [47].

REQ29 (OP): Time validity periods must be defined for the execution of each smart contract.

Management of smart contracts and oracles. A presentation of active smart contracts must be implemented on the platform [48]. I5, I7, and I9 suggest a process map. It should enable real-time monitoring of smart contracts and their relationships (I9 and I10). If information not stored on the platform is required to execute smart contracts, oracles must be used (I6).

REQ30 (MA): To display active smart contracts, an implementation of a representation must be performed. The visualization must provide an overview of the smart contracts' activities and their relationships to other smart contracts and participants.

According to I7, only certified sources should be allowed to store in the blockchain to prevent the integration of falsified or manipulated information into the platform.

REQ31 (MA): Sources that provide information for oracles must be certified.

Dimension: application

According to I9 and I10, the collaboration platform must also contain a marketplace component-oriented towards existing digital trading platforms. This marketplace should offer the development of smart contracts or service bundles. Users should be able to search or be informed by using search functions and suggestions. Adjustments are to be made possible by individual agreement (I10).

REQ32 (OP): The platform must provide a digital marketplace for smart contracts or further services. The service providers will carry out the development of the services.
REQ33 (MA): Users should be able to search for (industry-specific) services and providers in the digital marketplace using search functions.
REQ34 (OP): Users should receive industry-specific services proposed through the digital marketplace.
REQ35 (OP): A communication interface should enable users and service providers to adapt existing services or to request new services individually.

Dimension: cryptocurrencies

Cryptocurrencies can be used for the realization of marketplaces [49]. In the validation interview, I7 suggests the integration of an interface to an existing token system as a possible alternative to a consortium

blockchain. According to [46], a price-stable crypto-currency must be chosen. It is also essential to be able to convert it back into a more common currency. Due to a tokens' price stability compared to cryptocurrencies, I2 and I4 primarily see the use of tokens on the platform.

Due to the lack of price stability of cryptocurrencies, acceptance is too low according to I1. I3 points out that traditional payment methods such as bank transfers or transfer cheques still have to be used in addition to tokens.

REQ36 (OP): The platform must enable payment for services as well as for the processing of automated transactions through an integrated token system or an interface to a token system.

REQ37 (MA): The platform must, in the case of an integrated token system, provide the possibility of exchanging tokens back into regular currencies.

REQ38 (MA): In addition to the use of tokens, traditional payment methods such as bank transfer and transfer cheques should also be available for payment on the platform.

Dimension: third parties

In literature, the certification authorities validate products or product batches, for example in quality control [50]. I1 and I2 confirmed the necessity of a collaboration platform. [5] extend this to additional verification of sensors used in production. It is also necessary to review smart contracts as well as to certify oracles periodically [45] and I9.

REQ39 (OP): Certification authorities are required to perform the inspection of products, product batches, and the used sensors.

REQ40 (OP): Certification authorities can perform the audit of smart contracts and oracles according to certifications.

Dimension: user interfaces

Design guidelines. User interfaces should be based on lightweight frameworks and be available on various application devices [51], (I1, I3). The interviewees mention the use of HTML for development. All user interfaces should be available at least 99 % of the time (I3, I7).

Similarly, a query of information should not exceed 10 seconds, whereas international queries should not exceed two minutes. Within the validation, I2 extends the restriction to only queries of data from the blockchain itself.

REQ41 (MA): The user interfaces must be developed using a Web-based description language to allow access from different devices.

REQ42 (MA): All implemented user interfaces should be available at least 99 % of the time.

REQ43 (MA): A query of data from the blockchain must not exceed 10 seconds. For international queries, a maximum of 2 minutes applies.

Handling of incorrect input. Authors such as [52] describe the issue of irrevocably stored data with incorrect inputs on a blockchain platform. As a potential solution, I7 represents an automated input validation based on plausibility checks. I6 considers the use of the four-eye-principle as critical due to the time delay.

REQ44 (OP): In order to reduce incorrect manual inputs by users, automated plausibility checks must be performed in the user interfaces. The plausibility checks are defined in cooperation with the users.

Dimension: further aspects

[53] as well as I6 highlight that many users are not familiar with the blockchain technology. To ensure acceptance as well as efficient handling of the platform, it is necessary to offer various training sessions. In the validation phase, I9 also adds the necessity of developing training videos and Frequently Asked Questions (FAQ) sections.

REQ45 (MA): Training sessions, training videos, and FAQs on blockchain technology as well as the use of the collaboration platform must be offered.

6. Conclusion and outlook

Globalization enables new potentials for companies, including the possibility of participating in global SCNs and thus focusing on their core competencies. These potentials are not without issues [54]. Companies often have concerns about the eventuality of cooperation partners not adhering to contractual agreements [15]. This can lead to inherent consequences for the process flow in SCNs. Blockchain enables immutable storage of data [2]. The use of the blockchain within SCNs can thus make fraud attempts and manipulations more difficult [21]. This data storage also allows for the automation and monitoring of transactions in the context of a platform, which has been discussed previously [7].

The objective of our contribution was to identify requirements for such a blockchain-based collaboration platform. The requirements should enable a transfer into practice. Based on a literature review, expert interviews as well as a survey, we identified 45 requirements,

which can be divided into ten thematically different dimensions.

In the process of data synthesis, we also identified several limitations. Due to the topicality as well as the lack of scientific publications, it was necessary to settle with qualitative limitations in the literature review [40]. Similarly, there are limitations in the data evaluation of the expert interviews. Primarily, open legal questions make a concrete survey from practice difficult. For example, there are legal uncertainties in handling data privacy guidelines or currently open efforts by various governments, such as the Federal Republic of Germany, to handle cryptocurrencies in practice [55]. Furthermore, we contacted several CPs for interviews. However, none of these CPs were willing to talk to us, due to concerns regarding their company policies.

Nevertheless, our requirements can serve as guidance for the establishment of blockchain-based DSCN platforms. In our further research, we want to use these requirements to develop different prototypes for practice and subsequently develop a reference architecture to integrate blockchain-based platforms in DSCNs.

7. Acknowledgement

This research and development project is funded by the German ministry of education and research (BMBF) within the research program "Industrie 4.0– Kollaborationen in dynamischen Wertschöpfungs-netzwerken (InKoWe)" (grant no.: 02P17D160) and managed by the Project Management Agency Karlsruhe (PTKA).

8. References

[1] S. Nakamoto, A peer-to-peer electronic cash system, 2008, https://bitcoin.org/bitcoin.pdf (Accessed: 19-05-2020)

[2] X. Xu, I. Weber, and M. Staples, Architecture for blockchain applications, Springer, Berlin, Heidelberg, 2019.

[3] T. Economist, The trust machine, 2015, https://www.economist.com/leaders/2015/10/31/the-trust-machine (Accessed: 20-05-2020)

[4] Y. Yang, W. Huisman, K. Hettinga, N. Liu, J. Heck, G. Schrijver, L. Gaiardoni, and S. van Ruth, "Fraud vulnerability in the Dutch milk supply chain: Assessments of farmers, processors and retailers", Food control, 95, 2019, pp. 308-317.

[5] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: Analysis, requirements and open issues", Future Generation Computer Systems, 100, 2019, pp. 325-343.

[6] I. Weber, Q. Lu, A. B. Tran, A. Deshmukh, M. Gorski, and M. Strazds, "A platform architecture for multi-tenant blockchain-based systems", In Conference on Software Architecture, IEEE, Hamburg, 2019, pp. 101-110.

[7] Q. Lu, X. Xu, Y. Liu, and W. Zhang, "Design pattern as a service for blockchain applications", In International Conference on Data Mining Workshops, IEEE, Singapore, 2018, pp. 128-135.

[8] K. Behnke and M. Janssen, "Boundary conditions for traceability in food supply chains using blockchain technology", International Journal of Information Management, 52 (C), 2020, pp. 1-10.

[9] T. Sund and C. Lööf, Performance Evaluation of a Blockchain-Based Traceability System: A Case Study at IKEA, 2019, http://www.diva-portal.org/ smash/get/-diva2:1307991/FULLTEXT01 (Accessed: 23-05-2020)

[10] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration", In Proceedings of the 50th Hawaii International Conference on System Sciences, IEEE, Hawaii, 2017, pp. 4182-4191.

[11] T. Levitt, "The globalization of markets", Harvard Business Review, 61 (3), 1993, pp. 92-102.

[12] H. Wannenwetsch, Integrierte Materialwirtschaft, Logistik und Beschaffung, Springer, Berlin, 2014.

[13] H. Håkansson and G. Persson, "Supply chain management: the logic of supply chains and networks", The international journal of logistics management, 15 (1), 2004, pp. 11-26.

[14] J. Yan, S. Xin, Q. Liu, W. Xu, L. Yang, L. Fan, B. Chen, and Q. Wang, "Intelligent supply chain integration and management based on cloud of things", Journal of Distributed Sensor Networks, 10 (3), 2014, pp. 1-15.

[15] Y. Wang, M. Singgih, J. Wang, and M. Rit, "Making sense of blockchain technology: How will it transform supply chains?", International Journal of Production Economics, 211, 2019, pp. 221-236.

[16] M. Swan, Blockchain: Blueprint for a new economy, O'Reilly Media, Inc., Tokyo, 2015.

[17] H. Wu, Z. Li, B. King, Z. Ben Miled, and J. Wassick, "A distributed ledger for supply chain physical distribution visibility", Information, 8 (4), 2017, pp. 137-155.

[18] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey", International Journal of Web and Grid Services, 14 (4), 2018, pp. 352-375.

[19] L. Wu, X. Yue, A. Jin, and D. C. Yen, "Smart supply chain management: a review and implications for future research", The International Journal of Logistics Management, 27 (2), 2016, pp. 395-417.

[20] J. Wang, P. Wu, X. Wang, and W. Shou, "The outlook of blockchain technology for construction engineering management", Frontiers of engineering management, 4 (1), 2017, pp. 67-75.

[21] H. Min, "Blockchain technology for enhancing supply chain resilience", Business Horizons, 62 (1), 2019, pp. 35-45.

[22] V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model", Business Horizons, 62 (3), 2019, pp. 295-306.

[23] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research", Journal of management information systems, 24 (3), 2007, pp. 45-77.

[24] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research", MIS quarterly, 20 (4), 2004, pp. 75-105.
[25] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review", MIS quarterly, 26 (2), 2002, pp. xiii-xxiii.
[26] K. Pohl, Requirements engineering: fundamentals, principles, and techniques, Springer, Berlin, 2010.
[27] J. L. Fleiss, "Measuring nominal scale agreement among many raters", Psychological bulletin, 76 (5), 1971, pp. 378-382.
[28] G. Paré, "Investigating information systems with positivist case research", Communications of the association for information systems, 13 (1), 2004, pp. 18.
[29] H. Moosbrugger and A. Kelava, Testtheorie und Fragebogenkonstruktion, Spring, Berlin, 2012.
[30] J. Gläser and G. Laudel, Experteninterviews und qualitative Inhaltsanalyse als Instrument rekonstruierender Untersuchungen, Verlag für Sozialwissenschaften, Wiesbaden, 2010.
[31] D. W. Stewart and P. N. Shamdasani, Focus groups: Theory and practice, Sage publications, London, 2014.
[32] T. Wilde and T. Hess, "Forschungsmethoden der Wirtschaftsinformatik", Wirtschaftsinformatik, 49 (4), 2007, pp. 280-287.
[33] T. Meiren and V. Liestmann, Service Engineering in der Praxis, Fraunhofer-IRB, Stuttgart, 2002.
[34] P. Berander and A. Andrews, "Requirements prioritization", Engineering and managing software requirements, Springer, Berlin, 2005, pp 69-94.
[35] L.-V. Herm and C. Janiesch, "Requirements analysis for a collaborative platform in blockchain-based supply chain networks", Working Paper Series of the Institute of Business Management - University of Wuerzburg, 7, 2019.
[36] S. E. Chang, Y.-C. Chen, and M.-F. Lu, "Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process", Technological Forecasting and Social Change, 144, 2019, pp. 1-11.
[37] M. Cash and M. Bassiouni, "Two-tier permission-ed and permission-less blockchain for secure data sharing", In International Conference on Smart Cloud, IEEE, New York, 2018, pp. 138-144.
[38] M. Hulea, O. Rosu, R. Miron, and A. Aştilean, "Pharmaceutical cold chain management: Platform based on a distributed ledger", In Conference on Automation, Quality and Testing, Robotics, IEEE, Cluj-Napoca, 2018, pp. 1-6.
[39] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. Van Nieuwenhuyse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology", Future Generation Computer Systems, 86, 2018, pp. 641-649.
[40] H. Yuan, H. Qiu, Y. Bi, S.-H. Chang, and A. Lam, "Analysis of coordination mechanism of supply chain management information system from the perspective of block chain", Information Systems and e-Business Management, 2 (1), 2019, pp. 49-72.
[41] S. Hua, E. Zhou, B. Pi, J. Sun, Y. Nomura, and H. Kurihara, "Apply blockchain technology to electric vehicle battery refueling", In Proceedings of the 51st Hawaii International Conference on System Sciences, IEEE, Hawaii, 2018, pp. 25657-25665.
[42] O.-B. Kwame, Q. Xia, E. B. Sifah, S. Amofa, K. N. Acheampong, J. Gao, R. Chen, H. Xia, J. C. Gee, X. Du, and M. Guizani, "V-Chain: A Blockchain-Based Car Lease Platform", In Physical and Social Computing, IEEE, Halifax, 2018, pp. 1317-1325.
[43] M. C. Lacity, "Addressing key challenges to making enterprise blockchain applications a reality", MIS Quarterly Executive, 17 (3), 2018, pp. 201-222.
[44] A. Angrish, B. Craver, M. Hasan, and B. Starly, "A case study for blockchain in manufacturing:"FabRec": a prototype for peer-to-peer network of manufacturing nodes", Procedia Manufacturing, 26, 2018, pp. 1180-1192.
[45] R. P. George, B. L. Peterson, O. Yaros, D. L. Beam, J. M. Dibbell, and R. C. Moore, "Blockchain for business", Journal of Investment Compliance, 20 (1), 2019, pp. 17-21.
[46] F. Glaser, "Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis", In Proceedings of the 50th Hawaii International Conference on System Sciences IEEE, Hawaii, 2017, pp. 1543-1552.
[47] M. Bartoletti and L. Pompianu, "An analysis of Bitcoin OP_RETURN metadata", In International Conference on Financial Cryptography and Data Security, Springer, Malta, 2017, pp. 218-230.
[48] Q. Lu, X. Xu, Y. Liu, I. Weber, L. Zhu, and W. Zhang, "uBaaS: A unified blockchain as a service platform", Future Generation Computer Systems, 101, 2019, pp. 564-575.
[49] Y. Yanovich, I. Shiyanov, T. Myaldzin, I. Prokhorov, D. Korepanova, and S. Vorobyov, "Blockchain-Based Supply Chain for Postage Stamps", In Informatics, vol. 5, 2018, pp. 2-9.
[50] S. Seebacher and M. Maleshkova, "A model-driven approach for the description of blockchain business networks", In Proceedings of the 51st Hawaii International Conference on System Sciences, IEEE, Hawaii, 2018, pp. 3487-3496.
[51] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance", Intelligent Systems in Accounting, Finance and Management, 25 (1), 2018, pp. 18-27.
[52] M. Zachariadis, G. Hileman, and S. V. Scott, "Governance and control in distributed ledgers: understanding the challenges facing blockchain technology in financial services", Information and Organization, 29 (2), 2019, pp. 105-117.
[53] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things", In International Conference on Service Systems and Service Management, IEEE, Dalian, 2017, pp. 1-6.
[54] J. Sydow, Strategische Netzwerke: Evolution und Organisation, Springer, Wiesbaden, 2013.
[55] Bundesregierung, Blockchain-Strategie, 2020, https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/blockchain-strategie-1546662 (Accessed: 01.04.2020)