



HAL
open science

Blockchain-Based Master Data Management in Supply Chains: A Design Science Study

Jacob Lohmer, Lasse Bohlen, Rainer Lasch

► To cite this version:

Jacob Lohmer, Lasse Bohlen, Rainer Lasch. Blockchain-Based Master Data Management in Supply Chains: A Design Science Study. IFIP International Conference on Advances in Production Management Systems (APMS), Sep 2021, Nantes, France. pp.51-61, 10.1007/978-3-030-85910-7_6 . hal-03806509

HAL Id: hal-03806509

<https://inria.hal.science/hal-03806509>

Submitted on 7 Oct 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.




Distributed under a Creative Commons Attribution 4.0 International License



This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

Blockchain-based master data management in supply chains: a design science study

Jacob Lohmer¹[0000-0002-3197-6159], Lasse Bohlen², and Rainer Lasch¹

¹ Chair of Business Management, esp. Logistics, Technische Universität Dresden, Germany
² Chair of Business Informatics, esp. Intelligent Systems and Services, Technische Universität Dresden, Germany

{jacob.lohmer, lasse.bohlen, rainer.lasch}@tu-dresden.de

Abstract. Master data management is an essential task for organizations and even more critical when collaborations are pursued. Using centralized platforms to manage master data across business partners is straightforward but also entails risks. Besides the dependency on intermediaries, data sovereignty is limited and a single point of failure persists. With new decentralization trends and the uprising blockchain technology, there is potential for optimized and sovereign master data management across entities. We conduct a design science study to assess blockchain technology's suitability to store and share master data in supply chains. The developed artifact was quantitatively evaluated, focusing on costs and transaction time to further contribute insights to blockchain technology's economic suitability. The Ethereum-based application was implemented in *evan.network* and *Ropsten* test networks. The results substantiate the previous theoretical statements in the literature with reliable numerical data, which indicate that permissioned blockchain networks are more scalable and low-cost than permissionless networks. We also highlight further research opportunities.

Keywords: Blockchain technology, digital supply chain management, master data management, design science research, technology implementation

1 Introduction

In the modern business world, information systems are the backbone of activities. Business transactions' success depends significantly on data, which have to be maintained and shared while kept up to date at high-quality levels. Effective information flow among supply chain partners enhances the integration of supply chains [1]. Most transactions between entities in supply chains rely heavily on master data stored in individual databases like ERP systems. Therefore, the quality of master data is even more relevant [2]. Ensuring that correct and up-to-date master data is available and integrated into the information systems enables business transactions to be carried out in a time- and resource-efficient manner. Master data is usually created once and regularly re-used, referring to customers, products, or vendors as central business objects [2, 3]. The increasing collaboration of companies in supply chain management (SCM) also makes

it necessary to exchange master data more frequently, which is difficult due to individual firms' often isolated data silos. Therefore, concepts such as master data management (MDM) aim to eliminate quality problems and integrate information systems [4, 5]. The mentioned issues have led to central players in the market providing platforms that support data sharing and accessibility for many companies, e.g. *Infor Nexus*, *E2open* or *One Network Enterprises*. However, new problems arise with central data storage or integration of the central interface, such as dependency and a single point of failure. A decentralized solution for MDM offers some advantages, but the technical implementation has been a complicated task until now. Here the aspiring blockchain technology (BCT) comes into play. Initially developed for financial transactions, this decentralized technology enables many participants to agree on a valid state for a distributed system even when malicious agents are involved. No central instance is needed in the process, while BCT promotes high data quality [6, 7]. An application of BCT for collaborative MDM is promising but has not yet been explored. In the context of a design science study, we assess the usefulness of a blockchain master data application and develop a technical artifact to answer the following research questions: **RQ1**. How can blockchain technology improve MDM in supply chains? **RQ2**. What are the economic implications, chances and risks of a blockchain-based MDM application for SCM?

The remainder of this study is structured as follows. We discuss the theoretical background of our study in Sect. 2, focusing on collaborative data management and blockchain technology. Sect. 3 provides details on the methodology of this article and our approach. Next, we present the MasterData Application as the developed artifact in Sect. 4, followed by the application tests and assessment of results. We discuss the findings in Sect. 5 and conclude with further research opportunities in Sect. 6.

2 Theoretical Background

Many organizations maintain disparate systems with redundant data storage due to historically grown IT landscapes [3]. Master data is used to describe the main entities of business activities, is rarely changed with a constant overall volume and is referenced by transactional data [8, 9]. Virtually all IT processes in a business depend on master data, and they form the basis for cross-company collaboration. Accurate master data is crucial in this context and requires substantial effort, as standardized or automated processes rarely exist [8]. Managing master data is complex due to various requirements, often unclear data ownership and spread management responsibilities [4]. One of the tasks is metadata maintenance, which describes and defines other data's properties, such as reading and writing permissions, modification dates or data origin [5, 9]. Efficient data management is even more challenging in collaboration, as the participating partners' IT departments have to be aligned. Besides, there is a lack of cross-company standards for data models and functionalities [8, 10]. MDM addresses data quality issues through standardization and integration of processes and information systems [4]. Existing architectures for collaborative MDM can be broadly classified into three groups: decentralized synchronization (bilaterally between partners); centralized synchronization via an intermediary (storing and providing metadata and master data in a data pool);

and a hybrid form, in which e.g. metadata is stored in a central data pool and master data is exchanged bilaterally [10]. In the last years, a move towards central players as intermediaries is evident due to missing methods for decentralized or hybrid MDM [10]. New problems arise with centralized platforms, such as dependency or single points of failure. Thus, alternatives to centralized systems are worth exploring.

Blockchain is an uprising technology that might lead to a substantial change here. The database operates on a transaction basis rather than a state-based approach. Centered on cryptography and peer-to-peer networks, BCT is one of several distributed ledger technologies (DLT) that immutably log transactions of virtually any form in a chronological chain of blocks [11]. Other forms of DLT that are not in the focus of this study include directed acyclic graphs [12]. Key features of BCT in SCM include transparency, immutability, irreversibility, disintermediation, and smart contract automation potential [6, 13, 14]. Initial research has examined BCT for leak-free and qualitative data sharing in supply chains [15]. Various forms of blockchain systems can be differentiated, e.g. by consensus algorithm and accessibility. Consensus defines how the participants agree on the system's status, with variants differing according to the basic concept of trust creation. The most common variants are Proof-of-Work (PoW) and Proof-of-Authority (PoA). In PoW, the decision-making authority about the system's status is distributed among the network participants according to their committed computing power. As anyone can participate in reaching consensus, these networks are called permissionless [11]. In PoA, the majority of a subset of nodes, called "authorities", decides whether to include or reject a transaction [16]. PoA is especially suited for permissioned networks in which all authorities are known and trusted, and reputation is an important parameter [17]. Therefore, accessibility can be differentiated into permissioned and permissionless networks (writing rights) and public and private systems (reading rights) [6]. Famous examples for public and permissionless systems are cryptocurrencies like Bitcoin or Ethereum, while most proof-of-concepts and industry applications are based on private and permissioned networks. Collaborating entities can automate data management in distributed configurations with BCT by using smart contracts, i.e. a program that runs on the blockchain and blockchain-based identity management.

In SCM, a wide variety of aspects have been considered (see e.g. [15, 17–21]), but the area of master data management has not yet been linked to BCT. Relating the technology features to the theoretical background of data management and the diverse sets of quality criteria for MDM, we focus on three categories of quality criteria that are discussed in the literature to assess the suitability of BCT: data accuracy, data accessibility and data representation [2, 8, 22, 23]. Table 1 shows the criteria that will be used to evaluate BCT for MDM.

Table 1. Quality criteria for MDM

<i>Category</i>	<i>Rationale</i>
Data accuracy	
timeliness	the time interval between a real-life data change and the corresponding adjustment of the attribute values in the IT system
completeness	no missing data points, and all relevant data for respective processes available
accuracy	match of attribute values of the data objects with the real-life data properties

<i>Category</i>	<i>Rationale</i>
reputation	data source, transport medium and the processing information systems are highly reputable, traceable, and well-known
Data accessibility	
access security	describes the reliability of data access (i.e. resilience)
accessibility and availability	data accessibility is at a high level if retrievable by users using simple procedures
processability	attribute values can be easily adapted and supplemented by authorized users
flexibility	basic characteristics can be easily adapted as e.g. requirements change
Data representation	
identifiability	data objects should be easily identifiable (i.e. clearly assigned to real-life counterpart)
metadata	describe additional data properties - if comprehensive metadata is available and trustworthy, it can support master data management processes
non-redundancy	minimal redundancy is targeted to prevent possible data inconsistencies

3 Methodology

We follow the design science research (DSR) methodology for this study [24, 25]. Originating in research on information systems, the DSR aims to create a technical artifact that addresses a relevant problem and evaluate it rigorously [24]. The main stages of DSR include problem identification and motivation, defining objectives of a solution, design and development of the artifact, demonstration, evaluation and communication with iteration steps between the phases [25].

The first DSR stage (problem identification) has been addressed in the first two sections. We assess BCT's suitability to manage master data in supply chains to overcome the issues in centralized, platform-based MDM. Based on insights from centralized platforms and the literature, we derived functionalities that the blockchain-based concept should provide for SCM applications: The concept should comprehensively map master data on the blockchain, replacing a centralized data pool. Thus, firms can create their representations and organizational units (as digital twins) and assign specific master data attributes shared in the network. The ability to represent relationships between individual organizational units should enable the efficient identification of master data objects. Besides, features to rate and digitally sign individual data attributes of other network participants need to be integrated to enable collaborative MDM. Such cross-organizational processes also require basic rights management. Roles should be assigned to individual network participants for each organizational unit. These roles determine who can create, edit, delete, rate, and sign individual data attributes.

In this way, the blockchain-based MDM system can enable minimizing the trust needed for interactions: Data and transactions are stored persistently, digital signatures are enabled, transparency is increased, and smart contracts are integrated. The artifact's objectives are a demonstration of technical feasibility, sufficient scalability and economic applicability. Test runs in varying configurations in different systems are necessary to provide an accurate statement about the expected scalability and costs.

4 Concept

4.1 MasterData Application

The developed technical artifact is a web-based application suitable for collaborative MDM. It includes a backend consisting of smart contracts running on Ethereum and a graphical user interface (GUI) developed on the JavaScript software library *React* as the frontend. The GUI supports the basic functionalities needed for collaborative MDM, e.g. searching or filtering of organizational elements. Communication between the GUI and the backend was established using the Ethereum JavaScript API *web3js* that enables the creation of transactions, signing and generally exchanging data with an Ethereum-based network. The technical architecture of the system is shown in Fig. 1:

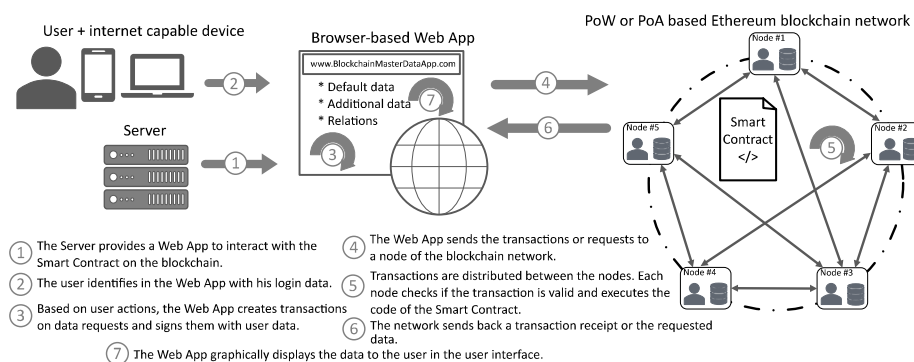


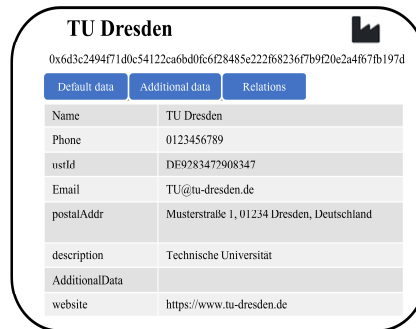
Fig. 1. Technical architecture and workflow of the MasterData application

Smart contracts were developed in *Solidity*. They contain data structures (organizational elements, data fields, data signatures) and functions (rights management, creation and deactivation of organizational elements, management of the respective master data, management of the relationships between the organizational elements and evaluation and signing of data attributes). The organizational elements, as the main data objects, represent the individual entities or business objects. They consist of the attributes *ID*, *owner/participants/rights*, *orgType* (e.g. corporation or product), *relationTypes*, and *dataKeys*. Data fields store attribute values for the appropriate data key. Besides, metadata relating to this value is stored in the specifically defined data structure. Participants in the blockchain network can digitally sign individual data attributes to increase the trustworthiness of data and confirm the signed data's validity. The executing user needs appropriate rights, both in the signing and in the signed element. When the signature is saved, some metadata is recorded to ensure quick verifiability, including *signingAddress*, *dataHash*, *signature* and *validFrom/validTo*.

We provide a brief overview of the smart contracts' functionalities to dive a bit deeper into the artifact's functionalities (the full source code can be obtained from the corresponding author). For each organizational element, there are three different roles, which are hierarchically structured. Each element has exactly one *owner*, but any number of *admins* and *participants*. So-called function modifiers can be used to specify which functions can be performed by which role. Two basic functions in the developed smart contracts are the creation and deactivation of organizational elements. A new

element can be created using the function 'newOrgElement()' and passing on a suitable ID and the desired element type. The sender of the calling transaction is defined as the owner. Data management can be handled via 'setData()' to create new data fields, 'removeData()' to remove fields or 'changeData()'. A relationship between elements can also be established via 'addRelation()'. Other functions include rating and signing data attributes via 'rateData()' and 'addSignature()'. The organizational elements are displayed in the frontend in the form of a simple business card. Fig. 2 shows an example of the authors' university business card, next to an excerpt of the smart contract.

```
function newOrgElement(bytes32 _id, uint256 _orgType)
public {
    orgElements[newId] = orgElement (
        _id,
        msg.sender,
        orgTypes[_orgType],
        new address[](0), //participants
        new bytes32[](0), //relatedIDs
        new bytes32[](0) //dataKeys
    );
}
```



TU Dresden	
0x6d3c2494f71d0c54122ca6bd0f6f28485c222f68236f7b9f20e2a4f67fb197d	
Default data Additional data Relations	
Name	TU Dresden
Phone	0123456789
ustId	DE9283472908347
Email	TU@tu-dresden.de
postalAddr	Musterstraße 1, 01234 Dresden, Deutschland
description	Technische Universität
AdditionalData	
website	https://www.tu-dresden.de

Fig. 2. Excerpt of the smart contract for creating a new organizational element (left) and exemplary representation of an organizational element (right)

4.2 Application Tests

Most of the potentials, risks, and limitations of BCT have only been studied qualitatively. The limited adoption in existing information systems impedes extensive empirical studies. Therefore, the developed artifact offers an opportunity to assess the scalability and economic feasibility of MDM based on BCT. With the Ethereum-based smart contracts, testing can be done in different test networks based on different consensus algorithms and allows for a statement about permissioned vs. permissionless network suitability. There is a growing debate about the criticality of network accessibility, which we aim to support through our quantitative analysis. The results allow stakeholders to assess the extent to which the blockchain solution can be implemented in a resource-efficient manner. We chose the permissioned test network of *evan.network* with PoA consensus (*Aura* on *Parity* nodes) using *Eve* as the integrated currency and the permissionless *Ropsten* test network of the Ethereum main net (imitating its behavior) with PoW consensus. The two networks were chosen for their popularity and comparability. Smart contracts in *Solidity* can be executed on both networks while ensuring reproducibility of results.

The node.js based script's flow is as follows (refer to Table 2 for the full list) and has been conducted in the same way in both test nets: The test is initialized with the required blockchain accounts being passed to the *web3js* object. Then, 50 organization elements are randomly created (similar to the element shown in Fig. 2) and given pseudo-data. Next, 30 participants are set up and 20 of them are granted admin rights. Then, some participants are removed and new owners are set for 20 of the organizational elements. Relations between the elements are created and finally, data attributes are changed,

rated and signed for 50 elements. This flow is intended to emulate real-world processes in collaborative MDM and allow the comparison of blockchain configurations.

4.3 Results

The results of the application tests are shown in Table 2. The computing operations in the Ethereum-based test networks are settled with a certain amount of *gas* (1 Gwei = 10^{-9} Ether/Eve). For each transaction, the gas consumption was recorded and converted in Ether/Eve and €. We also recorded the time in milliseconds (ms) for transaction execution. The gas price in the *Ropsten* network can be freely determined by the transaction's sender, influencing the execution time. The chosen gas price of 125 Gwei was the average gas price in the *Ropsten* network at the time of testing. The gas price in the *evan.network* is fixed at 20 Gwei, with each transaction treated equally. The fourth and the sixth column contain the converted costs per transaction in €.

Table 2. Results of the test runs in *evan.network* and *Ropsten*

Functions of the smart contract	Number of TX with function calls	gas consumption / time in ms	Ø cost per TX in €	gas consumption / time in ms	Ø cost per TX in €
		<i>evan.network</i>	<i>evan.network</i>	<i>Ropsten</i>	<i>Ropsten</i>
newOrgElement ()	50	6877532 / 3357	0,0028	6710794 / 94489	4,44
setData()	~ 450	86064055 / 35870	0,0038	83061475 / 323967	5,96
addParticipant()	30	3312161 / 2795	0,0022	3108329 / 12015	3,43
addAdmin()	20	1335070 / 2674	0,0013	1406242 / 49849	2,33
rmParticipant()	10	358120 / 2866	0,0007	355398 / 87890	1,18
rmAdmin()	10	677655 / 2805	0,00135	660575 / 35766	2,19
setOwner()	20	1790043 / 2866	0,0018	1556626 / 50380	2,58
addRelation()	50	50524099 / 3115	0,0035	8117831 / 182267	5,37
rmRelation()	25	1254523 / 2801	0,001	1250291 / 21264	1,65
changeData()	50	5707374 / 1538	0,0023	6392227 / 257651	4,23
rateData()	50	2099752 / 1820	0,00085	2143254 / 27573	1,42
addSignature()	50	6326825 / 1753	0,0025	6153900 / 351221	4,07
rmSignature()	25	729642 / 2296	0,0006	639293 / 45135	0,85

gas price for *evan.network* in Gwei: 20, eve price in €: 1 | gas price for *Ropsten* in Gwei: 125, Ether price in €: 264,71 | 1 Gwei = 10^{-9}

5 Discussion

It is evident from Table 2 that the permissioned *evan.network* with PoA consensus has significantly lower average execution times per gas, which means improved scalability compared to the *Ropsten* test network, which mimics the Ethereum mainnet. Besides, costs per transaction and smart contract deployments are considerably lower in *evan.network*. While there are arguments for a permissionless (and public) network like auditability and open accessibility to third parties, permissioned systems with consensus mechanisms other than PoW are more cost-effective and scalable for data-intensive MDM processes. Other risks in public and permissionless networks include the volatility of cryptocurrencies, which complicates reliable cost planning. Besides, as many other network partners are active in the public networks, there is no certainty regarding the costs and the execution times of transactions. It should still be emphasized that increased costs will be incurred compared to centralized solutions. There is also greater demand for initial alignment among network participants. Here, stakeholders need to balance the desired distribution of decision-making power, trust-less collaborative ef-

forts, and resource efficiency (costs) to decide on the suitability of a blockchain solution. BCT's strength is minimizing and automating underlying processes and providing higher data quality by avoiding isolated data silos.

Although BCT is particularly useful once the network reaches a certain size, for critical processes that require increased access security and traceability, there is added value even in small networks. It is reasonable to consider the proportion of data to be stored and shared via the blockchain in light of the high cost in permissionless networks compared to permissioned networks. Data creation and modification as the most critical functionalities should be handled off-chain and only referenced on-chain (e.g. hashed). To some extent, this consideration also applies to permissioned networks, as structured master data can be stored on-chain. In contrast, large-size unstructured master data can be referenced and handled off-chain.

We revisit the quality criteria of Sect. 2 to answer the first research question: On the *data accuracy* level, BCT supports the correctness and timeliness of data through the smart contract functionalities and the network-wide distribution of the ledger. Combined with the high failure and access security of blockchain systems, data completeness is ensured even in the event of technical failures. Signatures make it easy to trace changes and increase the trustworthiness of the system. *Data accessibility* is similar to a centralized database. Users can use standardized interfaces to retrieve data directly from the network. Editing data objects directly in the blockchain is costly due to the on-chain writing processes. However, blockchain systems provide increased access and failure security. Democratic processes limit flexibility. If new or changed requirements arise, adjustments cannot be enforced by a central instance. Besides, adaptations are limited concerning the “blockchain trilemma” of security vs. decentralization vs. scalability [26]. Permissioned networks perform well on security and scalability at a lower level of decentralization, whereas permissionless networks perform better on security and decentralization. Turning to *data representation*: The use of digital signatures and persistent transaction storage creates reliable metadata in blockchain systems. If rights are managed with the help of smart contracts, the scope and trustworthiness of this metadata can be increased even further. The integrity of the data is not based on a central authority but arises from the consensus-based trust. Redundancy is not limited but an inherent feature of blockchain, with inconsistencies largely eliminated by fast synchronization.

The technology also influences MDM. Blockchain enables secure, scalable and inter-organizational user management with consensus-based trust and increased transparency. Especially for new international business relationships, blockchain can offer an alternative to the DUNS standard [7]. However, firms can still decide which data to make accessible and manage critical business data off-chain. BCT can be a beneficial option for hybrid MDM configurations. Automatic archiving of records and transactions increases the security of the system. Data can also be exchanged with companies that were previously not trusted. However, further standards for collaborative MDM based on blockchain are needed to exploit the technology's potential fully. Besides, the interoperability of blockchain protocols needs to be improved. It must be noted here that the potentials, risks, and limitations depend on the blockchain's respective configurations. Examining these in detail is beyond the scope of this article.

6 Conclusion

We assess blockchain technology for cross-organizational master data management in this study. Design science research is conducted to develop a concept, which allows an economic evaluation of the technology's usability. This study addresses the need for focused studies on applying BCT in SCM while ensuring practical utility through the developed concept. Answering the research questions concisely, BCT can improve MDM in supply chains through its transparency features, promoting collaborative decentralization, enhanced security and automation potential through smart contracts. Important stakeholder decisions involve the choice of network type, the scope of data to be shared, and the user base. This article offers both quantitative and qualitative statements for these management decisions and provides insights on implications, chances and risks of using BCT for collaborative MDM in SCM.

Limitations of this study include the focus on a specific subarea of SCM. Thus, results for MDM cannot be easily generalized to other business domains, e.g. financial transactions. Further, the derived results of the DSR artifact are based on specific test networks and pseudo-data for transactions. Nevertheless, several implications can be derived from the results of this study. First, as a theoretical implication, the use of BCT for MDM may open a new research area in decentralized data storage and sharing. This study takes initial steps in this direction and can serve as a starting point for further studies to qualitatively and quantitatively assess the usability of the technology. Second, the findings indicate a technological fit of the technology and promising economic results regarding transaction costs. Besides, we substantiate previous qualitative statements with reliable numerical data and confirm the proposition that permissioned networks with PoA consensus are more scalable than permissionless networks.

Future research should include a more sophisticated proof-of-concept in a complex supply network to assess the application's technical fit and scalability for real-life processes. In the context of MDM, hybrid configurations using BCT are significant and should be assessed. Besides, exploring the concept of sidechains seems reasonable to facilitate solutions that combine the real decentralization of permissionless networks with the low costs and scalability of permissioned networks. Open issues also arise concerning the governance of supply chains and the trust-free implications of BCT. How do decentralized equality of partners and "code-is-law" features affect collaboration? A potential trend toward increased short-term business relationships and even more fragmented supply chains should be explored. Data sharing based on BCT also provides leeway for innovative solutions in supply chain finance or revenue sharing based on compensation for real-time data sharing by upstream partners [15].

References

1. Vanpoucke E, Boyer KK, Vereecke A (2009) Supply chain information flow strategies: An empirical taxonomy. *Int J Oper Prod Manag* 29:1213–1241.
2. Knolmayer GF, R othlin M (2006) Quality of material master data and its effect on the usefulness of distributed ERP systems. *Lect Notes Comput Sci* 4231 LNCS:362–371.
3. Vilminko-Heikkinen R, Pekkola S (2017) Master data management and its organizational

- implementation: An ethnographical study within the public sector. *J Enterp Inf Manag* 30:454–475. doi:10.1108/JEIM-07-2015-0070
4. Silvola R, Jaaskelainen O, Kropsu-Vehkapera H, Haapasalo H (2011) Managing one master data - Challenges and preconditions. *Ind Manag Data Syst* 111:146–162.
 5. Loshin D (2009) *Master Data Management*. Morgan Kaufman, Burlington, NJ
 6. Lohmer J, Lasch R (2020) Blockchain in operations management and manufacturing: Potential and barriers. *Comput Ind Eng* 149:106789. doi:10.1016/j.cie.2020.106789
 7. Banerjee A (2018) *Blockchain Technology: Supply Chain Insights from ERP*. In: *Advances in Computers*. Elsevier, pp 69–98
 8. Otto B, Hüner KM (2009) Functional reference architecture for corporate master data management
 9. White A, Radcliffe J (2007) *Four Dimensions of MDM: Understanding the Complexity*. Stanford, CT, USA
 10. Schemm J (2009) *Zwischenbetriebliches Stammdatenmanagement*. Springer Berlin Heidelberg, Berlin, Heidelberg. doi: 10.1007/978-3-540-89030-0
 11. Swan M (2015) *Blockchain: Blueprint for a New Economy*, 1st ed. O'Reilly Media, Sebastopol, CA
 12. Kurpjuweit S, Schmidt CG, Klöckner M, Wagner SM (2019) Blockchain in Additive Manufacturing and its Impact on Supply Chains. *J Bus Logist* 1–25.
 13. Babich V, Hilary G (2020) Distributed Ledgers and Operations: What Operations Management Researchers Should Know About Blockchain Technology. *Manuf Serv Oper Manag* 22:223–240. doi:10.1287/msom.2018.0752
 14. Jain G, Singh H, Chaturvedi KR, Rakesh S (2020) Blockchain in logistics industry: in fizza customer trust or not. *J Enterp Inf Manag* 33:541–558. doi:10.1108/JEIM-06-2018-0142
 15. Wang Z, Zheng Z, Jiang W, Tang S (2021) Blockchain-Enabled Data Sharing in Supply Chains: Model, Operationalization, and Tutorial. *Prod Oper Manag* 0:1–21.
 16. Casino F, Dasaklis TK, Patsakis C (2019) A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat Informatics* 36:55–81. doi:10.1016/j.tele.2018.11.006
 17. Lohmer J, Bugert N, Lasch R (2020) Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: An agent-based simulation study. *Int J Prod Econ* 228:107882. doi:10.1016/j.ijpe.2020.107882
 18. Kamble S, Gunasekaran A, Sharma R (2020) Modeling the blockchain enabled traceability in agriculture supply chain. *Int J Inf Manag* 52:1–16.
 19. Röck D, Sternberg HS, Hofmann E (2020) Distributed ledger technology in supply chains: a transaction cost perspective. *Int J Prod Res* 58:2124–2141.
 20. Wang Y, Singgih M, Wang J, Rit M (2019) Making sense of blockchain technology: How will it transform supply chains? *Int J Prod Econ* 211:221–236.
 21. Lohmer J, Ribeiro da Silva E, Lasch R (2021) Blockchain technology in operations & supply chain management: a content analysis. *Logistics Research* (forthcoming)
 22. Redman T (1996) *Data quality for the information age*. Artech House, Boston, MA
 23. Wang RY, Strong DM (1996) Beyond accuracy: What data quality means to data consumers. *J Manag Inf Syst* 12:5–34. doi:10.1080/07421222.1996.11518099
 24. Hevner AR, March ST, Park J, Ram S (2004) Design Science in Information Systems Research. *MIS Q* 28:75. doi:10.2307/25148625
 25. Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. *J Manag Inf Syst* 24:45–77.
 26. Zhou Q, Huang H, Zheng Z, Bian J (2020) Solutions to Scalability of Blockchain: a Survey. *IEEE Access* 8:16440–16455. doi:10.1109/ACCESS.2020.2967218