BLOCKCHAIN APPLICATION IN INFORMATION SYSTEMS RESEARCH

Inauguraldissertation

zur

Erlangung des Doktorgrades

der

Wirtschafts- und Sozialwissenschaftlichen Fakultät

der

Universität zu Köln

2020

Olga Labazova

M.Sc.

aus

Moskau, Russische Föderation

Referent: Prof. Dr. Claudia Loebbecke

Korreferent: Prof. Dr. Christoph Rosenkranz

Tag der Promotion: June 3rd, 2020

ACKNOWLEDGEMENTS

Without a Ph.D. scholarship (2016-2019) from the Cologne Graduate School in Management, Economics and Social Sciences of the University of Cologne this dissertation project would not be possible. I am grateful to the Department of Media and Technology Management and the Department of Information Systems and Systems Development for providing an excellent environment for doing scientific studies. The frequently conducted research seminars and feedback sessions motivate new perspectives, views, and solutions to broad research challenges.

I am extremely lucky that this project was supervised by Prof. Dr. Claudia Loebbecke and Prof. Dr. Christopher Rosenkranz. Both have proven to be constructive and trusted advisors. Besides, I could rely on a knowledgeable team of colleagues. Being part of the team for four years brings a tremendous positive shift in my personality and educational background.

I am greatly obliged to Prof. Dr. Ali Sunyaev for warmly inviting me for a nine-month research stay at the Karlsruhe Institute of Technology. Working together with the CII research group allows me to improve the computer science aspects of my research.

I am sincerely grateful to co-authors Prof. Dr. Tuure Tuunanen, Prof. Dr. Wolfgang Prinz, Prof. Dr. Ali Sunyaev, Dr. Tobias Dehling, Dr. Erol Kazan, Sandra Klein, and Wolfgang Gräther for supporting this research with their knowledge and expertise.

I have enjoyed plenty of discussions during seminars that were organized inside and in cooperation with the University of Cologne. Prof. Dr. Detlef Schoder, AR Dr. Dirk Basten, Jun.-Prof. Dr. Lea Ellwardt, Prof. Dr. Jan Mendling, Prof. Dr. Stefan Siegel, Prof. Dr. Roland Holten, and Prof. Dr. Nick Berente, Prof. Dr. Robert Winter introduced the most important aspects of the Information Systems research and theory during seminars at the University of Cologne, the University of Kassel, Karlsruhe Institute of Technology, and skiing seminars in Switzerland and Austria. Face-to-face sessions with Prof. Dr. Bob Briggs and Prof. Dr. Kale Lyytinen bring more theoretical meaning to this research.

I am pleased to be chosen to present this research at the IESS Doctoral Consortium 2019. I am grateful to Prof. Dr. Lia Patricio, Prof. Dr. Daniel Beverungen, Prof. Dr. Werner H. Kunz, Dr. Mohamed Zaki, Prof. Dr. Paul P. Maglio, and Hon.-Prof. Dr. Gerhard Satzger for helpful comments and suggestions.

I am thankful to editors and reviewers of the Journal of the Association for Information Systems, Business & Information Systems Engineering, and Electronic Markets for undergoing several rounds of revisions of this paper. Besides, I gladly appreciate the decision of the editors of Electronic Markets to kindly invite us to consider the journal as a potential publisher.

I am sincerely grateful to the chairs, reviewers and audience of the Future of Research Communications and e-Scholarship 2017, Hawaii International Conference on System Sciences 2019, and the International Conference on Information Systems 2019 for improving and accepting this paper for publication and organizing excellently in the conferences.

I would like to thank the organizers of the Blockchain Hackathon Bonn 2017, Digital Blockchain Workshop 2019 and the regular Cologne Blockchain workshops for exchanging research and practical knowledge in a friendly atmosphere.

I would like to thank the Mentoring Program for International Female Scholars of the University of Cologne and, specifically, Dr. Phuong Glaser for providing additional opportunities for international scholars to learn peculiarities of the German academic system. The Program effectively encourages women to pursue and advance careers in academia.

Finally, I am grateful to my family, my boyfriend, and my friends for being proud of my achievements and supporting me in periods of uncertainty.

Cologne, February 2020. Olga Labazova

ABSTRACT (English)

Blockchain is a radical innovation with a core value proposition of shifting trust from institutions towards algorithms. Still, the potential of Blockchains remains vague due to the knowledge gap between computer science and socio-economic activities. Ninety percent of current Blockchain projects did not move from ideas to production-ready prototypes. Researchers and practitioners are searching for the meaningful leveraging of Blockchains for value creation.

This dissertation aims to bridge the gap between technical and managerial knowledge of Blockchain that allows successful Blockchain system design and implementation. Therefore, the objective of the project is to identify the scope of Blockchain applications and introduce guidelines to make purposeful decisions of Blockchain implementations.

The dissertation project covers four research questions. First, I consolidated knowledge of Blockchain technical configurations through the development of a taxonomy. Second, I considered the design patterns of smart contracts that represent the application logic of Blockchain systems. Third, I offered guidance for transforming initial conceptions of Blockchain ideas into working system prototypes by introducing a Blockchain configuration process model. Fourth, I investigated the common factors of Blockchain decisions to evaluate Blockchain implementations in the form of the framework.

I employed a Design Science Research approach to developing four artefacts. The first three artefacts consider technical, application, and organizational aspects of Blockchain. The synergy reflects in the fourth, combinational artefact, which employs the high-level factors of Blockchain decisions. During the project, I have investigated the scientific and business studies, run Blockchain-based applications, conduct interviews, and evaluate the findings on Blockchain projects.

The dissertation project contributes to research by bridging knowledge gaps between computer science and socio-economic research on a Blockchain that provides a fruitful ground for future conceptual and empirical studies. For practitioners, the developed artefacts are useful to identify and guide Blockchain projects that facilitate purposeful Blockchain adoption.

Keywords: Blockchain, DLT, Design Science Research.

ABSTRAKT (Deutsch)

Blockchain ist eine radikale Innovation, deren zentraler Wert darin besteht, das Vertrauen von Institutionen zu Algorithmen zu verlagern. Dennoch bleibt das Potenzial von Blockchains aufgrund der Wissenslücke zwischen Informatik und sozioökonomischen Aktivitäten unbestimmt. Neunzig Prozent der aktuellen Blockchain-Projekte konnten nicht von Ideen zu serienreifen Prototypen übergehen. Forscher und Praktiker suchen nach einer sinnvollen Nutzung von Blockchains zur Wertschöpfung.

Dieses Dissertationsprojekt zielt darauf ab, die Lücke zwischen technischem und betriebswirtschaftlichem Wissen über Blockchain zu schließen, das einen erfolgreichen Entwurf und die Implementierung von Blockchain-Systemen ermöglicht. Ziel des Projekts ist es daher, den Umfang von Blockchain-Anwendungen zu ermitteln und Richtlinien einzuführen, um gezielte Entscheidungen für Blockchain-Implementierungen zu treffen.

Das Dissertationsprojekt umfasst vier Forschungsfragen. Zunächst vertiefe ich das Wissen über die technischen Konfigurationen der Blockchain durch die Entwicklung einer Taxonomie. Zweitens betrachte ich die Entwurfsmuster von intelligenten Verträgen, die die Anwendungslogik von Blockchain-Systemen darstellen. Drittens biete ich eine Anleitung für die Umwandlung erster Konzepte von Blockchain-Ideen in funktionierende Systemprototypen, indem ich ein Blockchain-Konfigurationsprozessmodell einführe. Viertens untersuche ich die gemeinsamen Faktoren von Blockchain-Entscheidungen, um Blockchain-Implementierungen in Form des Frameworks zu bewerten.

Ich verwende einen gestaltungswissenschaftlichen Forschungsansatz, um vier Artefakte zu entwickeln, mit denen technische Blockchain-Eigenschaften basierend auf bekannten Geschäftsanforderungen konfiguriert werden. Die ersten dre I Artefakte berücksichtigen die technischen, anwendungsbezogenen und organisatorischen Aspekte der Blockchain-Entwicklung und -Implementierung. Die Synergie spiegelt sich in dem vierten kombinatorischen Artefakt wider, das die Hauptfaktoren von Blockchain-Entscheidungen verwendet. Während des Projekts untersuche ich die wissenschaftlichen und betriebswirtschaftlichen Studien, führe Blockchain-basierte Anwendungen durch, führe Interviews durch und werte meine Ergebnisse zu Blockchain-Projekten aus.

Die Ergebnisse tragen zur Forschung bei, indem sie Wissenslücken zwischen Informatik und sozioökonomischer Blockchain-Forschung schließen, die eine fruchtbare Grundlage für zukünftige konzeptuelle und empirische Studien bietet. Für Praktiker sind die entwickelten Artefakte nützlich, um Blockchain-Projekte zu identifizieren und zu steuern, die eine zielgerichtete Blockchain-Übernahme ermöglichen.

Schlüsselwörter: Blockchain, DLT, gestaltungswissenschaftlicher Forschungsansatz.

PAPERS

Paper 1	Labazova, O., T. Dehling, A. Sunyaev. “From Hype to Reality: A Taxonomy of Blockchain Applications.” In: *52nd Hawaii International Conference on System Sciences (HICSS 2019)* (pp. 4555–4564). Waikoloa, Hawaii, USA (published).
Paper 2	Klein, S., Prinz W., Gräther W., Labazova O. “Smart Contract Design Patterns to Assist Blockchain Conceptualization.” In: *28th European Conference on Information Systems (ECIS 2020)*. Marrakech, Morocco (submitted, under review).
Paper 3	Labazova, O., Kazan E., Dehling T., Tuunanen T., Sunyaev A. “Managing Blockchain Systems and Applications: A Process Model for Blockchain Configurations.” *Electronic Markets* (revise & resubmit).
Paper 4	Labazova, O. “Towards a Framework for Evaluation of Blockchain Implementations.” In: *40th International Conference on Information Systems (ICIS 2019)* (pp. 1-16). Munich, Germany (published).

Contents

List of Abbreviations

Abbreviation	Explanation
ACM	The Association for Computing Machinery
AISeL	The Association for Information Systems Electronic Library
BTC	Bitcoin
DAO	Decentralized Autonomous Organization
DB	Deutsche Bahn
DLT	Distributed Ledger Technology
dSCM	Decentralized Supply Chain Management
DSR	Design Science Research
EBSCO	Elton B. Stephens Co.
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IBM	The International Business Machines
IEEE	The Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IOTA	Internet of Things Application
IP	The Internet Protocol
IS	Information Systems
IT	Information Technology
MB	megabyte
ORCID	Open Researcher and Contributor Identifier
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance
PoS	Proof of Stake
PoW	Proof of Work
RWTH Aachen	Rheinisch-Westfälische Technische Hochschule Aachen
SCM	Supply Chain Management
SWIFT	The Society for Worldwide Interbank Financial Telecommunication
tps	Transactions per Second
TTP	Trusted Third Party

List of Figures

List of Tables

1. Introduction

1.1. Motivation

Blockchain promises to be one of the top emerging technologies of this decade (Beck, Müller-Bloch and King, 2018). Blockchain meets the growing needs for private and secure information exchange in terms of increased integrity and availability by replacing conventional centralized information infrastructures with decentralization (Yli-Huumo et al., 2016). Blockchain requires no intermediaries since all communication processes are enforced through cryptographic proof instead of trust (Nakamoto, 2008). The immutability of stored data reduces the risks of information abuse. The multiple copies of the distributed database are consistently updated that allows us to have reliable access to data and decrease the number of errors (Glaser, 2017).

Blockchain was introduced as the Bitcoin Blockchain – an ongoing chain of the financial transactions between members of a decentralized peer-to-peer network (Nakamoto, 2008). Since then, Blockchain redefines processes, businesses, financial models, and enterprise architectures by relying on distributed networks of users. The cost of one innovative Blockchain initiative is estimated to be worth between $10 billion and $3.1 trillion by 2030 (Furlonger and Valdes, 2017).

The number and diversity of Blockchain investigations grow. Technical projects aim to develop new components (e.g., consensus mechanisms, cryptography) to increase advantages and overcome limitations of the Blockchain (Yli-Huumo et al., 2016). Blockchain applications expand from cryptocurrencies to energy trading (Albrecht et al., 2018), supply chain management (Mendling et al., 2017), authentication services (Miscione, Ziolkowski, Zavolokina and Schwabe, 2018), luxury products tracking (Loebbecke, Lueneborg and Niederle, 2018), health records (Azaria et al., 2016), and smart contracts (Watanabe et al., 2015). The legal, social, and economic effects of Blockchain are increasingly debated (Davidson, De Filippi and Potts, 2016).

1.2. Problem Statement

Despite the growing number of Blockchain research, the understanding of Blockchain possibilities is hard to obtain (Labazova, Dehling and Sunyaev, 2019). A division of the literature into independent research streams keeps extant knowledge on Blockchain separated (Risius and Spohrer, 2017). The technical research stream seldom looks at application cases beyond Bitcoin. The research on Blockchain applications is idea-driven and struggles due to a lack of ready-made technical solutions, implementation and management strategies, and industry and societal regulations (Risius and Spohrer, 2017).

Besides, the ongoing debates on the scope of Blockchain applications prevent the designation of general areas for Blockchain adoption. Some literature postulates that Blockchain is a revolutionary technology, which will perform the whole data processing (Tapscott and Tapscott, 2017). Other sources adhere to a modest view on Blockchain as a revolutionary technology, where application areas are restricted due to technological limitations (Swan, 2015a).

Therefore, Blockchain implementation remains risky because implementation costs and challenges can outweigh expected benefits (Yli-Huumo et al., 2016). Although investments in Blockchain projects have reached $1.5 billion during 2016 and continue to rise, the outcomes of Blockchain projects are often unpredictable. Due to a lack of best practices, Blockchain projects are more akin to experimentation than purposeful information system development projects (Beck and Müller-Bloch, 2017). As a result, ninety-two percent of the 26,000 Blockchain projects launched in 2016 are now defunct (Trujillo, Fromhart and Srinivas, 2017). Reasons for failure include inappropriate areas of Blockchain application and flawed system designs. For example, the Bank of Canada realized that their Blockchain-based system, developed in the multimillion-dollar Jasper project, is not suitable to handle settlements because the benefits of using Blockchain do not outweigh the risks (Risius and Spohrer, 2017).

To understand the true potential of Blockchain and account for its transactional nature, the integration of research on all relevant layers—technical, application, and ecosystem is required. The usefulness of Blockchains depends on the fit between Blockchain technology, application areas, and ecosystem conditions. Not all and diverging technical Blockchain configurations are suitable for different application-specific and industry-specific cases (Glaser, 2017). For example, Blockchain-based business process management only allows for private Blockchains because the intellectual property that creates competitive advantages should not be released to the general public (Salviotti, de Rossi and Abbatemarco, 2018).

1.3. Research Objective and Research Questions

In this dissertation project, I argue that purposeful Blockchain solutions will find a place for a limited number of application areas, but only if Blockchain implementations are soundly supported by the underlying Blockchain configurations. Therefore, the objective of the dissertation project is *to identify the scope of Blockchain applications and introduce guidelines to make purposeful decisions of Blockchain implementations*.

I have answered four research questions that correlate with corresponding papers. I started with consolidating knowledge of Blockchain in the form of a taxonomy. I have answered the first research question: *What application areas fit Blockchains with what technical characteristics?* The taxonomy of Blockchain applications was developed using the taxonomy development method by Nickerson, Varshney and Muntermann (2013). The taxonomy classifies Blockchain application cases by technical Blockchain characteristics. The taxonomy serves as a starting point for further investigations of Blockchain application possibilities.

Beck, Avital, Rossi and Thatcher (2017) formulated the need for more research about novel approaches to the development of Blockchain applications and suggest addressing the challenges of implementing business logic with smart contracts. Therefore, I continued with smart contracts, i.e. software code that represents the logic of Blockchain applications for the process automation (Christidis and Devetsikiotis, 2016), and their design patterns (Huang et al., 2017). I answered the second research question: *Which design patterns can be detected in smart contracts and how do these patterns interact with each other?* The structure of smart contract design patterns is based on the existing literature and the technical code. Further, the pattern language was created by consolidating relationships between patterns. The pattern language provides researchers and practitioners with a solid library for the development of reusable smart contracts.

Further, I offered guidelines for transforming initial Blockchain ideas into working system prototypes. A Blockchain configuration process model was introduced, which establishes relationships between application areas and technical Blockchain characteristics. I answered the third research question: *What application areas are advisable for Blockchain systems and how can Blockchain systems be purposefully configured across application cases?* The utility of the Blockchain configuration process was evaluated on four Blockchain projects, namely, DB System & IBM: Public Mobility, Lit Sonar, dSCM Tool, and Blockchain4openscience.org. The findings are useful to guide the development and design of Blockchain-based systems.

Blockchain design components and business outcomes differ from traditional technologies and business models because the infrastructure is decentralized and relies on peer-to-peer information exchange, the business value is collectively generated by nodes, and cooperation on intra- and inter-organizational levels are required to fully leverage the technology (Beck and Müller-Bloch, 2017). Therefore, I answered the fourth research question: *What are the common factors of Blockchain decisions to evaluate Blockchain implementations and how do these factors interconnect with each other?* The resulting factors are organized in a framework for evaluation of Blockchain implementations. The framework consists of four semantic categories: Blockchain innovation, Blockchain design, inter-organizational integration, and implementation environment.

Overall, the dissertation project contributes to the scientific literature by synthesizing and operationalizing previous research efforts and bridging the gap between technical and managerial studies. For practitioners, the developed artefacts are useful to identify and guide Blockchain projects that facilitate purposeful Blockchain adoption.

1.4. Structure of the Dissertation

The cumulative dissertation consists of the extended introduction and the papers included. I introduce the topic (section 1) with motivation (subsection 1.1), problem statement (subsection 1.2), the objective and research questions (subsection 1.3). Then, the theoretical background (section 2) gives an overview of the fundamental theories applied in the dissertation (subsection 2.1), basics of the Blockchain technology (subsection 2.2), and the importance of DSR in Blockchain research (subsection 2.3). This is followed by the DSR approach of the dissertation (section 3), including DSR contribution types (subsection 3.1), DSR cycles (subsection 3.2), and DSR methodology (subsection 3.3). Results recap the dissertation papers (section 4).

Sections 5, 6, 7, and 8 respectively comprise the following dissertation papers and corresponding tables with bibliographical information:

(1) Labazova, O., T. Dehling, A. Sunyaev. “From Hype to Reality: A Taxonomy of Blockchain Applications.” In: *52nd Hawaii International Conference on System Sciences (HICSS 2019)* (pp. 4555–4564). Waikoloa, Hawaii, USA (published);

(2) Klein, S., Prinz W., Gräther W., Labazova O. “Smart Contract Design Patterns to Assist Blockchain Conceptualization.” In: *28th European Conference on Information Systems (ECIS 2020)*. Marrakech, Morocco (submitted, under review);

(3) Labazova, O., Kazan E., Dehling T., Tuunanen T., Sunyaev A. “Managing Blockchain Systems and Applications: A Process Model for Blockchain Configurations.” *Electronic Markets* (revise & resubmit);

(4) Labazova, O. “Towards a Framework for Evaluation of Blockchain Implementations.” In: *40th International Conference on Information Systems (ICIS 2019)* (pp. 1-16). Munich, Germany (published).

The discussion (section 9) covers principal findings (section 9.1), theoretical contribution (section 9.2), practical implications (section 9.3), limitations of this dissertation (section 9.4), and possibilities for future research (section 9.5). I conclude the dissertation project with a summary (section 10).

I preserve consistency with font styles and sizes aligned. Figures and tables are continuously numbered. A uniform citation style is applied, and all references are consolidated at the end of the dissertation. All abbreviations, figures, and tables are listed at the beginning of this dissertation.

2. Theoretical Background

2.1. Fundamental Theories

2.1.1. IT/Blockchain Governance

IT (Information Technology) governance is defined as decision rights and accountabilities to encourage desirable behavior in the use of IT (Brown and Grant, 2005). Decision rights represent the governing control over assets. Accountabilities capture the monitoring of decision-making processes. Incentives motivate agents to act according to the purposes of systems (Brown and Grant, 2005).

The literature discusses three basic types of IT governance (Brown and Magill, 1994; Schwarz and Hirschheim, 2003). First, centralized governance includes executive committees for decision making, centralized business processes and architectures, and formal post-implementation assessments and monitoring of decisions. Centralized governance is applied by the most profitable companies that are centralized in their strategies of efficient operations, encourages a high degree of standardization, and pursuits a low business cost. Second, decentralized approaches to IT governance require few governance mechanisms of decision-making and insists on local accountability. Innovative and developing companies apply decentralized approaches to IT governance to follow local customer needs and minimize constraints on creativity and business unit autonomy by establishing few standardizations of processes and products. Third, companies that aim to balance the benefits of centralized and decentralized models follow a hybrid governance approach. The companies establish a centralized group to provide core services while allowing business units to control a portion of the overall function (Boynton and Zmud, 1987; Rockart, 1988).

To be initially introduced as a decentralized database, Blockchain evolves with the different approaches to Blockchain governance. Beck et al. (2018) specify decision rights as a degree of Blockchain centralization whether decision-making power is concentrated in governing node(s) or distributed equally among nodes in the Blockchain network. Accountability differs in rights to monitor decisions on Blockchains and address actions taken, and consequences incurred (Beck et al., 2018). Different incentives motivate agents to act on the purpose of Blockchains for monetary or non-monetary rewards.

The most successful Blockchains will be those who adopt their governance to the organizational environment (Kharitonov, 2017). Blockchain governance types should further determine technical Blockchain configurations, for example, consensus mechanisms and anonymity approaches.

2.1.2. Theory of Co-Evolution of (Blockchain) Technologies and Applications

Extant theory of the coevolution of technologies and applications during industry emergence focuses on the mechanism of continuous coevolution of technological designs and application areas (Grodal, Gotsopoulos and Suarez, 2015). The process starts with a period of divergence and continues with a period of convergence. The period of divergence is characterized by high diversity in attempted technological designs to address emerging application requirements. Technological designs evolve and fulfill more application requirements through design recombination. Application areas are influenced by ready-made technological designs, which satisfy groups of application requirements. Application areas related to abandoned technological designs are also abandoned. The following period of convergence results in consensus among producers for effective technological designs and mature application areas.

The Blockchain domain is currently at an early stage of industry emergence and is characterized by application and technology over determinism (Beinke, Nguyer and Teuteberg, 2018). A diversity in attributes of Blockchain execution, such as consensus mechanisms (Karame et al., 2015) or anonymity approaches (Reid and Harrigan, 2013), produces experimental technological designs (Yli-Huumo et al., 2016). The number of Blockchain application cases increasingly grows leading to different Blockchain-based services. However, Blockchain application cases are not fully supported by ready-made technological solutions (Risius and Spohrer, 2017).

The process of the Blockchain industry emergence cannot be fast. Through specification, structuring, and refinement of technology-related and application-related Blockchain concepts and exploration of their relationships, technological designs and application areas will be further delineated, to reach maturation of the Blockchain domain.

2.2. Blockchain Foundations

2.2.1. The Process of Blockchain Functioning

Blockchain is a transparent, global, and openly-accessible asset ledger that keeps a history of transactions between members of a decentralized peer-to-peer network (Nakamoto, 2008). Blockchain is represented by data blocks linked through a cryptographic algorithm in chronological order. The Blockchain contains all transactions which have been executed, shared, and approved by participating parties that guarantee integrity in a public infrastructure running by untrustworthy nodes (Lin and Liao, 2017).

Consequently, the Blockchain is generally based on a peer-to-peer (P2P) network in terms of its typological structure and distribution. The principle of a P2P network is that the users of this network provide the required resources, such as computing power or storage space, as well as use them from other participants (Schollmeier, 2001). The stored transactions are automatically synchronized between all nodes, eliminating the need for a central node to process and distribute data. Three consecutive steps process transactions on Blockchain: creation, validation, and confirmation (Figure 1).

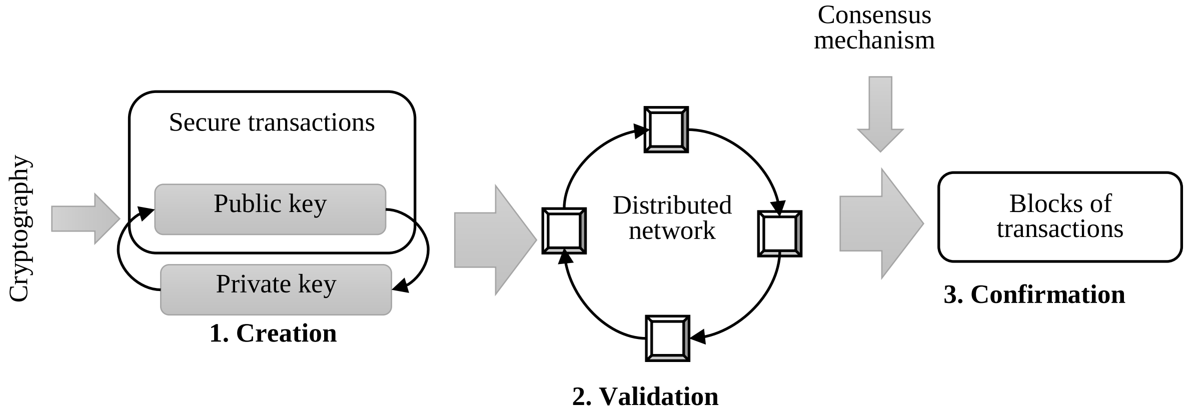

Figure 1. The Process of Blockchain Functioning

2.2.1.1. <u>Creation</u>

All nodes in the network can create a transaction. A transaction includes information on any action with data (Beck et al., 2016). Each transaction is cryptographically secured using the signature of the creating node. Then the transaction is added to the transaction block following the creation time interval.

A transaction block is mainly composed of two parts, a block header and a block body. The block header consists of a timestamp to prove that the data exists at that time (Nakamoto, 2008), a hash value of the previous block, a version number for protocol updates, block size, and several transactions (Khan and Salah, 2018). A block body contains transaction data to be verified and a nonce (Nakamoto, 2008). Transition data represents value, sender and receiver accounts. A nonce is a variable to guarantee the validity of the hash value et al., 2017).

Cryptography calculates a unique hash value of a particular block. This value must meet predefined criteria (e.g., the Bitcoin value begins with 0). Each block has the hash value of its predecessor. Therefore, no block can be changed without changing the hash values of its successors because all changed successors would lose their validity (Singh and Singh, 2016).

2.2.1.2. <u>Validation</u>

The signed block of transactions is sent to another block in the network for validation. The transaction in a block is valid if the reference to the previous block is unused. Transactions are broadcasted through the network of nodes and validated by other nodes until the transaction reaches all nodes in the network. Each node tries to solve a puzzle to create the right nonce. The first node which succeeds adds a timestamp to the block and distributes it through the network. For each block, a unique hash code is generated, which is then incorporated into the next block, building the references between blocks and tying the blocks together into a chain (Nakamoto, 2008). All spread transactions within a certain time interval are ordered and packaged into a timestamped candidate block.

The mining process is used to determine the nonce, calculate the hash value, and apply the new block to the Blockchain. This process is carried out by special nodes, which are called miners or validators. Miners provide the computing power for transaction processing, validation, and data synchronization.

2.2.1.3. <u>Confirmation</u>

All valid transactions are aggregated into blocks to be added to a chain. Once data is entered, the information can never be erased (Lin and Liao, 2017).

For nodes to agree on the transactions, a consensus mechanism is needed (Christidis and Devetsikiotis, 2016). Various consensus mechanisms (e.g., proof of work, proof of stake) are proposed (Ziolkowski, Miscione and Schwabe, 2018). Consensuses use elements of the game theory to reward miners who spend resources to secure a block. Usually, the first miner who finds the hash and attaches the block to the Blockchain gets the reward. Consensus guarantees that any action of the agent corresponds to the current state of the local repositories of all the agents. When consensus is found, the transactions are confirmed and become immutable as the next block.

2.2.2. Blockchain Typology

Blockchain was introduced by Satoshi Nakamoto in 2008 as the Bitcoin Blockchain - a common transparent, global, and openly-accessible asset ledger that keeps the history of financial transactions between members of a decentralized peer-to-peer network (Nakamoto, 2008). Over time, other Blockchain types emerged that differ in approaches to Blockchain governance. Blockchain governance can be distinguished into the rights to read data from the Blockchain and write information to the Blockchain (Table 1).

Reading access can be public or private (Beck et al., 2018). Public reading access gives no restrictions; any node can read transactions. Private reading access allows only a predefined list of users to access Blockchain data (Walsh et al., 2016). Nodes need to be registered with a centralized authority to enter the network (Beck et al., 2018).

Writing access implies permissionless and permissioned restrictions. Permissionless access gives no limitations for nodes regarding transaction processing. Any node in the network can create transactions and participate in the consensus mechanism. Permissioned access limits writing rights to a certain user group (Walsh et al., 2016). Only nodes that have been authorized can interact with the Blockchain and participate in the data transfer and block creation processes (Labazova et al., 2019).

Table 1. Blockchain Typology (Beck et al., 2018, p. 1022)

Reading / Writing	**Public**	**Private**
Permissionless	All nodes can read, submit, and validate transactions.	Not applicable.
Permissioned	All nodes can read and submit transactions. Only authorized nodes can validate transactions.	Only authorized nodes can read, submit, and validate transactions.

Blockchain types differ in combinations of permissions to read and write information on the Blockchain. Public permissionless Blockchains are fully decentralized Blockchains. Everyone can read, write, and validate the information. The consensus is enforced by proof-of-work or proof-of-stake. Users are usually anonymous and pseudonymous. The examples are cryptocurrencies, where participants do not have to trust each other but the Blockchain itself (Nakamoto, 2008).

Public permissioned Blockchains are more centralized Blockchains. Only authenticated and pre-defined users can read and write transactions. However, all nodes participate in consensus finding. Identifiable nodes determine consensus mechanisms. Organizations consortia (e.g., Ripple) are examples of public permissioned Blockchains, where pre-defined nodes in the network are trustful organizations and deal directly with each other to support a peer-to-peer transaction exchange (Walsh et al., 2016).

Private permissioned Blockchains are fully centralized Blockchains. Access authorization does not entail validation permissions, which require additional authorization rights given to several nodes. Consensus (e.g., practical Byzantine fault tolerance) is enforced by trustful nodes. A private Blockchain is managed by one single institution. These Blockchains are especially attractive for organizations like the government, which is not in the position to reduce control.

Private permissionless Blockchains are not applicable. Applications are not identified (Beck et al., 2018).

2.2.3. Types of Consensus Mechanisms

Consensus mechanisms are concerned with employed means for updating Blockchains. Reaching consensus is one of the central elements of the Blockchain. The three mature consensus mechanisms are proof of work, proof of stake, and practical Byzantine fault tolerance (Labazova et al., 2019).

2.2.3.1. <u>Proof of Work</u>

Proof-of-Work (PoW) requires some resources (or work) from a requester, usually the processing time of a computer to solve a computationally difficult puzzle (Salviotti et al., 2018). PoW applies in Bitcoin and since then was used in other configurations. PoW utilizes a fixed-size hash function to create the conditions that allow a participant to disclose conclusions about the information puzzles. The conclusions are independently verified by other participants in the network (Salviotti et al., 2018).

PoW is a random process with many trials and errors before a valid PoW is created (Salviotti et al., 2018). Therefore, PoW is secure until the majority of the network (51%) acts honestly, without criminal intentions.

2.2.3.2. <u>Proof of Stake</u>

Proof-of-Stake (PoS) asks users to prove the ownership of a certain amount of digital data to establish their stake in this data (Labazova et al., 2019). PoS is an alternative to PoW, where mining is performed by stakeholders, who have a financial interest in Blockchain. Proof-of-Stake replaces the mining process by measuring the amount of currency or stake of the node. The larger the stake, the more probability exists to be the validator of the next block.

However, the nothing-at-stake problem exists. Because of the low probability to validate the next block, no-stake nodes make forks of Blockchains.

2.2.3.3. <u>Practical Byzantine Fault Tolerance</u>

Practical Byzantine fault tolerance (PBFT) gathers individual decisions made by trusted nodes in a network that together determine system-level agreements (Labazova et al., 2019). PBFT starts with a user who sends a transaction to the network. The request is multiplied to different network participants, each of those executes the request and sends it back to the starting user. The results are accepted when a specified amount of replies (e.g., 1/3) is identical.

The algorithm works securely until more than 1/3 of the participants act honestly. The only requirements are that the network participants must operate deterministically and start from the same base.

2.2.4. Smart Contracts

Smart contracts were firstly mentioned by Nick Szabo in 1997 as a possibility to implement clauses of a contract into hardware and software to penalize a fraudulent party (Szabo, 1997). Smart contracts are automatically executable programs that make decisions when certain conditions are met (Morabito, 2017). Smart contracts guarantee that the rights and obligations of a contract are executed as written and that malicious actions are prevented. The automation of the contract execution reduces transaction costs and removes the necessity of a third party (Yuan et al., 2018).

Smart contracts increase the Blockchain potential by implementing business logic (Khan and Salah, 2018). That resulted in the introduction of decentralized applications and laid the foundation for second-generation Blockchains (Hawlitschek, Notheisen and Teubner, 2018). With smart contracts, Blockchain can be used to automate complex business processes (e.g., recruiting) (Christidis and Devetsikiotis, 2016).

Once a smart contract is programmed, it is uploaded into the Blockchain. As transactions, smart contracts are usually broadcasted to the network and verified by other nodes (Yuan et al., 2018).

The actions that are triggered by smart contracts are transparent. Therefore, the participants can audit inputs, outputs, and current states of the contracts. However, once a smart contract lends Blockchain, it is immutable. That rises difficulties in dealing with programming errors and deadlocks (Christidis and Devetsikiotis, 2016).

The network participants, other smart contracts, or the outside actions invoke smart contracts' triggers (Beck et al., 2016). When the smart contract gets triggered, it automatically executes the appropriate transactions and fulfills the contract without the need for a third party (Yuan et al., 2018). In the case of outside triggering, oracles are used to collect the necessary data and put it on the Blockchain (Lamberti et al., 2018). Moreover, oracles can also be used to send information that is generated by smart contracts outside of the Blockchain (Lamberti et al., 2018).

2.2.5. Technical Advantages and Limitations of Blockchain

2.2.5.1. <u>Blockchain Technical Advantages</u>

Blockchain incorporates several technical improvements compared to other technologies including increased availability through decentralization, the possibility to achieve trust in a trustless network, and increased data integrity that provides an auditable historicization of data changes.

Availability measures the probability of a system being accessed when needed (Xu et al., 2017). In Blockchain systems, availability is offered through data replication across decentralized nodes (Wüst and Gervais, 2018). Therefore, the probability that every node is shut off and the data is gone decreases. In centralized systems, availability is generally achieved through replication on different physical servers and backups, which is a more expensive solution (Wüst and Gervais, 2018).

Data integrity ascertains that the whole Blockchain starting with a genesis block is kept and distributed between hosts. The data integrity allows to audit the validity and immutability of an entire history of transactions that are consistent between many nodes in a global network. Blockchains use complex data structures (e.g. Merkle trees) to store all transactions in a way that the current state of the system depends on all previous transactions (Glaser, 2017). The manipulation of the historical transactions by a malicious node results in invalid states of the system. Therefore, other nodes in the network ignore the malicious node. The immutability of the Blockchain ensures that once the transaction is verified by the network and added into a block, this transaction cannot be altered (Wang, Luo and Xue, 2018). This makes Blockchain technology suitable to record critical information (Kuo, Kim and Ohno-Machado, 2017).

Blockchain can initiate trust in a trustless network (Nakamoto, 2008). Shifting the trust from a central managing point (e.g., banks) to democratized Blockchain networks is suitable for projects like sharing economies where there is no control in the network. Additionally, smart contracts can establish policies on the Blockchain.

2.2.5.2. <u>Blockchain Technical Limitations</u>

Scalability, security and privacy, and transaction costs are identified as the main technological challenges of the Blockchain. Scalability determines the capacity of Blockchain is changed in size or scale. It combines such characteristics as throughput, latency, and size and bandwidth (Yli-Huumo et al., 2016). Throughput represents the number of transactions that can be successfully delivered over the network. The throughput of the Bitcoin Blockchain is up to 7tps (transactions per second) versus VISA (2,000tps) and Twitter (5,000tps). Latency describes the duration required for the block generation (Walsh et al., 2016). The latency is around 1 hour (10-minute block interval with 6-block confirmation) on Bitcoin and around 3 minutes (14-second block interval with 12-block confirmation) on Ethereum. For Bitcoin, transactions have a size between 0.1 and 5 BTC. The number of transactions included in each block is limited by the bandwidth of nodes. For Bitcoin, the bandwidth per block is 1MB.

Security and privacy are separate issues. Blockchains have a possibility of a 51% attack where a single entity can manipulate the whole network. Several attacks on the Bitcoin network have already resulted in high cryptocurrency losses (Yli-Huumo et al., 2016). Other risks like the theft of private keys for authentication are also possible. Besides, all transactions are transparent and announced to the public. Despite the public can see all transactions without linking transactions to identities, the pseudonymity of users can be trackable (Nakamoto, 2008). Some linking is not avoidable in the Bitcoin network, because multi-input transactions reveal that their inputs were held by the same owner. The risk for privacy emerges when the owner of one public key is revealed, as linking could result in exposing other transactions that belong to the user (Lischke and Fabian, 2016).

The process of a transaction confirmation wastes a huge amount of resources (e.g., $15 million per day for Bitcoin). Besides, Blockchain requires additional transaction costs for nodes to be rewarded for the processing of transactions. Therefore, the value of the transactions should be higher than the resources wasted to overcome the expenses (Yli-Huumo et al., 2016). The transaction costs are represented by tokens. To be transmitted into the real value, the consideration of the volatility of tokens is required because the token markets change fast and dramatically.

2.3. Design Science Research in the Blockchain Domain

DSR guides developing IT artefacts and their use in practice. The usual DSR process considers technology as innovation, design, organizational integration, and implementation environment (Hevner, March, Park and Ram, 2004). Blockchain is itself an inter-organizational technology, though one could argue that it is a useful technology for a single organization when there are conflicting objectives or game-theoretic situations where trust is not guaranteed, and a single version of the truth is beneficial.

In the last years, interest in Blockchain moved far beyond Bitcoin. The financial sector and other industries investigate Blockchain proofs-of-concept prototypes. The need for understanding of how to evaluate Blockchain projects starts to gain momentum. However, the Blockchain domain is lacking clear rules to guide the design and adoption of Blockchains

(Glaser, 2017; Beck and Müller-Bloch, 2017). Therefore, the importance of DSR in the Blockchain domain is increasingly highlighted in the scientific literature (Beck et al., 2016; Naerland, Müller-Bloch, Beck and Palmund, 2017). The three types of DSR artefacts in the Blockchain domain can be distinguished: (1) Blockchain classifications, (2) Blockchain-based system prototypes, and (3) guiding frameworks.

2.3.1. Blockchain Taxonomies and Topologies

The role of taxonomies is well recognized in IS research. Glass and Vessey (1995) noted that taxonomies structure and organize the knowledge of a field, thus enabling researchers to study the concepts and hypothesize about their relationships.

DSR firstly arises in the Blockchain domain in the form of taxonomies, topologies, and other classifications that structure, connect and diversify Blockchain archetypes, Blockchain design components, and related concepts (e.g., smart contracts). The discussion opened Glaser and Bezzenberger (2015), who postulate that the technical protocols and implementations of technologies in the field of distributed ledgers and other consensus systems are quite complex. Therefore, the authors developed a comprehensive taxonomy of decentralized consensus systems. The taxonomy provides a tool for researchers and practitioners to facilitate classification and analysis of emerging technologies in the field of "Crypto 2.0", the next level of innovation beyond cryptocurrencies.

In contrast, Walsh et al. (2016) focused explicitly on the Blockchain. The author reviewed the Blockchain literature and identified eight key design characteristics of Blockchains: permission restrictions, restricted public access to data, investment weighting for transaction consensus, chain modularity, scalability, interoperability, centralized regulation, and anonymity. From these characteristics, four Blockchain archetypes emerged with similarities and differences across the archetypes.

Xu et al. (2017), extended the key design characteristics by comparing different Blockchain design components. The authors proposed how to classify and compare Blockchains to assist with the design and assessment of their impact on software architectures. The developed taxonomy captures major architectural characteristics of Blockchains grouped by principal design decisions including cost efficiency, performance, and failure points.

Concerning other similar classifications, Kazan, Tan and Lim (2015), Brenig, Schwarz and Rückeshäuser (2016), and Seebacher (2018) focused on developing Blockchain business network ontologies, which formalize the concepts and properties of a Blockchain network (Oliveira et al., 2018) explored Blockchain tokens in the form of a taxonomy. The authors brought insights into the representation of tokens and their connection to the underlying business models. Further, Diniz, Siqueira and Van Heck (2016) and Fridgen et al. (2018) proposed classifications for understanding community currencies and Blockchain-enabled forms of crowdfunding.

2.3.2. Blockchain System Prototypes

Blockchain is still in its technological infancy. Experimental adoption and customization seem to be in full progress in various potential fields of application ranging from decentralized grids for computation and storage to global financial services. The financial sector is most experimenting with Blockchain. Beck et al. (2016) developed a Blockchain solution for financial transactions that can replace trust-based coffee shop payments. Elsman, Egelund-mu, Henglein and Ross (2017) explored an automatic execution of Blockchain-based financial contracts using formal languages of smart contracts. Fridgen, Radszuwill, Urbach and Utz (2018) conducted a case study for cross-organizational workflow management in a German bank that runs on Blockchains. Wang et al. (2018) aimed to reduce costs of know-your-customer verification processes, which are around USD 500 million per year per bank. Further, the authors aimed to revolutionize loyalty programs with Blockchain by keeping customers motivated in participation behaviors and achieving financial goals.

In the public sector, Beck et al. (2018) investigated a new form of organizational design—decentralized autonomous organizations (DAO). DAO are organizations with governance rules specified in the Blockchain. The authors discussed Blockchain governance among dimensions of IT governance, specifically, decision rights, accountability, and incentives. Hyvärinen, Risius and Friis (2017) examined Blockchain prototypes, which can overcome the double taxation of investors on dividend payment and move land records from paper to Blockchain. Azaria et al. (2016) developed a prototype for managing medical records on Blockchains. Zhang, Sharma and Wingreen (2018) improved precision healthcare with Blockchain. Kuo et al. (2017) proposed to audit the healthcare value chain to improve patient outcomes.

For the energy sector, Albrecht et al. (2018), Lacity (2018), and Mengelkamp et al. (2018) discussed an approach for Blockchain-based processing of charging payment transactions and proved the technical feasibility of validating and storing charging-related data and processing payment transactions with Blockchain. Kirpes and Becker (2018) investigated Blockchain implementation in an electric vehicle and their further integration into the smart power grid. A Blockchain-based mechanism was proposed to manage battery swapping and solve the trust lacking issue.

In logistics and supply chain management, Naerland et al. (2017) proposed to reduce high transactional uncertainty and risk by introducing certainty into economic transactions with Blockchains. The authors developed a prototype to turn central documents in shipping (e.g., the Bill of Lading) into smart contracts on Blockchains in collaboration with Maersk. Loebbecke et al. (2018) discussed the automated transaction of real-world assets such as diamonds with Blockchain proofs-of-concept. Notheisen, Cholewa and Shanmugam (2017) proposed to trade Real-World Assets on Blockchain and discussed an Application of Trust-Free Transaction Systems in the Market for Lemons.

For social businesses, Ciriello, Beck and Thatcher (2018) considered Blockchain as a basic technology of crowdlending platforms. Schweizer et al. (2017) continued with a discussion about the paradoxical effects of Blockchain technology on social networking practices. The author designed, developed, and evaluated a Blockchain-based crowdlending platform of social business. Maher (2018) proposed to improve IoT trust models with Blockchain. The author considered Blockchain as a tool, which supports a minimal set of human-centric trust management capabilities in IoT.

2.3.3. Blockchain Implementation Guidelines

The interest in Blockchain provoked the need to develop convincing system designs together with implementation guidelines (Fridgen et al., 2018). Therefore, artefacts for the development and integration of Blockchain systems emerged. The artefacts focus on multiple layers of Blockchain implementations and their surroundings.

Glaser (2017) raised the question of how Blockchain could amend the existing landscape of digital services, processes, and infrastructures. The author developed an ontology that delineates common terminology, core concepts, and components, their relationships as well as innovative features of Blockchain technology. These insights are further connected with implications for relevant types of digital market models. Based on Glaser (2017), Notheisen et al. (2017) proposed a Blockchain market engineering framework, which supports in analyzing and designing the elements of Blockchain-based markets on an individual and global level. The Blockchain market engineering approach introduces elements of Blockchain-based platforms and surrounding factors (e.g., legal, social and economic constraints) that are a basic macro layer for the infrastructure layer. The infrastructure layer implements the Blockchain protocol that specifies the basic elements of Blockchain system designs including distributed database, consensus mechanism, and cryptographic protocol. The infrastructure layer, in its turn, influences the application logic of implementations and is the foundation of the microeconomic design.

Considering Blockchain as a (distributed) database, Wüst and Gervais (2017) critically analyzed permissionless and permissioned Blockchains and contrasted their properties to those of a centrally managed database. The authors provided a structured methodology to determine the appropriate technical solution to solve a particular application problem. The methodology includes six questions: (1) Do you need to store state? (2) Are there multiple writers? (3) Can you use an always online TTP? (4) Are all writers known? (5) Are all writers trusted? (6) Is public verifiability required? Further, B. Pedersen, Risius and Beck (2019) extended the findings and presented a ten-step decision path that can help determine whether the application of Blockchain is justified and, if so, which kind of Blockchain technology to use (public vs. private, permissionless vs. permissioned). The authors described how this decision path was used to develop a Blockchain prototype for the Danish maritime shipping industry. The questions of the path include: (1) Need for a shared common database? (2) Multiple parties involved? (3) Do involved parties have conflicting interests/trust issues? (4) Parties can/want to avoid a trusted third party? (5) Rules governing system access differ between participants? (6) Transacting rules remain largely unchanged? (7) Need for an objective immutable log? (8) Need for public access? (9) Are transactions public? (10) Where is consensus determined?

To study organizational and managerial challenges, Beck and Müller-Bloch (2017) analyzed how an incumbent bank deals with the radical innovation of Blockchain. The authors developed a framework illustrating how the process of discovering, incubating, and accelerating with Blockchain can look like. The research sheds light on the organizational challenges of companies as they engage with Blockchain. Further, Lacity (2018) described the strategies that LO3 Energy, Moog, Inc. and the Center for Supply Chain Studies are pursuing to address managerial challenges in the areas of solutions, standards, regulations, shared governance, and viable ecosystem. The authors investigated enterprise adoption journeys from initial business visions, the proposed Blockchain-enabled solutions, proofs-of-concept, and plans to deploy solutions into production. Based on that information, five main questions were distinguished that should be asked before initiating Blockchain projects: (1) Is a Blockchain the right solution? (2) How are Blockchain standards being established? (3) How can a Blockchain solution comply with legislation given the regulatory uncertainty? (4) How should a Blockchain solution be governed? (5) How can a viable ecosystem be established?

3. Design Science Research Approach

The overall dissertation project follows a design science research (DSR) approach. DSR is a relevant research method for this dissertation because, besides the understanding of how things are, I aim to develop artefacts that are useful for mitigating problems of researchers and practitioners.

In contrast to the natural sciences that are concerned with the current states of the phenomena, DSR is focused on the development and implementation of artefacts to attain certain goals (Hevner et al., 2004; Peffers et al., 2008). The development of an entirely new artefact should be relevant to the domain of interest and grounded in the previous knowledge base, while the design and evaluation of the solution should iteratively happen. In the dissertation project, I achieved relevance with investigating requirements to Blockchain implementations and rigor with knowledge of Blockchain theories, best practice of real-world Blockchain implementations, and IT artefacts in the Blockchain domain.

3.1. Design Science Research Contribution Types

DSR is based on the problem-solving paradigm. Therefore, DSR aims to create an artefact that is innovative, useful and generic for the application environment (Hevner et al., 2004).

DSR artefacts can be in different forms. March and Smith (1995) distinguished between constructs, models, methods, and instantiations. Constructs represent groups of vocabulary and symbols. Models are abstractions of reality. Methods show algorithms and practices. Instantiations are considered as implementations and prototypes. Further, Gregor and Hevner (2013) argued that abstract contributions (e.g., design theories, design principles, technical rules) should be considered as artefacts as well.

The artefacts vary from more specific, limited and less mature knowledge about a domain of interest to more abstract, complete and mature knowledge of the phenomena (Gregor and Hevner, 2013). Therefore, Gregor and Hevner (2013) allocated three levels of DSR contribution types (Table 2). Situated implementations of artefact (e.g., software products or implemented processes) are considered as the first level of DSR contribution. Nascent design theories, which represent knowledge as operational principles or architecture (e.g., constructs, methods, models, design principles, and technological rules) are at the second level of DSR contribution and are more abstract and complete. Well-developed design theories (e.g., mid-range and grand design theories) report the most abstract, complete and mature knowledge (Gregor and Hevner, 2013).

Table 2. DSR Contribution Types (Gregor and Hevner, 2013, p. 342)

	Contribution Types	**Examples**
More abst**ract complete and mature knowledge**	Level 3. Well-developed design theories about embedded phenomena	Mid-range and grand Design Theories
	Level 2. Nascent design theories–knowledge as operational principles or architecture	Constructs, frameworks, methods, models, design principles, technological rules, taxonomies
More specific, limited, and less mature knowledge	Level 1. Situated implementations of artefacts	Instantiations (software products or implemented processes)

The artefacts that are developed in this dissertation belong to the second level of design theory (i.e., a taxonomy, a model, a framework, and design patterns), but consider different angles (i.e., technical, application, organizational, and their combinations). First, I defined the taxonomy of Blockchain applications to organize knowledge of Blockchain (Nickerson et al., 2013). As taxonomies stress the aspect of reuse, they belong to reference models, methods, or ultimately to every artefact that is designed in a design-oriented research process (Winter, Gericke and Bucher, 2009).

Second, I looked at Blockchain 2.0 – Blockchain as decentralized applications – to develop design patterns of smart contracts. Baskerville and Pries-Heje (2010) classify patterns as an explanatory design theory that is defined as a general design solution to a class of problems that relates a set of general components to a set of general requirements.

Third, I developed a process-model to assist with developing Blockchain prototypes. The Blockchain configuration process-model assists with the configuration of Blockchain systems and supports the selection of Blockchain attributes based on a set of known business requirements (i.e., Blockchain governance, Blockchain application area). The model also belongs to nascent design theories.

Finally, I introduced the framework for the evaluation of Blockchain implementations, which uses the requirements of enterprise projects as an input and provides users with an assessment of the Blockchain readiness of their enterprise Blockchain projects as an output. The framework does so by guiding the user through four steps and, therefore, also belongs to the second type of DSR contribution. Overall, the developed artefacts present the Blockchain knowledge contribution that embodies the insights on how best to understand and position Blockchain in the implementation environment.

3.2. Design Science Research Cycles

Hevner (2007) introduced DSR as an embodiment of three closely related cycles of activities: the relevance cycle, the rigor cycle, and the design cycle (Figure 2). The recognition of these three cycles positions and differentiates DSR from other research paradigms.

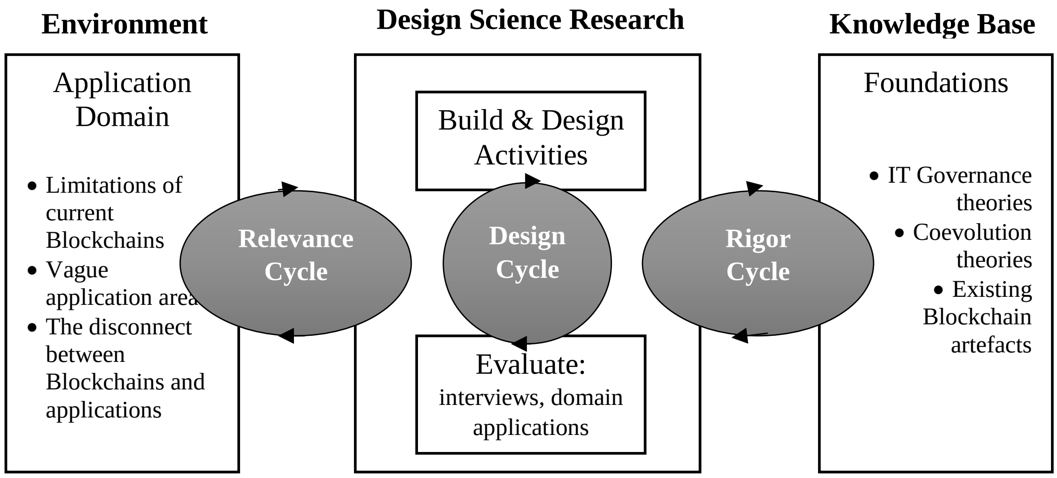

Figure 2. DSR Research Cycle (Hevner, 2007, p. 2)

3.2.1. The Relevance Cycle

The Relevance Cycle bridges the contextual environment with design activities. The relevance cycle gathers requirements of the application environment to the design artefact and introduces the current states of the field testing. The cycle motivates artefact development and introduces the acceptance criteria as environment improvements (Hevner, 2007). The criteria of the relevance cycle include people, organizational systems, and technical systems that are interacting to achieve certain goals. Besides, the relevance cycle identifies challenges and opportunities for the implementation environment.

To get the data for the solution of the problem, this dissertation project utilized scientific literature, business sources, and qualitative interviews. For the scientific and business literature, I have used all sources that have keywords Blockchain, distributed ledger or smart contracts depending on associated research questions. The interviews followed the semi-structured principle, in which predetermined questions were asked. In doing so, I gathered, summarized, and classified the common requirements from the literature and practice to the Blockchain phenomenon.

3.2.2. The Rigor Cycle

Design science is based on a broad knowledge base of theories and methods to follow the rigor of DSR. The rigor cycle connects design science activities with the knowledge base of scientific foundations, experience, and expertise that inform the design artefact. Vice versa, the cycle returns the newly generated knowledge to the knowledge base.

The knowledge can be two types: (1) the experiences and expertise of the state-of-the-art in the domain and (2) the existing artefacts and processes of the application domain. The rigor cycle provides past knowledge of the research project to ensure its innovation. Research rigor in design science is predicated on the researcher's skilled selection and application of the appropriate theories and methods for constructing and evaluating the artefact.

As a rigor cycle, the artefacts of the dissertation are based on both, experiences and expertise as well as existing artefacts. For the development of artefact, I have utilized theories of IT and Blockchain governance and the theory of co-evolution of technologies and applications. I analyzed the existing knowledge base of Blockchain as well as based the artefacts on related artefacts in the Blockchain domain that include, at least, Blockchain taxonomies and topologies, Blockchain system prototypes, and Blockchain implementation guidelines.

3.2.3. The Design Cycle

The design cycle iterates between the core activities of building and evaluating the design artefacts and processes of the research (Hevner, 2007). It is the main part of design science research. The iterations between the construction and evaluation provide feedback for the design refinements. Hevner (2007) described the nature of this cycle as generating design alternatives and evaluating the alternatives against requirements until a satisfactory design is achieved. Both activities must be convincingly based on relevance and rigor. The requirements are input from the relevance cycle, while the design and evaluation theories and methods enter from the rigor cycle. During the performance of the design cycle, it is important to maintain a balance between the efforts spent in constructing and evaluating the evolving design artefact (Beck and Müller-Bloch, 2017).

To evaluate the results, I have conducted semi-structured expert interviews. Besides this, the feedback was by demonstrating versions of artefacts on the scientific conferences, consortiums, and other thematic events with the Blockchain-friendly audience. Besides, the applicability of the artefacts was ensured by applying them back to the application domains.

3.3. Design Science Research Methodology

Peffers et al. (2007) introduced a methodology for information systems research that comprises six steps: problem identification, objective definition, design and development, demonstration, evaluation, and communication. All six steps should be performed iteratively; however, evaluation puts a special emphasis on iterative nature (Hevner, 2007).

Pries-Heje, Baskerville and Venable (2008) highlighted the importance of both ex-ante and ex-post evaluations. Ex-ante evaluation happens before the artefact is constructed. Ex-post evaluation is performed after the development of the artefact. Sonnenberg and vom Brocke (2012) went further and proposed the iterations of evaluation after each DSR activity, which together comprises two ex-ante two ex-post evaluations. To strengthen the quality of the artefact, the dissertation project utilized DSR methodology for information systems research (Figure 3) (Peffers et al., 2007).

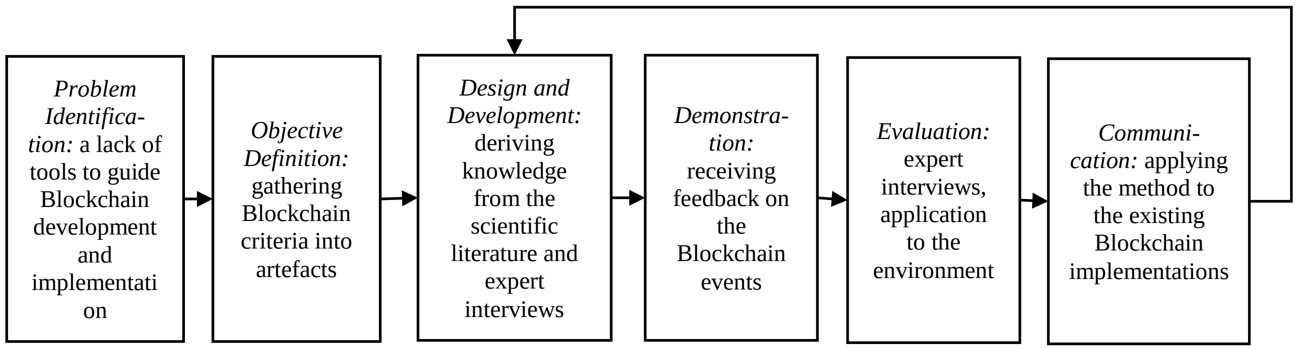

Figure 3. The Dissertation Research Methodology (Peffers et al., 2007, p. 93)

3.3.1. Problem Identification

The Blockchain domain is at an early stage of development and is concerned with a lack of defined tools to guide Blockchain system development and integration in industries and markets (Glaser, 2017; Beck and Müller-Bloch, 2017). I departed from an instance problem that emerges from a running Blockchain project where the stakeholders must take a decision on whether they need Blockchain and, if so, how the solution should be designed and implemented. The main problems result in misunderstandings of the core purposes of Blockchains, mismatches between Blockchain design components, failures in interoperability with existing IT solutions, and confusion regarding future visions of technology.

3.3.2. Objective Definition

To explore the potential use of the artefacts, experts were being asked whether solutions are needed. Moreover, I systematically attended the thematic Blockchain events (e.g., conferences, meetups) for four years to come up with the objectives of the solutions.

The objectives were as follows. First, knowledge of Blockchain configurations was consolidated through the development of a taxonomy. Second, the design patterns of smart contracts were considered that represent the application logic of Blockchain systems. Third, I offered guidance for transforming initial conceptions of Blockchain ideas into working system prototypes by introducing a Blockchain configuration process model. Fourth, I have looked into the common factors of Blockchain decisions to evaluate Blockchain implementations in the form of a framework.

3.3.3. Design and Development

I iteratively designed and refined the solutions depending on the incoming data from the rigor and relevance of Blockchain knowledge and feedbacks after evaluations (Hevner, 2007). First, I collected data by conducting a literature review of the scientific sources to uncover Blockchain knowledge in previous research on Blockchain (Webster and Watson, 2002). I searched for peer-reviewed research on Blockchain and related topics (e.g., distributed ledger) to identify important aspects of Blockchains. I searched articles in the top information systems journals (Schrader and Hennig-Thurau, 2009) with the search string ("Blockchain" OR "distributed ledger") in title, abstract, and keywords, covering the whole period of publications. I have only considered journal articles published in English. I read the abstracts of the resulted articles. After the screening process, I performed a backward search.

Second, the conduction of open-ended, semi-structured interviews with leading researchers, solution architects, or leading developers who engaged with Blockchain took place. The interviews were transcribed and coded using NVivo software. During the interviews, interviewees discussed Blockchain concepts and their relationships according to their Blockchain project. Besides, I used secondary data sources (e.g., scientific articles) to triangulate data and understand the relationships between Blockchain concepts and actual usage.

For data analysis, open coding is applied first for the initial categorization of Blockchain concepts and then axial coding for removal of overlapping concepts while iteratively testing the concepts against data (Strauss and Corbin, 1990). If available, I also coded the theoretical foundations that were used to delineate and structure interconnections between criteria. Next, I aggregated the criteria in broader categories that were derived from the analysis and counted the number of papers and expert statements on Blockchain. Interconnections between concepts were identified based on the semantic influence of one concept on another found in the scientific texts from the literature review and the interview transcripts. Interconnections reported in scientific texts and interviews were coded along with descriptive information, such as the text excerpts from which interconnections were derived. I coded the sources several times during four years of the dissertation project and the arising papers in between for the initial coding and validation of the results (Strauss and Corbin, 1990). Disputes were resolved in discussions.

Finally, the data went into the artefacts. The groups of the concepts in the artefacts arisen in semantic similarities and architecture of the related artefacts in the Blockchain (or other) domains (Glaser, 2017).

3.3.4. Demonstration

I demonstrated versions of the solutions on the scientific conferences, consortiums, and other thematic events with a Blockchain-friendly audience.

3.3.5. Evaluation

To evaluate the results, semi-structured expert interviews are conducted. I searched for experts in different fields including computer science, finance, and social science because the results cover broad aspects of Blockchains. Interviews were held face-to-face, via Skype and telephone.

The interview guide was used. I initially discussed with interviewees the criteria suitable for Blockchain. Then, the first versions of the developed artefacts were shown. The interviewers consequently discussed the proposed artefact. I followed the interviewers with questions. The interviews were transcribed and coded using NVivo software.

After the artefacts' revisions, I asked for the phone or the writing feedback from the same experts. All experts provided additional feedback.

3.3.6. Communication

I communicated the applicability of the developed artefacts back to the knowledge base. The existing Blockchain implementations were selected to demonstrate the applicability of the artefacts. I have done so because the artefacts are generalized abstractions and should apply to any Blockchain implementation.

4. Papers of the Dissertation

In this dissertation project, I have argued that successful Blockchain solutions will find a place for a limited number of application areas, but only if Blockchain implementations are soundly supported by the underlying Blockchain configurations. Therefore, the objective of the project is to identify the scope of Blockchain applications and introduce guidelines to make purposeful decisions of Blockchain implementations.

The dissertation project covers four research questions that correlate with corresponding papers (Table 3). First, I consolidated my knowledge of Blockchain technical configurations through the development of a taxonomy. Second, the design patterns of smart contracts were considered that represent the application logic of Blockchain systems. Third, I offered guidance for transforming initial conceptions of Blockchain ideas into working system prototypes by introducing a Blockchain configuration process model. Fourth, the investigation of the common factors of Blockchain decisions was conducted to evaluate Blockchain implementations in the form of the framework.

Table 3. Overview of the Papers of the Dissertation

№	Outlet	Authors	Status	Title
1	52nd Hawaii International Conference on System Sciences, 2019	Labazova, Dehling, Sunyaev	Published	From Hype to Reality: A Taxonomy of Blockchain Applications
2	28th European Conference on Information Systems, 2020	Klein, Prinz, Gräther, Labazova	Under Review	Smart Contract Design Patterns to Assist Blockchain Conceptualization
3	Electronic Markets	Labazova, Kazan, Dehling, Tuunanen, Sunyaev	Revise & Resubmit	Managing Blockchain Systems and Applications: A Process Model for Blockchain Configurations
4	40th International Conference on Information Systems, 2019	Labazova	Published	Towards a Framework for Evaluation of Blockchain Implementations

4.1. From Hype to Reality: A Taxonomy of Blockchain Applications.

This paper consolidates knowledge on Blockchain technical configurations through the development of taxonomy using the taxonomy development method by Nickerson et al. (2013). I answered the first research question of the dissertation: *What application areas fit Blockchains with what technical characteristics?*

A taxonomy is systematically developed based on extant literature, business reports and previous Blockchain classifications. The taxonomy is defined as a set of dimensions (Nickerson et al., 2013). Each dimension consists of mutually exclusive and collectively exhaustive characteristics in a way that each object under consideration has one and only one characteristic in every dimension (Nickerson et al., 2013). To analyze the sources, I have employed three types of coding: open coding, axial coding, and selective coding (Strauss and Corbin, 1990).

The developed taxonomy consists of eight dimensions with twenty-one technical characteristics and six application areas with twenty-five application cases. The technical dimensions include reading access, writing access, main consensus mechanism, anonymity level, event handling, data exchange type, encryption, and history retention. The application areas comprise financial transactions, smart contracts, data management, storage, communication, and ranking. The utility of the taxonomy is demonstrated in ninety-nine Blockchain-based systems.

The paper contributes to the scientific literature by delimiting Blockchain application areas, identifying new technical dimensions, and linking application and technical knowledge on Blockchain to guide the development of Blockchain-based systems. For practitioners, an overview of current Blockchain-based systems is presented.

This paper is published in proceedings of the 52nd Hawaii International Conference on System Sciences, 2019. The three authors contributed to the paper. Olga Labazova is a doctoral fellow at Cologne Graduate School in Management, Economics and Social Sciences, University of Cologne, Germany. Tobias Dehling is a postdoctoral researcher at the Institute of Applied Informatics and Formal Description Methods of the Karlsruhe Institute of Technology, Germany. Ali Sunyaev is a professor of Information Systems at the Institute of Applied Informatics and Formal Description Methods of the Karlsruhe Institute of Technology, Germany.

4.2. Smart Contract Design Patterns to Assist Blockchain Conceptualization

The paper aims to provide researchers and practitioners with a solid baseline for the development of reusable smart contract libraries. I answered the second research question: *Which design patterns can be detected in smart contracts embedded in Blockchain applications and how they interconnect with each other?*

To describe the patterns, a list of structural elements has been identified. A total of 16 smart contract design patterns has been defined by analyzing existing smart contract implementations. Further, a pattern language was created by revealing and visualizing relationships between the individual patterns to support the methodological development of new Blockchain applications.

Twelve smart contract design patterns include pattern name, classification, summary, problem, solution, participants, consequences, Blockchain characteristics, graphical representation, variations, application examples, are references to other patterns. The pattern language examines and summarizes the relationships between smart contract design patterns.

I contribute to the scientific literature by connecting the concept of smart contracts and Blockchains. A comprehensive list of design patterns and a pattern language is created to show dependencies between smart contract design patterns. For practitioners, the smart contract design patterns can function as a common vocabulary. Also, standardization in Blockchain development is enabled by providing a catalog of smart contracts’ functionalities.

The paper is submitted and accepted for review at the 28th European Conference on Information Systems, 2020. There are four contributing authors. Sandra Klein is an employee of the Fraunhofer Institute for Applied Information Technology, Germany, and a master's student at the University of Cologne, Germany. Wolfgang Prinz is a professor and a vice-chair of the Fraunhofer Institute for Applied Information Technology, Germany, and a professor at the RWTH Aachen University, Germany. Wolfgang Gräther is an employee of the Fraunhofer Institute for Applied Information Technology. Olga Labazova is a doctoral fellow at Cologne Graduate School in Management, Economics and Social Sciences, University of Cologne, Germany.

4.3. Managing Blockchain Systems and Applications: A Process Model for Blockchain Configurations

This paper develops a Blockchain configuration process model that captures Blockchain capability dimensions and its application areas. I answered the third research question: *What application areas are advisable for Blockchain systems and how can Blockchain systems be purposefully configured across application cases?*

I started with allocating Blockchain applications with mutually exclusive technical characteristics together with their relationships (Nickerson et al., 2013). Further, the findings are consolidated in the form of the Blockchain configuration process model. I demonstrated the applicability of the proposed model on four Blockchain projects, namely, DB Systel & IBM: Public Mobility, LitSonar, dSCM Tool, and Blockchain4openscience.org.

The model is based on IT governance literature and the theory of the coevolution of technologies and applications. The model assists with the configuration of Blockchain systems and supports the selection of Blockchain attributes based on a set of known business requirements (i.e., Blockchain governance, Blockchain application area).

By establishing relationships between Blockchain and application areas, the Blockchain configuration process captures knowledge useful to guide projects of integrating Blockchain-based systems into the inter-and intra-organizational landscape. The findings inform empirical research on Blockchain measurements and performance indicators. For practical audiences, the findings are useful to guide the development and design of Blockchain-based systems, in which application requirements are aligned with Blockchain configurations.

The paper underwent two rounds of Business and Information Systems Engineering Journal and two rounds of the Journal of the Association for Information Systems. Finally, the paper received an invitation to be submitted to the Electronic Markets journal. After a round of reviews, the paper received a revise and resubmit.

There are five contribution authors. Olga Labazova is a doctoral fellow at Cologne Graduate School in Management, Economics and Social Sciences, University of Cologne, Germany. Dr. Erol Kazan is a postdoctoral researcher at the Faculty of Information Technology, University of Jyväskylä, Finland. Tobias Dehling is a postdoctoral researcher at the Institute of Applied Informatics and Formal Description Methods of the Karlsruhe Institute of Technology, Germany. Prof. Dr. Tuure Tuunanen is a professor of Information Systems, University of Jyväskylä, Finland. Ali Sunyaev is a professor of Information Systems at the Institute of Applied Informatics and Formal Description Methods of the Karlsruhe Institute of Technology, Germany.

4.4. Towards a Framework for Evaluation of Blockchain Implementations

The paper takes the first step towards a framework for the evaluation of Blockchain implementations. I answered the fourth research question: *What are the common factors of Blockchain decisions to evaluate Blockchain implementations and how do these factors interconnect with each other?*

This study follows a DSR approach (Peffers et al., 2007). For data collection, the scientific literature and expert interviews are used that help us to arrive at a set of Blockchain decision factors. I have evaluated the developed framework by interviewing experts and showcasing the applicability of the framework on the Brooklyn Microgrid project (Lacity, 2018; Mengelkamp et al., 2018). I demonstrated the developed framework during the scientific conferences, consortiums, and other thematic events with a Blockchain-friendly audience.

Based on IT artefacts in the Blockchain domain, the resulting factors of Blockchain decisions are organized in a framework for the evaluation of Blockchain implementations. The framework uses the requirements of the implementations as an input to provide users with an evaluation of Blockchain implementations as an output. The framework does so by guiding the user through four steps: Blockchain innovation, Blockchain design, inter-organizational integration, and implementation environment.

I contribute to the scientific literature by structuring previous research efforts in a four-step framework, which provides a fruitful ground for future conceptual and empirical studies. For practitioners, the framework is useful to identify Blockchain projects that facilitate purposeful Blockchain adoption.

This paper is published in the 40th International Conference on Information Systems, 2019. The contributing author is Olga Labazova, a doctoral fellow at Cologne Graduate School in Management, Economics and Social Sciences, University of Cologne, Germany.

5. From Hype to Reality: A Taxonomy of Blockchain Applications

Table 4. Bibliographical Information for Paper 1	
Title	From Hype to Reality: A Taxonomy of Blockchain Applications
Authors	(1) Olga Labazova, University of Cologne (2) Tobias Dehling, Karlsruhe Institute of Technology (3) Ali Sunyaev, Karlsruhe Institute of Technology
Outlet	Hawaii International Conference on System Sciences
Publication Type	Conference Proceedings
Publication Year	2019
VHB-JOURQUAL3	C
Publication Status	Published

Abstract. Blockchain is a decentralized digital ledger that challenges existing business models and theories by shifting the trust from institutions towards algorithms. However, the number of successfully developed Blockchain-based systems remains low. This points towards a research gap between Blockchain applications and technical Blockchain characteristics. We answer the research question: What application areas fit Blockchains with what technical characteristics? We develop a taxonomy, which comprises six Blockchain application areas that are classified across eight technical dimensions. We demonstrate the utility of the taxonomy on ninety-nine Blockchain-based systems. We contribute to the scientific literature by delimiting Blockchain application areas, identifying new technical dimensions, and linking application and technical knowledge on Blockchain to guide the development of Blockchain-based systems. For practitioners, we present an overview of current Blockchain-based systems.

5.1. Introduction

A Blockchain is a decentralized digital ledger (Friedlmaier, Tumasjan and Welpe, 2018) with the unique value proposition to shift the trust from institutions towards algorithms (Nakamoto, 2008). The future impact of Blockchains on existing business models and theories might be comparable to the invention of smartphones or the internet (Pongnumkul, Siripanpornchana and Thajchayapong, 2017; Beck and Müller-Bloch, 2017; Constantinides, Henfridsson and Parker, 2018; Welpe, Zavolokina, Krcmar and Mehrwald, 2020). Therefore, researchers and practitioners jump on the Blockchain bandwagon (Avital et al., 2016; Beck and Müller-Bloch, 2017) in attempts to replace established trust-based business models with Blockchains (The Economist, 2015; Friedlmaier et al., 2018). The hype emerging around Blockchains suggests that Blockchains can replace banks in the financial sector (Nakamoto, 2008; The Economist, 2015), support agreements among individuals or internet-of-things devices using smart contracts (Higgins, 2015; Pureswaran, Panikkar, Nair and Brody, 2015), and manage essential records (e.g., health records, education records) that are currently maintained by centralized organizations (Azaria et al., 2016; Sharples and Domingue, 2016).

Yet, the challenges of developing Blockchain-based systems outweigh envisioned benefits (Yli-Huumo et al., 2016). Most of the current Blockchain projects could not move from ideas to production use (Furlonger and Valdes, 2017). For example, projects aimed at employing Blockchains to support tokenization of space missions (e.g., Space BIT) or artificial intelligence (Swan, 2015b) did not reveal proofs of concept. Narrow-scoped Blockchain prototypes experience issues with the scalability of Blockchain protocols, waste of computational resources required for consensus mechanisms, traceability of users, and a lack of network protection against fraud (Swan, 2015a; Fabian, Ermakova and Sander, 2016; Yli-Huumo et al., 2016; Xu et al., 2017). Currently, practitioners continue experimenting with proofs of concept and system designs based on trial-and-error approaches (Furlonger and Valdes, 2017).

Extant research in the Blockchain domain is focused on the development of Blockchain-based systems and the diversity of technical components (e.g., consensus mechanisms, permissions) and applications (e.g., financial transactions, the internet of things). A closer examination of extant research reveals the diversity of Blockchain application areas with no-size-fits-all technical Blockchain characteristics (Walsh et al., 2016; Xu et al., 2017; Kannengießer et al., 2019). For example, the Bitcoin network is untrusted and requires a secure proof-of-work consensus mechanism (Nakamoto, 2008) while a Hyperledger business network ensures trust and can employ lighter consensus mechanisms, such as practical Byzantine fault tolerance (Hyperledger Architecture Working Group, 2017). The relevant technical Blockchain characteristics, however, remain abstract, fragmented, and scattered across applications.

More knowledge connecting technical Blockchain characteristics and Blockchain applications is crucial to provide the guidelines on the development of successful Blockchain-based systems. Trial-and-error development leads to unfulfilled expectations in Blockchain-based systems and loss of investments. Therefore, we answered the research question "*What application areas fit Blockchains with what technical characteristics"?*

Taxonomies are used to organize knowledge in many fields (e.g., Darwin's classification of species in biology) (Bloom, 2001; Darwin, 2009; Schneider, Lansing, Gao and Sunyaev, 2014; Mrosek, Dehling and Sunyaev, 2015). We chose a taxonomy as the fundamental tool to organize knowledge on Blockchains (Nickerson et al., 2013). We developed a taxonomy of Blockchain applications, which captures six Blockchain application areas that are classified across eight technical dimensions (Nickerson et al., 2013). The taxonomy is based on extant scientific literature, business reports, and previous Blockchain classifications. We demonstrated the utility of the taxonomy by classifying ninety-nine Blockchain-based systems (Wörner, Von Bomhard, Schreier and Bilgeri, 2016; Friedlmaier et al., 2018). Extant Blockchain taxonomies and other classifications describe Blockchains from either technical or application perspectives (Glaser and Bezzenberger, 2015; Walsh et al., 2016; Böhm et al., 2017; Xu et al., 2017). Our taxonomy is different because it integrates technical and application knowledge that allows guiding the development of Blockchain-based systems.

This research contributes to the scientific knowledge base in three ways. First, we established an overview of extant research on Blockchain application areas. Second, we identified new technical dimensions of importance to Blockchain applications, which complement extant work in the technical literature. Third, we linked Blockchain application areas and technical Blockchain characteristics, which can guide the development of Blockchain-based systems. For practitioners, the taxonomy gives an overview of successful Blockchain applications that can reduce development challenges for future Blockchain-based systems.

This paper proceeds as follows. We started with related research on Blockchain. Next, we outlined the approach employed for taxonomy development. Then, we presented the taxonomy of Blockchain applications and demonstrated its utility on ninety-nine Blockchain applications. Finally, we discussed principal findings, future research, limitations of our study, and implications for theory and practice.

5.2. Related Research

The scientific literature on the Blockchain is at an early development stage. An absence of guidelines on the development of Blockchain-based systems hinders successful Blockchain projects. Extant Blockchain taxonomies and other classifications consider technical Blockchain characteristics and Blockchain application areas separately. Technical Blockchain classifications are focused on the diversity of technical components (e.g., permissions to read transactions, consensus mechanisms) and cover predominantly the financial sector (Kazan, Tan and Lim, 2014; Morisse, 2015; Tschorsch and Scheuermann, 2016; Wörner et al., 2016; Yli-Huumo et al., 2016). For instance, a study comparing digital payment providers identifies permissions to read and write financial transactions as important technical characteristics to consider when choosing between centralized and decentralized payment platforms (Kazan et al., 2014). Centralized payment platforms give permissions on reading and writing financial transactions to authorized users; decentralized payment platforms do not require user authorization to read and write financial transactions. A review of cryptocurrencies investigates different consensus mechanisms, levels of anonymity, and data integrity among cryptocurrencies (Morisse, 2015). Different consensus mechanisms (e.g., proof-of-stake, practical Byzantine fault tolerance) are determined to be suitable to improve the efficiency of second-generation cryptocurrencies (Tschorsch and Scheuermann, 2016; Yli-Huumo et al., 2016). Compared to Bitcoin, Zero coin guarantees stronger anonymity of users that prevents user traceability (Ziegeldorf et al., 2015) and Lite coin has lower data integrity that allows for support of devices with low storage capacity (e.g., mobile phones) (Gibbs and Yordchim, 2014). Further overviews of key technical characteristics of Blockchains gather previous findings in the financial sector including reading and writing permissions of transactions, consensus mechanisms, anonymity levels, and other technical characteristics that are not focused on Blockchain design but rather on interoperability (e.g., chain modularity) (Glaser and Bezzenberger, 2015; Walsh et al., 2016; Xu et al., 2017).

Investigations of Blockchain application areas start with the idea that Blockchains can be useful beyond the financial sector. Extant research focuses predominantly on applying Blockchains for digital payments, certification, cloud storage, identity management, energy distribution, and advanced tracking (Salviotti et al., 2018). Business reviews of Blockchain startups reveal new application areas including customer loyalty, cybersecurity, digital rights management, digital voting and government, gaming, content distribution, platform development, prediction markets, and smart contracts (Friedlmaier et al., 2018; Salviotti et al., 2018).

Isolated knowledge of technical and application research causes hypes of Blockchain application areas and technical Blockchain characteristics. Further consideration and consolidation of application and technical knowledge on Blockchains will result in a foundational classification of Blockchain application areas in alignment with technical Blockchain characteristics and provide the first steps to guide the development of successful Blockchain-based systems.

5.3. Research Approach

To organize knowledge on Blockchains, we used the method for taxonomy development proposed by Nickerson et al., who define a taxonomy as a set of dimensions (Nickerson et al., 2013). Each dimension consists of “mutually exclusive and collectively exhaustive characteristics in a way that each object under consideration has one and only one” (Nickerson et al., 2013, p. 5) characteristic in every dimension. The taxonomy development method proceeds in three stages (Figure 4). In the initial stage, metacharacteristics and ending conditions are defined according to the purposes of the taxonomy to be developed. In the main stage, the taxonomy is developed. Taxonomy objects (here application cases), dimensions, and characteristics are identified during inductive or deductive iterations. In inductive iterations, empirical cases are analyzed to determine dimensions and characteristics in the taxonomy. In deductive iterations, dimensions and characteristics are derived from the scientific knowledge base. In the final stage, the taxonomy is evaluated against ending conditions.

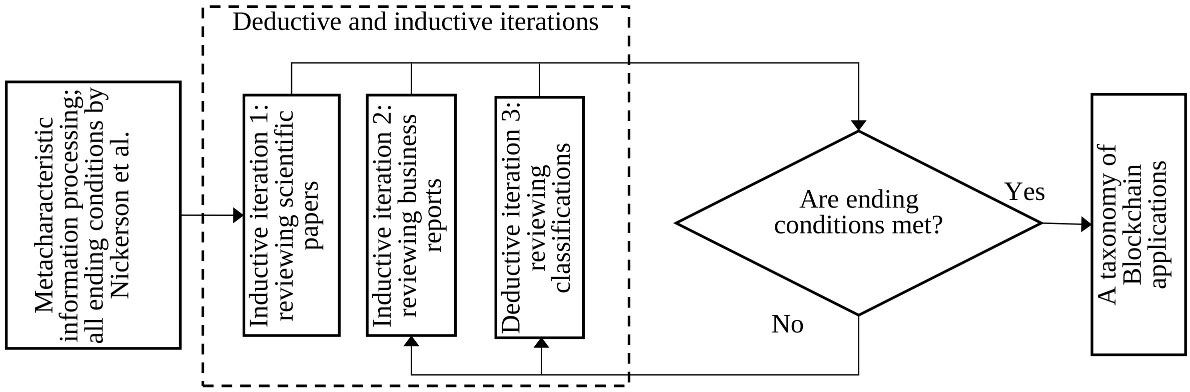

Figure 4. Research Approach. A Taxonomy of Blockchain Applications

5.3.1. Development of the Taxonomy of Blockchain Applications

The objective of the taxonomy is to classify Blockchain application areas based on technical Blockchain characteristics. Therefore, we have selected technical Blockchain characteristics (e.g., consensus mechanism, anonymity level) as the metacharacteristics. The choice and combination of technical Blockchain characteristics are central to the success or failure of Blockchain-based systems. The metacharacteristics serve as the basis for the identification of further dimensions and characteristics.

We developed the taxonomy in three iterations. The first two iterations were inductive iterations, where we have identified application cases to derive dimensions and characteristics. For each inductive iteration, we used different types of sources: scientific literature and business reviews, respectively. The third iteration was a deductive iteration where we revised the taxonomy based on previous classifications. *In the first iteration,* we searched articles in the web of science core collection[1] with the search string “Blockchain OR distributed ledger” on October 17, 2016, in title, abstract, and keywords, covering the whole period of publications

[1] Used indices: “Science Citation Index Expanded (1900-present), Social Sciences Citation Index (1900-present), Arts & Humanities Citation Index (1975-present), Conference Proceedings Citation Index- Science (1990-present), Conference Proceedings Citation Index- Social Science & Humanities (1990-present), Book Citation Index– Science (2005-present), Book Citation Index– Social Sciences & Humanities (2005-present), and Emerging Sources Citation Index (2015-present)”

(Webster and Watson, 2002; vom Brocke et al., 2009). The search returned fifty-one papers. After screening of titles and abstracts, we coded the forty-one remaining relevant articles. In the first iteration, we identified six dimensions with fourteen characteristics and six application areas with sixteen application cases. The analysis of the scientific literature revealed detailed information on separate Blockchain characteristics (e.g., consensus mechanisms) or specific Blockchain application examples (e.g., energy markets, prediction platforms) but lacked comprehensiveness. *In the second iteration*, we analyzed business reviews, which provide less profound but more comprehensive information. We investigated twenty business reports by national agencies, consulting companies, and international institutions. We revised the taxonomy and added two dimensions, seven characteristics, and nine application cases. *The third iteration* was deductive, where we derived characteristics, dimensions, and application cases from fifteen previous classifications. We used all previous classifications that could be identified in extant literature until May 2018. Our taxonomy covers all characteristics in classifications related to technical Blockchain characteristics.

All ending conditions proposed by Nickerson et al. (Nickerson et al., 2013) were fulfilled after the third iteration as follows. First, all found Blockchain application cases described in the scientific literature or business reports can be classified into an application case in the taxonomy. Second, each dimension is unique and mutually exclusive, and each character is unique within its dimension. Third, all application cases were classified with a single characteristic for each dimension. Fourth, the taxonomy is concise—consists only of meaningful dimensions that classify application cases. Fifth, the taxonomy is robust—differentiates each application case from all others. Sixth, the taxonomy is explanatory, comprehensive, and extensible—highlights the main features of each application case and can be extended when new application cases arise.

5.3.2. Data Analysis

To analyze the sources, we have used three types of coding: open coding, axial coding, and selective coding (Wiesche, Jurisch, Yetton and Krcmar, 2017). Open coding is a process for grouping categories and subcategories. Axial coding is a process for testing that categories are related to their subcategories and the relationships against data. Selective coding is a process by which all categories are unified around a 'core' category, and categories that need further explication are filled-in with descriptive details. We applied open coding for initial categorization of dimensions, characteristics, application areas, and application cases; axial coding for removal of overlapping dimensions, characteristics, application areas, and application cases while iteratively testing the taxonomy against data; and selective coding to classify each application case with a characteristic for each dimension. One researcher coded the sources three times, in November 2016, April 2017, and November 2017, and other researchers validated the results after each iteration (Strauss, 1987). Disputes were resolved in group discussions.

5.4. Taxonomy of Blockchain Applications

The developed taxonomy consists of eight dimensions with twenty-one technical characteristics and six application areas with twenty-five application cases (Table 5).

5.4.1. Technical Blockchain Characteristics

The first dimension is *reading access* and represents different modes for reading information on Blockchains. Private reading allows only authorized members to access a Blockchain. Public reading access allows everyone to read data from a Blockchain. The second dimension is *writing access* and represents different modes of writing information on a Blockchain. Permissioned writing access requires users to be authorized to add transactions. If writing access is not permissioned, a user does not have to be authorized to add transactions. The third dimension is the *main consensus mechanism* and is concerned with employed means for updating Blockchains; we focused on four predominant consensus mechanisms. Proof-of-work requires some resources (or work) from a requester, usually the processing time of a computer to solve a computationally difficult puzzle. Proof-of-stake asks users to prove the ownership of a certain amount of digital data to establish their stake in this data. Practical Byzantine fault tolerance gathers individual decisions made by trusted nodes in a network that together determine system-level agreements. Self-developed consensus mechanisms are used in some application cases and usually include several highly trusted nodes for arriving at system-level agreements. The fourth dimension is *anonymity level* and assesses whether users can be matched to identities. If Blockchains have the characteristic anonymous, users do not have to provide any data to work with Blockchains. If Blockchains are pseudonymous, users have to work under a pseudonym. Blockchains with the characteristic identifiable ask for or automatically collect personally identifiable information, such as email addresses. The fifth dimension is *event handling* and discerns whether Blockchains can handle application logic or events. No event handling shows an inability to handle application logic. Fixed event handling supports built-in events. Custom event handling means that a Blockchain supports the processing of any application logic provided by users. The sixth dimension is *data exchange type* that focuses on the type of information sharing between users on Blockchains and includes the characteristics transaction and content. The transaction implies an exchange of logs of executed actions. Content means that digital assets, such as documents, messages, and video or music files, are exchanged. The seventh dimension is *encryption* and specifies whether data on Blockchains is encrypted. Unencrypted means that no data on the Blockchain is encrypted. Partially-encrypted represents Blockchain, where some data is encrypted. Totally-encrypted means that all data on Blockchains is encrypted and has to be decrypted for all operations. The eighth dimension is *history retention* and ascertains whether the whole Blockchain or only its recent updates are kept and distributed between hosts. The whole retention means that the whole history starting with a genesis block is kept in a Blockchain and distributed between nodes. Recent updates retention specifies that only the latest updates are kept and distributed.

5.4.2. Blockchain Application Cases

We identified six Blockchain application areas comprising a total of twenty-five application cases. Application areas capture the basic functionalities that can be performed by Blockchains and group application cases with similar semantic features and similar combinations of technical Blockchain characteristics. The first application area is *financial transactions* and captures seven application cases concerned with money transfer and exchange. Conventional cryptocurrencies use public unpermissioned Blockchains, where consensus is achieved through proof-of-work, and users act under pseudonyms. Blockchains with the same characteristics except for anonymous user access support anonymous cryptocurrencies. To confirm the interest of users in Blockchain and to reduce processing costs, wealth storage & micro-payments require proof-of-stake consensus mechanisms along with public unpermissioned Blockchains and pseudonymous users. Public permissioned Blockchains with some modifications of proof-of-work consensus mechanism support financial services by expanding the functionality of payments through financial checks and deposits. Energy-efficient financial services use Blockchains with the same characteristics as financial services except for proof-of-stake consensus mechanisms. Enterprise global- and micro-financial transactions employ private unpermissioned Blockchains with practical Byzantine fault tolerance consensus mechanism, which requires unique identification of nodes in the network. Global centrally issued financial instruments are deployed on private permissioned Blockchains with self-developed consensus mechanisms, which also require unique identification of the nodes.

The second application area is *smart contracts* and processes application logic. The application area contains eight application cases. Most smart contracts work on public unpermissioned Blockchains with a proof-of-work consensus mechanism. At the same time, a proof-of-stake consensus mechanism supports energy-efficient smart contracts. For testing purposes, one can create private Blockchains that comprise only one node. Community smart contracts, which must comply with different community rules, are based on public permissioned Blockchains with proof-of-work consensus mechanisms. Energy-efficient community smart contracts apply proof-of-stake consensus mechanisms. Enterprise smart contracts use private unpermissioned Blockchains. Global agreements between institutions can be achieved based on private permissioned Blockchains.

The third application area is *data management* and is concerned with information management, such as authentication, know-your-customer services, and control of business assets. The area includes three application cases. To manage assets registered off-chain, global authentication and ownership require public unpermissioned Blockchains with proof-of-work consensus mechanisms and pseudonymous users. Sharing economies and enterprise asset management require data management with identification and authorization schemes implemented directly on a Blockchain. To avoid fraud although opening a network for many nodes, sharing economies use public permissioned Blockchains with proof-of-work consensus mechanisms and identifiable users. To keep the information confidential, enterprise asset management applies private permissioned Blockchains that reach system-level consensus by practical Byzantine fault tolerance and require unique identification of nodes.

The fourth application area is *storage* and is concerned with keeping digital assets, such as certificates or music and video files, on Blockchains. Open access publishing uses public Blockchains and requires no data encryption. Content preview employs public Blockchains with partial encryption of data. Blockchain-based decentralized storage is implemented on public Blockchains with total data encryption and some modifications for faster content sharing and decoding.

The fifth application area is *communication*. Broadcasting is supported by public unpermissioned Blockchains with proof-of-work consensus mechanisms and without data encryption because the content is intended for mass communication. Public permissioned Blockchains with proof-of-work consensus mechanisms are suitable for discussion forums, which allow any user to participate in communication but automatically collect IP addresses. Internet-of-things communication uses private unpermissioned Blockchains and practical Byzantine fault tolerance consensus mechanism to control information exchange between devices in enterprise or home networks.

The sixth application area is *ranking* with a single application case. Global reputation & rating is supported by public permissioned Blockchain with proof-of-work consensus

Table 5. A Taxonomy of Blockchain Applications

A TAXONOMY OF BLOCKCHAIN APPLICATIONS		Reading access		Writing access		Main consensus mechanism				Anonymity level			Event handling			Data exchange type		Encryption			History retention	
		Pr	Pu	P	U	W	S	B	SD	A	P	I	N	F	C	T	C	U	P	T	W	R
Financial transactions	Anonymous cryptocurrencies		X		X	X				X			X			X				X	X	
	Cryptocurrencies		X		X	X					X		X			X		X			X	
	Wealth storage & micro-payments		X		X		X				X		X			X		X			X	
	Financial services		X	X		X					X		X			X		X			X	
	Energy-efficient financial services		X	X			X				X		X			X		X			X	
	Enterprise global and micro-financial transactions	X			X			X				X	X			X			X		X	
	Global centrally issued financial instruments	X		X					X			X	X			X			X		X	
Smart contracts	Smart contracts		X		X	X					X				X	X		X			X	
	Testing of smart contracts	X			X	X					X				X	X		X			X	
	Energy-efficient smart contracts		X		X		X				X				X	X		X			X	
	Testing of energy-efficient smart contracts	X			X		X				X				X	X		X			X	
	Community smart contracts		X	X		X					X				X	X		X			X	
	Energy-efficient community smart contracts		X	X			X				X				X	X		X			X	
	Enterprise smart contracts	X			X			X				X			X	X			X		X	
	Global agreements between institutions	X		X					X			X			X	X			X		X	
Data management	Global authentication and ownership		X		X	X					X			X		X		X			X	
	Sharing economies		X	X		X						X		X		X		X			X	
	Enterprise asset management	X			X			X				X		X		X			X		X	
Storage	Open access publishing		X	X		X						X		X			X	X			X	
	Content preview		X	X		X						X		X			X		X		X	
	Decentralized storage		X	X		X						X		X			X			X	X	
Communication	Broadcasting		X		X	X						X		X			X	X				X
	Discussion Forum		X	X		X						X		X			X	X				X
	IoT communication	X			X			X				X		X			X	X				X
Ranking	Global reputation & rating		X	X		X						X		X		X		X				X

LEGEND
X – characteristics belong to an application case
Reading access
Pr – Private: only authorized members of a limited community can read Blockchain
Pu – Public: everybody can read a Blockchain
Writing access
P – Permissioned: a user should be authorized to validate transactions
U – Unpermissioned: a user can validate transactions without authorization
Main consensus mechanism
W – Proof-of-work: consensus for secure Blockchain updating is achieved by Proof-of-Work
S – Proof-of-stake: consensus for secure Blockchain updating is achieved by Proof-of-Stake
B – Practical Byzantine fault tolerance: secure Blockchain updating is achieved by agreements of trusted nodes
SD – Self-developed mechanism: consensus for secure Blockchain updating is achieved by self-developed mechanism
Anonymity level
A – Anonymous: users do not have to provide any data for working with Blockchain
P – Pseudonymous: users can work with a Blockchain under a pseudonym
I – Identifiable: users should provide personal data to work with a Blockchain

Event handling
No – No: Blockchain does not support any events
F – Fixed: Blockchain supports built-in events
C – Custom: Blockchain supports processing of events created by user
Data exchange type
T – Transaction: logs of actions executed are exchanged among users and recorded on a Blockchain
C – Content: digital assets are exchanged among users and recorded on a Blockchain
Encryption
U – Unencrypted: all data on a Blockchain is unencrypted
P – Partially-encrypted: data on a Blockchain is partially encrypted
T – Totally-encrypted: all data on a Blockchain is encrypted
History retention
W – Whole: Blockchain keeps whole transaction history from a genesis block
R – Recent updates: Blockchain keeps only recent updates of the transaction history

mechanisms and automatic collection of identifiers to link identities to individual users and to prevent users from obtaining more than one identity.

5.4.3. Demonstration of the Utility of the Taxonomy

We demonstrated the utility of the taxonomy on ninety-nine Blockchain-based systems mentioned in the scientific and business sources. To classify identified Blockchain-based systems with the taxonomy, we have used white papers, the systems' websites, press releases, and set up the systems and tested them if it was possible. The demonstration of the utility of the taxonomy shows that the taxonomy classifies successful Blockchain-based systems and purposefully does not classify some Blockchain-based systems.

5.4.3.1 Classified Blockchain-Based Systems

The gathered Blockchain-based systems predominantly cover the financial sector. Anonymous cryptocurrencies include Zero coin, Dark coin, Crypto Note, and Monero. Conventional cryptocurrencies comprise Bitcoin, Prime coin, lite coin, Tether, DagCoin, Crypt Crypto sigma, DigixGlobal, Game Credits, Bit pay, and Solar Coin. Peer coin, Navcoin, AML, and Black coin target wealth storage & micro-payments. Counterparty, Master coin, and Digital Note execute financials services. Bit Shares allows for energy-efficient financial services. Ripple, SWIFT gpi, Stellar, and BitPesa support enterprise global and micro-financial transactions. R3, Fed coin, Symbian Assembly, RSCoin, and One coin represent global centrally issued financial instruments.

Smart contracts are popular for the identified Blockchain-based systems. Ethereum, Hawk, Stratis, Qtum, Blockcypher, deck bound, Rootstock, iExec, Chimera, We Trust, Sia, and Maid safe support original smart contracts. Testing of smart contracts is possible on Ethereum (testing environment), Hawk (testing environment), and EOS. Casper, Tender mint, and Next develop energy-efficient smart contracts. Testing of energy-efficient smart contracts is performed on Casper (testing environment). Counterparty supports community smart contracts. Lisk and Tezos execute energy-efficient community smart contracts. Hyperledger, Ripple Codius, Eris (Monax), Digital asset, Waves, and Catenis Enterprise support enterprise smart contracts. R3 Codra allows reaching global agreements between institutions.

Data management on Blockchains gains momentum. Colored coins, Name coin, one name, POEX.IO, OP_RETURN, Ever pass, The Real McCoy, Bit Health, BitAuth, UniquID, NEM Apostille, Block name, Filament, ePlug, and Showcard represent global authentication and ownership. Iconomi, NEO, Ridde & code, Aragon, and La'Zooz are examples of sharing economies. Ever ledger, Peer Nova, Factom, Chroma way, Block Verify, Peer Nova, Chronicled, and ShoBadge support enterprise asset management.

A smaller number of Blockchain applications supports Blockchain-based storage. Synereo fulfills open access publishing. Kishigami et al. (2015) describe content preview on Blockchains; although we did not find Blockchain-based systems to support the application case, we decided to keep the application case for further research. The Story project examines decentralized storage on the Blockchain.

Communication is not often implemented on Blockchains. Basic Attention Token shows broadcasting. Blockchain-based discussion forums include Whisper and Match pool. Blockchain of Things and IBM Adept support internet-of-things communication.

Ranking on Blockchains is an uncommon Blockchain application case. Augur, TRST.im, The World Table, and Trust Davis support global reputation & rating.

5.4.3.2 Unclassified Blockchain-Based Systems

We found Blockchain-based systems that purposefully remain unclassified by our taxonomy. The first reason for unclassified Blockchain-based systems is an application area that appears to be unsuitable for Blockchains. Such Blockchain applications have broad ideas and aim to replace current information systems with Blockchains (e.g., decentralized internet); however, they do not result in any proofs of concept. Other examples arise when Blockchain applications use Blockchains when Blockchains are not needed (e.g., private messengers on Blockchains can be replaced by conventional peer-to-peer systems).

The second reason for unclassified Blockchain-based systems is combinations of technical Blockchain characteristics that appear to be ineffective. These Blockchain-based systems exhibit or intensify security threats or privacy concerns. For example, hackers attack Blockchains by forking them, developers of Blockchain-based systems can falsify data on Blockchains, and users can be traceable when permissions to read and write data on Blockchains do not comply with consensus mechanisms or with anonymity protection of users.

The third reason for unclassified Blockchain-based systems is a combination of Blockchain application areas and technical Blockchain characteristics that appear to be unsuitable. For example, a Blockchain-based system that aims to manage certificates between trustful organizations (e.g., school diplomas between schools and employee companies) is an example of enterprise asset management. However, an application we identified uses a public Blockchain with a proof-of-work consensus mechanism instead of a private Blockchain with a practical Byzantine fault tolerance consensus mechanism. The reason why the application uses a Blockchain is not due to the actual number of nodes but due to the borrowed public infrastructure. The concerns arise. If the application uses a public Blockchain, transactions are expensive because of the consensus mechanism. For transactions on this Blockchain, the issuers of the certificates (e.g., schools) must be trustful to prevent information manipulation or fraud (e.g., an actor could send transactions to himself to change records). However, if issuers are trustful, a public Blockchain is useless. Therefore, the Blockchain application ignores the main dilemma in using Blockchains and public-private infrastructure: the more trustful issuers are, the less energy-consuming the employed consensus mechanism should be.

5.5. Discussion

The developed taxonomy serves as a bridge between Blockchain technology and Blockchain applications. The taxonomy constitutes a tool to connect technical Blockchain characteristics across a range of foundational application cases. There are five principal findings. First, application areas are at different maturity levels. Financial transactions constitute the most mature application area and are supported by existing proofs of concept. Smart contracts have found much attention because of the idea to execute agreements on Blockchains. Data management gains momentum because of emerging application cases (e.g., enterprise asset management). Storage, communication, and ranking on Blockchains are less prevalent. Blockchain scalability issues prevent the storage of data on Blockchains. The value of applying Blockchains for communication and ranking is specific to each application case. In particular, it is challenging to support mobile devices when energy-consuming consensus mechanisms and the transfer of the whole transaction history are required.

Second, application cases inside one application area vary in the dimensions reading access, writing access, main consensus mechanism, and anonymity level. The characteristics in these dimensions depend on the required levels of decentralization for application cases. The more centralization is required, the more private reading access and the more permissioned writing access is required. Main consensus mechanism and anonymity level follow the required level of decentralization so that the more centralization is required, the less energy-consuming are consensus mechanisms and the less anonymous are nodes.

Third, we reveal new technical dimensions that are overlooked in extant technical classifications on Blockchains. The new dimensions are event handling, data exchange type, encryption, and history retention. Custom event handling specifies smart contracts. Data exchange type allocates whether data is stored on or off Blockchains. Encryption is different between applications that require to store content on Blockchains. History retention is different for applications that store Blockchains on small-capacity external devices.

Fourth, not all and different technical Blockchain characteristics are suitable for different application areas. For example, communication systems based on private permissioned Blockchains do not appear to create additional value compared to peer-to-peer messengers such as Telehash, which are used by many decentralized services (e.g., IBM Adept). However, this statement requires further investigation.

Fifth, the taxonomy purposefully avoids the classification of poorly developed Blockchain-based systems because Blockchain application cases are identified and related to unique and effective combinations of technical characteristics. Therefore, Blockchain-based systems that are not captured by the taxonomy might represent application areas that are unsuitable for Blockchains. Combinations of technical characteristics that contradict the taxonomy can lead to inefficient technical designs. Inconsistencies between application areas and technical designs may indicate a lack of compliance with technical and application requirements. However, the taxonomy is only based on extant knowledge in research and practice and this assertion requires further research.

There are three promising areas for future research. First, research that replicates our research approach with more or different scientific and business sources will be useful to falsify or corroborate our findings. Second, further analysis of theoretical findings allows hypothesizing about the relationships between application areas and technical Blockchain characteristics. Third, research that focuses on socio-economic concepts different from application areas, for example, market regulations in different countries will be useful to contextualize the taxonomy for different industries and domains.

This study is not without limitations. First, the taxonomy cannot identify application areas that may emerge in the future. The rapidly evolving nature of the Blockchain domain will necessitate an extension of the taxonomy with new application cases. Second, the identified application areas do not directly capture more complex services, such as prediction markets or crowdsourcing platforms; instead, we decided to break complex application cases down into the basic functionalities that can be performed by Blockchains.

This research contributes to the scientific literature on Blockchain in three ways. First, the allocation of Blockchain application cases based on technical Blockchain characteristics reduces the hype around Blockchain application possibilities. Classification of application areas that are based on technical characteristics makes the identification of application areas more meaningful. The well-studied financial sector can serve as a good example of how to leverage Blockchains in less studied application areas and the other application areas may reveal opportunities that have been overlooked in the financial sector. Second, we identified additional technical dimensions of importance to the Blockchain. While some of the taxonomy dimensions (reading access, writing accesses, main consensus mechanisms, and anonymity level) align with previous taxonomies, the remaining dimensions (event handling, data exchange type, encryption, and history retention) represent specific application areas and complement previous taxonomies by offering more comprehensive insights into the technical nature of Blockchains. Therefore, technical research can go beyond Bitcoin and focus on other areas, for example, a Blockchain protocol for data transmission in healthcare. Third, previous taxonomies consider technical knowledge or application knowledge separately. Our taxonomy combines knowledge, which bridges the gap between technical and application research on Blockchain. Linking application areas and technical characteristics informs step-by-step guidelines for leveraging Blockchains across applications. Such guidelines are useful for the further development of successful Blockchain-based systems.

This research contributes to practice in three ways. First, we present further evidence that Blockchains are not only applicable to the financial sector, which is the focus of the majority of Blockchain projects but also for other promising areas. Thus, other industries can use Blockchain advantages for resolving their challenges. For example, in the media industry, Blockchain-based data management may be useful to monitor the use of media content to prevent copyright infringements. Second, we highlight other Blockchain characteristics besides the widely-known public Blockchains that can be useful if public Blockchains cannot be employed. Businesses may consider the implementation of private Blockchains that store information in a more reliable way. Third, we have proposed the taxonomy of Blockchain applications to guide the development of more successful Blockchain-based systems. The taxonomy establishes an overview of Blockchain applications, organizes them in application areas, and relates them to technical Blockchain characteristics. Furthermore, the taxonomy can be used to avoid poorly designed Blockchain applications. This might be useful for practitioners to identify the more promising Blockchain projects and assess risks during Blockchain implementation. For example, chief information officers could learn which modules in the enterprise information systems landscape can be realized on Blockchains and developers could learn which peer-to-peer system prototypes are worth to be developed on Blockchains.

5.6. Conclusion

A Blockchain is a decentralized digital ledger with a largely untapped potential to enhance many aspects in the information systems domain. Currently, research streams on Blockchain remain disconnected, which prevents further development of successful Blockchain-based systems. Our work consolidates knowledge on technical Blockchain characteristics and application areas in the form of a taxonomy. The taxonomy accounts for twenty-five application cases aggregated into six application areas that relate to twenty-one technical Blockchain characteristics in eight dimensions. Overall, the taxonomy consolidates extant knowledge on Blockchains to calm the Blockchain hype and foster the development of more realistic Blockchain-based systems.

6. Smart Contract Design Patterns to Assist Blockchain Conceptualization

Table 6. Bibliographical Information for Paper 2	
Title	Smart Contract Design Patterns to Assist Blockchain Conceptualization
Authors	(1) Sandra Klein, University of Cologne (2) Wolfgang Prinz, Fraunhofer Institute for Applied Information Technology, RWTH Aachen (3) Wolfgang Gräther, Fraunhofer Institute for Applied Information Technology (4) Olga Labazova, University of Cologne
Outlet	European Conference on Information Systems
Publication Type	Conference Proceedings
Publication Year	2020
VHB-JOURQUAL3	B
Publication Status	Submitted, Under Review

Abstract. Blockchain technology and how it can be used to enhance existing business models as well as create new ones receive a lot of attention from a variety of industries. Especially the possibility to automate business models with smart contracts makes Blockchain technology interesting. However, there is a lack of defined standards that Blockchain developers can use to make the implementation process easier and more successful. The design patterns of Blockchain smart contracts can provide these standards. This research aims to develop smart contract design patterns to close the gap in Blockchain research practice. To create the design patterns, we started with a list of structural elements that describe the patterns. Further, sixteen smart contract design patterns were derived from the existing literature and smart contract implementations. Lastly, a pattern language was created by examining and summarizing the relationships between smart contract design patterns.

6.1. Introduction

Blockchain is a new, innovative discovery and a current buzzword. Blockchain has reached a certain maturity together with a critique of overselling its potential. Some people describe it as a disruptive technology that rapidly creates new use cases in a variety of industries (Wang et al., 2018). Others see Blockchain as a foundational technology that will slowly change the way how the entire society works (Iansiti and Lakhani, 2017). Almost everyone, however, agrees that Blockchain has a great potential to transform industries, existing processes, and business models.

Especially smart contracts, i.e. software code that represents Blockchain application logic to automate processes (Christidis and Devetsikiotis, 2016), receive great attention (Möhring, Keller, Schmidt and Schulz, 2018). While the potentials of smart contracts can be endless, it is difficult to develop smart contract applications on the Blockchain (Möhring et al., 2018). To put the transformative ideas around smart contracts into practice, smart contracts and the way they can be used in Blockchain applications need to be thoroughly understood (Bartoletti and Pompianu, 2017). One way to aid developers in creating architectures for smart contract applications can be design patterns (Hahn, Singh, Liu and Chen, 2017). This research aims at providing those design patterns by answering the research question "*Which design patterns can be detected in smart contracts embedded in Blockchain applications and how do those patterns interact with each other?*"

Because Blockchain itself is a relatively recent technological development, research about Blockchain application development and smart contracts is similarly little advanced (Liu et al., 2018). Especially information systems (IS) research on the Blockchain is very scarce, and even though there are studies about the impacts of Blockchain technology, there are hardly any guidelines on how Blockchain-based applications should be implemented (Du, Pan, Leidner and Ying, 2019). Beck et al. (2017) formulate the need for more research about "novel approaches to [the] development of Blockchain applications" and suggest addressing the "challenges of implementing business logic in the smart contract[s]". The goal of this research touches both suggestions, as design patterns could support the structuring of business logic into smart contracts and consequentially the design of Blockchain applications.

To answer the research questions, three sub-goals are defined to provide a comprehensive solution to the research problem. The first sub-goal aims at defining an appropriate structure for the presentation of the smart contract design patterns. The second sub-goal aims at creating a list of smart contract design patterns by conducting a literature review on those Blockchain use case descriptions where smart contracts are applied. These design patterns will be described using the structure which has been defined during the first sub-goal. The third sub-goal then aims at creating a pattern language by revealing and visualizing relationships between the individual patterns identified during the second sub-goal to support the methodological development of new Blockchain applications. Overall, this research aims to provide practitioners with a solid baseline for the development of reusable smart contract libraries.

6.2. Theoretical Background

To understand the concept of smart contract design patterns, we give a background of Blockchain and smart contracts. Further, we present the idea of design patterns and their connection to the development of smart contracts.

6.2.1. Blockchain and Smart Contracts

Blockchain is a distributed ledger technology (DLT) which was introduced in 2008 by Satoshi Nakamoto, the inventor of the Bitcoin Blockchain (Nakamoto, 2008). In a distributed ledger, instead of one centralized entity having the entire control over one centralized database, a copy of the whole ledger is stored with each member of the network, each of them operating a node (Ølnes, 2016). Blockchain technology is a subcategory of DLT, thus every Blockchain is a DLT, but not every DLT is a Blockchain. A Blockchain consists of a chain of blocks and each block in the Blockchain consists of four elements: transactions, a reference to the previous block, a timestamp, and a nonce. A nonce represents a number that needs to be found or calculated by a node to be able to create the block (Nakamoto, 2008). The reference to the previous block is realized with the help of a unique hash code which is then incorporated into the next block, tying blocks together into a chain, the Blockchain (Chen and Bellavitis, 2020).

Originally, the idea of smart contracts was formulated by Szabo (1997), who described them as a possibility to implement clauses of a contract into hardware and software in a way that penalizes someone who tries to breach the contract. Smart contracts were incorporated into Blockchain by Vitalik Buterin in 2014, a founder of Ethereum (Buterin, 2014). By placing smart contracts immutably on the Blockchain, the technology can be used to automate complex business processes (Christidis and Devetsikiotis, 2016). They are generally used to provide a solution for a recurring problem that can automatically be executed once certain conditions are met (Ølnes, 2016). One example of a smart contract could be the automation of customer reimbursements of flight delays or cancellations (Hans, Zuber, Rizk and Steinmetz, 2017).

Smart contracts in Blockchain applications are implemented in a programming language that differs across Blockchains. Every smart contract has an address, thus the functions encoded in the smart contract can be triggered by network participants or another smart contract by calling the smart contract's address and invoking a specific function (Beck et al., 2016). When the smart contract gets triggered, it automatically executes the appropriate transactions and thus fulfills the contract without the need of a third party to intercept (Yuan et al., 2018).

Although the term "smart contract" incorporates the word "contract", their legal enforceability is not clear (Christidis and Devetsikiotis, 2016). On the one hand, only because a contract is written in an electronic form on a Blockchain doesn't mean that it is not a legitimate contract (Savelyev, 2017). However, as Giancaspro (2017) points out, there are issues like the anonymity of the contractual partners which could make the contract legally void if one partner is, for example under-aged. That cannot be detected by a smart contract on a public Blockchain.

Blockchain technology and smart contracts incorporate several features that provide advantages compared to other technologies. Firstly, decentralization removes the single point of failure inherent to centralized systems (Yli-Huumo et al., 2016) and instead creates redundancy by storing the ledger at every node while offering the same rights and obligations to each of these nodes (Kuo et al., 2017). Secondly, Blockchain provides a high degree of transparency. By enabling every participant of the network to access the information stored on the ledger, every node can also verify and inspect the correctness of this information (Wang et al., 2018). Thirdly, the immutability of the ledger ensures that once any type of transaction is verified by the network and added into a block, this transaction cannot be altered (Wang et al., 2018). And lastly, smart contracts enable the automation of workflows and business processes (Christidis and Devetsikiotis, 2016).

6.2.2. Design Patterns

The idea of design patterns does not originate in software design but was first introduced by Quinan and Alexander (1981). Beck and Cunningham (1987) applied design patterns to software design and were quickly followed by other researchers. Further, Gamma, Helm, Johnson and Vlissides (1993) developed one of the most popular collections of software design patterns. According to them, “design pattern names, abstracts and identifies are the key aspects of a common design structure” (Gamma et al., 1993). Therefore, design patterns are suitable means to express and pass on design experience and should be understandable by persons from different professions (Borchers, 1999).

However, design patterns are not absolute. They need to be continuously developed to keep pace with the current state of the art (Quinan and Alexander, 1977). Furthermore, they are subjective, because experts have different conceptions of what a pattern is (Gamma et al., 1993).

Design patterns usually do not exist in isolation (Quinan and Alexander, 1977). There are design patterns of different sizes, meaning that a pattern is often made up of several smaller patterns and can vice versa be a part of larger patterns. This leads to relationships between design patterns which define how patterns interact with one another (Gamma et al., 1993). From those relationships and connections between individual patterns, a pattern language can be deduced which can aid a designer in finding individual solutions to his design problems (Quinan and Alexander, 1977).

6.3. Related Research

There is already some research available about design patterns for Blockchain smart contracts, however, none of this previous work aims at providing the thorough and infrastructure-independent overview that this research intends to present. Bartoletti and Pompianu (2017) restrict their development of design patterns to smart contract implementations in Ethereum and come up with a total of 9 design patterns. Wohrer and Zdun (2018) also narrow their research down to Ethereum smart contracts, however, they describe 18 design patterns organized into 5 categories and they also include some examples of how hierarchical structures can be detected between those design patterns. Eberhardt and Tai (2017) describe 5 patterns specific to the purpose of using smart contracts to perform certain activities of the Blockchain, to improve application performance. These patterns can be used individually or in combination. Liu et al. (2018) investigate existing design patterns for distributed systems, peer-to-peer systems, and general software design to identify patterns suitable for Blockchain smart contracts. They result in 8 interconnected design patterns in 4 categories to guide the architectural design of smart contracts, independent of their functions. And finally, Xu et al. (2018) present a collection of 15 design patterns for Blockchain-based applications, however, although these patterns seem to be application-independent, the lack of a methodology description leaves the question open of how the design patterns were developed and for which Blockchain infrastructures they are suitable.

While these examples from the literature provide important insights into the use of smart contracts and smart contract design patterns, they differ significantly from the goals of this research. Firstly, this research will provide infrastructure-independent design patterns based on actual Blockchain implementations, thus there will be no restriction to Ethereum or any other infrastructure. Secondly, as far as possible, this research will cover the whole range of possible smart contract functions and application areas. And thirdly, besides describing the design patterns, a pattern language will be designed to show relationships between the individual design patterns and to aid designers of Blockchain applications.

6.4. Research Design

To develop infrastructure-independent design patterns, the literature review approach was chosen. By analyzing research papers instead of smart contract implementations on a Blockchain platform, even those use cases can be considered that have been implemented on lesser-known platforms or on platforms that may have been specifically designed for this use case. Furthermore, the goal of this research is to provide detailed descriptions instead of actual pseudo-code for the design patterns, which is why the rich contexts and explanations available in research papers are more useful than pure source code.

While conducting the literature review, a structured approach of vom Brocke et al. (2009) and Webster and Watson (2002) was applied. According to vom Brocke et al. (2009), the process for conducting a literature review consists of 5 phases. The first phase is to define the review's scope and intent. This phase has been carried out by defining and explaining the research questions in section 1. During the second phase, an overview of the current knowledge base in the respective research field needs to be created. This phase has been performed by explaining the relevant terms as well as the current state of research on smart contract design patterns in sections 2 and 3. The third phase involves the literature search. During this phase, a three-step approach as introduced by Webster and Watson (2002) was performed, which included a literature search in several databases, a backward search and a forwards search. The fourth phase according to vom Brocke et al. (2009) involves the analysis and synthesis of the identified literature. During the fifth and last phase, the results of the review are used to determine further research opportunities (vom Brocke et al., 2009).

6.4.1. Literature Search

Two literature searches were conducted, to determine an appropriate structure for describing smart contract design patterns and to identify Blockchain applications from which the design patterns, as well as their relationships, were deduced. To identify suitable research papers, the EBSCO databases "Business Search Complete, "EconLit" and "Academic Search Complete" were used, as well as the Association for Information Systems Electronic Library (AISeL), the Association for Computing Machinery (ACM) Digital Library, the Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library, Science Direct and ProQuest. As suggested by vom Brocke et al. (2009), during the literature search an ongoing evaluation took place to eliminate papers that were not relevant to the research question.

The literature search for the first sub-goal was carried out by searching for the keywords "Design Patterns" and "Software". Relevant papers were identified by several facts: Firstly, the respective paper included a description of novel software design patterns, secondly, the patterns were described in a way that covered several structural elements for describing design patterns, thirdly, more than one design pattern was described and lastly, all design patterns in the paper were described using the same structure. This database search resulted in 31 relevant papers. Together with relevant literature collected during the research for the theoretical background as well as a backward search, a total of 47 relevant papers were identified.

To conduct the literature search for the second and third sub-goal, the database search was conducted by searching for the keyword "Blockchain" as well as one of the terms "Smart Contract" and "Chain code", the latter describing smart contracts in the Hyperledger Fabric Blockchain (Vukolić, 2017). A paper was deemed relevant if it described a Blockchain use case utilizing smart contracts and if the functionalities of these smart contracts were described in the paper. This database search resulted in 146 papers. After adding relevant literature from the theoretical background and performing a backward search as well as a forward search, a second analysis of the collected research was carried out to eliminate those papers which did not provide enough detail on the utilized smart contracts. Only those papers providing real code or pseudo code were considered for the design of the smart contract design patterns, which resulted in a total of 101 relevant papers.

6.4.2. Literature Analysis

During the literature analysis for the first sub-goal, i.e. designing a structure for smart contract design pattern descriptions, a concept matrix as described by Webster and Watson (2002) was utilized to identify and analyze design patterns in software development concerning how often certain structural elements were used in their description. In this concept matrix, each row represented one piece of literature and each column one structural element for the description of smart contract design patterns. For each research article, those columns representing a structural element that appeared in the article were marked. Each time a new structural element was discovered that was different in its contents from all other elements, it was added to the matrix in a new column. In the end, as suggested by Webster and Watson (2002), all identified concepts, in this case, structural elements, were evaluated regarding their uniqueness, importance and usefulness in the context of Blockchain applications.

To achieve the second sub-goal, the creation of smart contract design patterns, a similar approach was used. However, unlike the structural elements of design patterns, the smart contract design patterns were not yet named in the literature, so the concepts, i.e. the design patterns, first had to be defined before a concept matrix could be created. For this purpose, two procedures from the field of Grounded Theory Methodology were used as described by Wiesche et al. (2017). Firstly, open coding was utilized to "attach initial labels to all available data" (Wiesche et al., 2017). In this case, the software code samples in the identified literature were analyzed to identify recurring patterns in how these code samples solve certain problems, and these patterns were then named. Afterwards, the names of these patterns could be used to create a concept matrix and identify all occurrences of the patterns in the literature. Secondly, and parallel to the creation of the concept matrix, axial coding was used to derive more detailed descriptions of the identified design patterns (Wiesche et al., 2017). To achieve this, parts of the information provided in the literature were collected and synthesized to deduce smart contract design patterns.

The third sub-goal, creating a pattern language from the smart contract design patterns, was completed by re-using the concept matrix from the second sub-goal. To deduce relationships between the design patterns, firstly, it was counted how many times different patterns were used in combination. Then, secondly, each design pattern was looked at individually and about its total number of occurrences it was calculated how often each other design pattern was used in combination with this pattern.

The results of this were expressed in percentages, for example, in X percent of the times where pattern A was used, pattern B was also used. And finally, in a third step literature samples for each relationship were identified and evaluated to find evidence that this relationship was a result of causality rather than of chance.

6.5. Results

Here, the results of the literature reviews will be presented. First, the structural elements that will be used to describe the smart contract design patterns are presented. Second, the smart contract design patterns deduced from the literature will be listed and explained. Third, the pattern language connecting all these design patterns is going to be outlined.

6.5.1. Structural Composition of Smart Contract Design Patterns

All descriptions of software design patterns in the literature adhere to a certain structure. In most cases, the authors use specific labels to divide the descriptions into understandable paragraphs, for example into the structural elements "context", "problem", "solution" and "examples" (Laurillau, 2013). As a first result of the literature analysis, 25 of these structural elements were identified. In a second step, those structural elements that were very similar in what they contributed to the design pattern description were summarized to one single element. Additionally, those elements that were only mentioned in one research paper were eliminated, since the lack of further mentions suggests only minor relevance. This summary and elimination process resulted in 17 remaining structural elements. However, not all of these 17 elements are relevant to describe smart contract design patterns. Using all these elements could result in redundancy, because they partly overlap in their meaning, as well as in too high complexity, and are thus better integrated into other, more overarching structural elements.

Additionally, providing very detailed implementation guidelines is not the goal of this research, which is why coding-related elements were not further considered. Therefore, in a third step, the list of structural elements was shortened to result in a list of 12 elements. Seven of these 12 elements were adopted as they are described in the literature, while three elements, namely “classification”, “graphical representation” and “references to other patterns”, were adapted in their meaning to better fit the context of smart contract design patterns. One element, “variations” had been eliminated in the second step due to only one mention in the literature but was re-introduced because it became apparent that there are often several different ways to solve the same problem in a Blockchain smart contract context. And finally, the structural element “Blockchain characteristics” was introduced as a new element to draw a bridge to the Blockchain context of the described smart contract design patterns. As a result, these 12 structural elements, which will be used to describe the smart contract design patterns (Table 7).

Table 7. List of Structural Elements of Smart Contract Design Patterns

Name	Description	Source
Pattern name	One or two words capturing the situation in which the design pattern is applied.	(Gamma et al., 1993)
Classification	Classification of the design pattern as either a support pattern, a smaller pattern to improve or extend the application, or a larger application pattern providing more comprehensive solutions.	(Gamma et al., 1993)
Summary	One-sentence description to summarize the problem and the solution that the design pattern proposes.	(Gamma et al., 1993)
Problem	Introduction of the general problem the design pattern aims to solve.	(Borchers, 1999)
Solution	A detailed description of how the design pattern solves the problem.	(Borchers, 1999)
Participants	A list of entities that interact in the Blockchain use case and a description of how they interact.	(Gamma et al., 1993)
Consequences	Listing of the benefits and challenges related to the design pattern.	(Gamma et al., 1993)
Blockchain characteristics	Characteristics are specific to Blockchain applications that the design pattern uses to solve the problem as opposed to other solutions without Blockchain. Blockchain characteristics are decentralization, automation, immutability and transparency.	new structural element
Graphical representation	A graphic displaying all involved participants of the design pattern as well as how they interact with the smart contract.	(Gamma et al., 1993)
Variations	Approaches solving the same problem differently or adding optional elements to the described solution.	(Ergin, Syriani and Gray, 2016)
Application examples	Several examples where the design pattern was applied to a use case.	(Gamma et al., 1993)
References to other patterns	List of other patterns that are often used by the described pattern to expand its functionality.	(Gamma et al., 1993)

6.5.2. Smart Contract Design Patterns

During the literature review, 101 papers were identified which describe Blockchain applications and contain detailed descriptions of design patterns by using code samples. These papers were used as a basis to extract the smart contract design patterns presented in this section. Out of these 101 papers, in 70 papers the application was developed for the Ethereum Blockchain, 9 papers described Hyperledger Fabric implementations and 22 papers did not mention a specific Blockchain infrastructure. Regarding the code samples, in 42 cases the complete smart contract code was provided, while 59 papers only provided excerpts of the smart contracts. Out of the 101 papers, 99 were found to include one or several of the identified design patterns, while 2 papers showed very simple implementations, not including any design patterns. The papers describe applications in 18 different application areas, including for example the Internet of Things (IoT), Supply Chain Management (SCM) and smart grids. After the review of this literature base, a total of 16 smart contract design patterns were identified (Table 8). Patterns 1 to 10 are support patterns, while patterns 11 to 16 are application patterns.

Table 8. Overview of Smart Contract Design Patterns

№	Design Pattern Name	Summary	№ of Mentions
1	Create smart contract	Creation of a smart contract as an interactive element for various entities.	11
2	Deactivate smart-contract	Deactivation of a smart contract that is no longer needed.	8
3	Blockchain communication	Updating and extracting information from the underlying Blockchain.	48
4	Oracle	Sending information to or receiving information from outside the Blockchain.	11
5	Fund transfer	Re-allocation of funds between the entities in a Blockchain application.	29
6	Encryption	Encryption and decryption of information on the Blockchain that is not allowed to be read by every application user.	13
7	Smart contract admins	Assignment of roles to entities that interact with smart contracts.	45
8	External arbitrator	Using a third-party arbitrator in situations where the smart contract cannot resolve a conflict by itself.	3
9	Token	Digital representations of assets, values or rights.	14
10	Process automation	Automation of processes by using contract states.	7
11	Entity management	Management of entities like persons, organizations or objects using smart contracts.	57
12	Voting	Provision of a list of options by the contract owner from which voters can choose.	9
13	Trading	Transfer of asset ownership between two parties.	11

14	Renting	Temporary transfer of usage rights to a customer, while the ownership rights stay with the owner.	9
15	Auction	After a request is published on the Blockchain, bids can be added and the initiator can choose the best one.	7
16	Track & Trace	Tracking and asset along with several handlers by using interconnected smart contracts.	6

For each smart contract design pattern, a detailed description has been created, which includes a table describing the pattern by using the structural elements deducted during the first sub-goal of this research, a textual description and a graphical representation which depicts the interactions of the smart contracts with stakeholders as well as the corresponding transactions. These illustrations are helpful to compare and differentiate the patterns. While the descriptions of most structural elements are a direct result of the literature review, the structural elements "classification", "problem", "consequences" and "Blockchain characteristics" were deduced in a second step from the literature review results and are an outcome of interpretations of the literature review which were performed as objective as possible. In the following, a description of the smart contract design pattern "renting" will be provided.

6.5.2.1. Renting

The application pattern "renting" can be applied in all environments where temporary rights to use a physical or digital asset are transferred. In the literature, renting operations occur in the areas of the sharing economy, data management, digital ownership rights and supply chain management.

For this design pattern, one smart contract per physical or digital asset is created by the owner in which he initializes all necessary information like the requested rental fee (Madhusudan et al., 2019). When a potential customer wants to rent the asset, he calls the rental function and deposits the requested funds which usually include the rental fee plus a deposit (Bogner, Chanson and Meeuw, 2016). If applicable, the smart contract then verifies if the object is currently not being rented and if the transferred amount corresponds to the owner's requests. If these verifications are successful, the new customer is stored in the smart contract as the current lessee. During the rental period, the remaining time is constantly observed to ensure that the customer does not use the object longer than he is allowed and, if applicable, sensors are used to detect violations of the rental contract. If any violations are detected, the access to the object is revoked and a penalty is applied to the customer. Both the owner and the customer can cancel the booking under certain conditions (Madhusudan et al., 2019). If the rental period ends without any violations, the information about the current lessee is set back to null, the deposit and any superfluous fees are transferred back to the customer and the owner receives the fees for the rental (Table 9).

Table 9. Design Pattern "Renting"	
Category Name	**Description**
Pattern name	Renting
Classification	Application pattern
Summary	Temporary transfer of usage rights to a customer, while the ownership rights stay with the owner
Problem	• The terms and conditions of a renting contract need to be clear to both sides; • During a renting process, it needs to be made sure that both parties adhere to their obligations, e.g. that the renting person does not inappropriately use the asset.
Solution	• One smart contract is created for each asset; • Customers deposit the necessary funds in the smart contract; • The smart contract verifies that the object is currently free and that the deposited funds correspond to the rental fee; • During the rental period, the smart contract constantly checks for rule violations; • At the end of the rental period, the customer receives his deposit back and the owner receives the rental fees.
Participants	• Owner • Customer
Consequences	+ Rules and obligations are clearly stated in the contract and automatically enforced by the smart contract, therefore both owner and customer have to adhere to the contract + The smart contract automatically handles the rental process, so the owner usually does not need to do anything - The smart contract cannot guarantee that physical assets are not damaged or stolen, so there needs to be a high enough deposit to ensure that the owner does not incur losses
Variations	• Selling of digital assets
Blockchain characteristics	• Decentralization • Automation • Transparency
Application examples	• Car lease platform (Madhusudan et al., 2019) • Protecting author royalty rights of digital (Nizamuddin, Hasan, Salah and Iqbal, 2019) • Renting decentralized storage space (Ruj, Rahman, Basu and Kiyomoto, 2018)
References to other patterns	Uses 3, 5, 7, 9, 11 — Used by /

6.5.3. A Pattern Language of Smart Contract Design Patterns

After having defined the smart contract design patterns, relationships between these patterns can be investigated to find out how the patterns interact with each other in Blockchain applications. To achieve this, the same literature base used for the second sub-goal, the deduction of smart contract design patterns, was utilized as a source to detect which design patterns are used in combination with each other. Of course, two design patterns occurring together in a lot of application examples does not necessarily imply causality between those patterns, however, it might suggest it. Therefore, each design pattern was looked at individually to analyze its relationships with other patterns. The relationships that were found in this analysis are mostly originating from a situation where one pattern uses another pattern to expand its functionality, thus, the pattern language that is created in this section is based on these “pattern x uses pattern y” relationships. Based on the investigated pattern’s total number of occurrences, those relationships with other patterns that occur in at least 50% of these cases will be called “strong relationships”, while “weak relationships” will describe relationships with patterns that occur in at least 30% but less than 50% of the investigated pattern’s occurrences. Aside from a bidirectional relationship between the design patterns “Blockchain communication” and “smart contract admins”, relationships are unidirectional, meaning that in a relationship between two patterns, one pattern uses the second one, but the second pattern does not use the first one.

For example, the design pattern “renting” shows a strong relationship with the design pattern “Blockchain communication” because in many cases, rental operations are recorded on the Blockchain to achieve transparency and certainty for both owner and customer (Nizamuddin et al., 2019). Additionally, weak relationships can be observed with the design patterns “fund transfer”, “smart contract admins”, “token” and “entity management”. A rental operation usually involves the transfer of funds, in this case, the rental fee (Nizamuddin et al., 2019). Smart contract admins are often required for specific functions in the rental process, for example, only an admin can grant access to the rented asset (Nizamuddin et al., 2019) while often only the customer can end the rental period (Madhusudan et al., 2019). Access tokens can be used to allow the customer to use the rented asset (Madhusudan et al., 2019). Lastly, entity management can be used to keep track of all customers (Bogner et al., 2016). Hence, the design pattern “renting” uses the patterns “Blockchain communication”, “fund transfer”, “smart contract admins”, “token” as well as “entity management”.

A pattern language visualizes the relationships between smart contract design patterns (Figure 5). This graphical representation underlines the importance of the design patterns “entity management”, “Blockchain communication”, “smart contract admins” as well as “fund transfer”, which are used the most in total numbers and are also used the most by other design patterns.

Besides these relationships, which describe how one pattern uses another pattern, there are some other types of relationships between the smart contract design patterns that are worth mentioning. Firstly, the patterns “create smart contract” and “deactivate smart contract”, even though they do not always occur together, are both parts of the smart contract lifecycle and are thus connected. And secondly, the design patterns “trading”, “renting” and “auction” are all patterns that concretize the general idea of purchasing in different ways, and as such, there is no evidence in the literature of them ever occurring in combination with each other. Instead, if any, only one of those three patterns is used in an application, thus they can be described as alternative patterns.

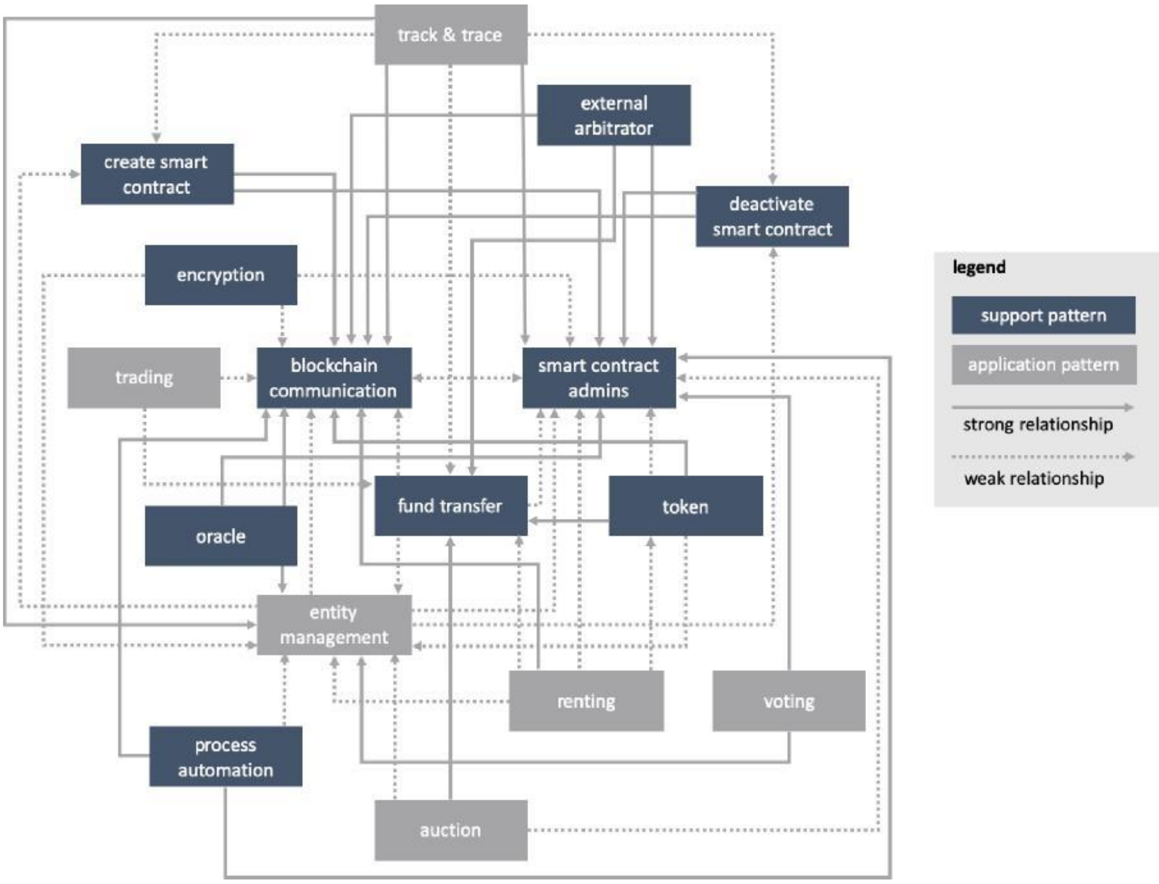

Figure 5. Smart Contract Design Pattern Language

6.6. Discussion

This section will explain the possible impacts of the results of this research by providing theoretical as well as practical implications. Furthermore, some limitations are going to be discussed and suggestions for future research are proposed.

6.6.1. Theoretical and Practical Implications

From the results of this research, several theoretical implications can be deduced. Firstly, by addressing the topic of Blockchain and especially Blockchain smart contracts, a general contribution to a research area that is still very young and in need of further exploration is given. Secondly, by developing smart contract design patterns, the concept of using design patterns for software development is broadened towards the new technology Blockchain. Although a few other research papers have already addressed this topic, none of these papers has created a list of design patterns that are as comprehensive as the one described in this research, based on thorough literature research and not focused on one single Blockchain infrastructure or application area. Thirdly, to develop this list of design patterns, a comprehensive analysis of how design patterns are presented in the software development literature has been conducted to define which structural elements are needed to adequately describe design patterns in the context of Blockchain. And lastly, this research has gone one step further than the existing body of research on smart contract design patterns by creating a pattern language to show dependencies between smart contract design patterns and uncovering which design patterns are best used in combination with other design patterns.

For practitioners, several practical implications can be derived from this research. Firstly, smart contract design patterns can function as a common vocabulary. It enables all stakeholders of a Blockchain application to discuss the application design without needing deep technological knowledge.

Secondly, a standardization in Blockchain development is enabled by providing a catalog of functionalities that smart contracts can provide. By looking through this catalog, application developers gain an overview of smart contract capabilities and can decide on how a certain application can be designed using standardized building blocks. Thirdly, the pattern language can provide developers with insights into how Blockchain applications can be enhanced by using a combination of several design patterns that work well together. Fourthly, using design patterns to structure Blockchain applications can make the maintenance and possible enhancements of those applications easier.

And lastly, although the research field of Blockchain smart contracts is still very young and most implementations are prototypes, the smart contract design patterns presented in this research depict the current best practices regarding the development of smart contracts, so Blockchain application developers can benefit from previous experiences.

6.6.2. Limitations and Future Research

There are a few limitations to the results of this research that have to be mentioned. Firstly, as already explained in the theoretical background, design patterns are subjective. Therefore, the design patterns described in this research are one way to go, but other interpretations of the Blockchain smart contract literature could be possible. Secondly, because the topic of Blockchain in general and specifically Blockchain smart contracts is still very young, the current extent of the literature base is limited. Many research papers have implemented prototypes, but production systems are rare. Therefore, not all Blockchain applications that have been used as input for the development of the smart contract design patterns have been proven successful. Thirdly, most literature concerned Ethereum implementations, Hyperledger Fabric implementations or infrastructure implementations that were not further specified, however, better results might have been attained with additional literature about more Blockchain infrastructures.

And fourthly, the presented pattern language might not comprise all existing relationships between the design patterns because the code samples in the literature are sometimes incomplete and only provide extracts of the smart contract code. Hence, some patterns might have been implemented and might have relationships with other patterns but are not described in the respective research paper and are thus not considered for the pattern language. Similarly, for relationships that include patterns with a limited amount of literature sources, any statements of strong and weak relationships might not be very expressive.

To encounter these limitations, future research should validate the smart contract design patterns in practice and in theory. Firstly, practical research could use the patterns for Blockchain development or take existing Blockchain applications and structure them according to the patterns to achieve better maintainability. Secondly, additional research is needed to identify more research papers as they are published, especially those regarding different Blockchain infrastructures and those offering complete smart contract code. The research could then verify the existing patterns from this work in the literature, create additional patterns and augment the pattern language by identifying further relationships between patterns. For example, although no research papers about pay-per-use applications or smart contracts in DAOs were found during the literature review, these could become important Blockchain use cases and extend the smart contract design patterns presented here. Furthermore, additional relationships between design patterns could include different types of relationships, like specializations, generalizations, sequences, groupings or alternatives of certain design patterns. To become aware of this additional research, a scouting technology could be implemented that automatically detects new suitable literature as it is being published. Thirdly, future research could extend the results of this research by adding a software component to each design pattern and providing sample code in common smart contract implementation languages. And lastly, the research results could be continued even further by implementing a library of secure smart contract design pattern implementations that could be used by developers to create Blockchain applications.

7. Managing Blockchain Systems and Applications: A Process Model for Blockchain Configurations

Table 10. Bibliographical Information for Paper 3

Title	Managing Blockchain Systems and Applications: A Process Model for Blockchain Configurations
Authors	(1) Olga Labazova, University of Cologne (2) Erol Kazan, University of Jyväskylä (3) Tobias Dehling, Karlsruhe Institute of Technology (4) Tuure Tuunanen, University of Jyväskylä (5) Ali Sunyaev, Karlsruhe Institute of Technology
Outlet	Electronic Markets
Publication Type	Journal Paper
Publication Year	2020
VHB-JOURQUAL3	B
Publication Status	Revise & Resubmit

Abstract. Blockchain is a radical innovation with a unique value proposition that shifts trust from institutions to algorithms. Still, the potential of Blockchains remains elusive due to knowledge gaps between computer science research and socio-economic research. Building on information technology governance literature and the theory of coevolution, this study develops a process model for Blockchain configurations that captures Blockchain capability dimensions and application areas. We demonstrate the applicability of the proposed Blockchain configuration process model on four Blockchain projects. The proposed Blockchain configuration process model assists with the selection and configuration of Blockchain systems based on a set of known requirements for a Blockchain project. Our findings contribute to research by bridging knowledge gaps between computer science and socio-economic research on Blockchain. Specifically, we explore existing Blockchain concepts and integrate them into a process model for Blockchain configurations.

7.1. Introduction

It will take years for Blockchain systems to be fully adopted by businesses, but the journey has already begun (Iansiti and Lakhani, 2017). Blockchain is a radical innovation that has the potential to change the business logic for many industries. Blockchain's unique value proposition is the shift from institutional trust towards algorithmic consensus mechanisms (Beck and Müller-Bloch, 2017). Network nodes within the Blockchain systems process and record transactions within so-called blocks (Nakamoto, 2008). Blockchain systems have the advantage of removing single points of failure and improving data integrity and availability in contrast to centralized databases. To leverage the aforementioned features, organizations in different industries (e.g., finance, energy, healthcare) are considering to deploy Blockchain systems to reduce intermediaries, decrease management costs, accelerate business processes, and tap into new revenue sources (Furlonger and Valdes, 2017).

However, current Blockchain projects are more akin to trial-and-error approaches than purposeful information systems development due to a lack of best practices for Blockchain development and unclear long-term business value (Furlonger and Valdes, 2017; Beck and Müller-Bloch, 2017). In other words, most initiated Blockchain projects are prone to failure or inefficient resource allocations. For instance, ninety-two percent of 26,000 Blockchain projects launched in 2016, with a total investment volume of over $1.5 billion, are defunct or indefinitely delayed (Trujillo et al., 2017).

The main reasons for failure are either flawed system designs or incompatible application areas (Risius and Spohrer, 2017). To illustrate, the Jasper project by the Bank of Canada revealed that a Blockchain system for wholesale payments is not competitive compared to centralized systems with regards to its operating costs (Chapman et al., 2017). The example illustrates that narrow-scoped Blockchain prototypes exhibit issues concerning technical scalability, resource efficiency, user traceability, or lacking protection against fraud (Yli-Huumo et al., 2016; Xu et al., 2017).

The existing literature on Blockchain focuses either on technical aspects or use cases (Lindman, Tuunainen and Rossi, 2017; Notheisen et al., 2017). For instance, technical studies explore various consensus mechanisms and cryptographic protocols, predominately focusing on financial transactions as an application case (e.g., Bitcoin). On the other hand, research on Blockchain use cases has focused on business applications such as energy trading (Rutkin, 2016), healthcare (Azaria et al., 2016), or supply chain management (Glaser, 2017; Mendling et al., 2017). However, the aforementioned studies are predominantly idea-driven and exhibit challenges due to a lack of feasible technical solutions (Avital et al., 2016; Lindman et al., 2017; Beck et al., 2017). To develop a successful proof of concepts for Blockchain application areas, research on Blockchain technology (i.e., technical aspects) and Blockchain applications (i.e., business use cases) should be considered conjointly.

We build on information technology (IT) governance literature and apply the theory of coevolution of technologies and application areas[2] (Grodal et al., 2015) as a lens to explore coevolving Blockchain configurations and application areas. Bridging knowledge about the

[2] By the term application areas, we refer to the concept of categories as mentioned by Grodal et al. (2015).

technology underlying Blockchains and their application areas will create conditions for developing successful Blockchain-based systems (Iansiti and Lakhani, 2017).

We explore the current body of Blockchain research and present our model in the form of a process model for Blockchain configurations that captures Blockchain capabilities, that is, routinized, repeatable, and application-specific processes, enabling businesses to transform resources into business value (Ray, Muhanna and Barney, 2005; Tallon, 2007). We answer the following research question: *What application areas are advisable for Blockchain systems and how can Blockchain systems be purposefully configured across application cases?*

To create the Blockchain configuration process model, we systematically developed a taxonomy that groups Blockchain application areas across mutually exclusive Blockchain configurations (Nickerson et al., 2013). The identified Blockchain concepts and their relationships are consolidated in the Blockchain configuration process model, which structures the Blockchain concepts in four categories by semantic features and reciprocal relationships: (1) Blockchain governance, (2) Blockchain application areas, (3) Blockchain properties, and (4) Blockchain deployment. We illustrate the applicability of the proposed Blockchain configuration process model on four selected Blockchain projects.

With this research, we contribute to the extant research on the Blockchain by presenting a more granular and holistic view on identified Blockchain concepts and their relationships. For practitioners, our proposed model offers guidance to managers to identify suitable Blockchain systems and their corresponding application areas before development.

This paper proceeds as follows. In section 2, we discuss the theoretical aspects of IT governance and the theory of coevolution of technologies and applications. In section 3, we outline our three-step exploratory research approach for creating the Blockchain configuration process model. In section 4, we present the Blockchain configuration process model. In section 5, we illustrate the applicability of the Blockchain configuration process model on four Blockchain projects. In section 6, we discuss our findings, implications for theory and practice, and suggest avenues for future research.

7.2. Theoretical Background

7.2.1. IT Governance

IT governance can be defined as a collection of decision rights and accountabilities to encourage desirable behavior in the context of IT (Brown and Grant, 2005). Decision rights represent the governing control aspect over assets, whereas accountabilities capture the monitoring of decision-making processes. Incentives play a vital part in IT governance because they motivate and guide agents to act favorably for specific systems. Overall, the literature on IT governance discusses three basic governance approaches. First, centralized governance includes executive committees for decision-making and is characterized by having centralized business processes, providing control over architectures, and possessing formal assessments and monitoring decisions. Second, a decentralized approach to IT governance requires no or few governance mechanisms for decision-making and insists on local accountabilities (Brown and Magill, 1994; Schwarz and Hirschheim, 2003; Brown and Grant, 2005). Lastly, companies that aim to balance the benefits of centralized and decentralized models follow a hybrid governance approach. These companies establish a centralized group to provide core services while allowing business units to control a portion of the overall functions (Boynton and Zmud, 1987; Rockart, 1988).

7.2.1.1. Blockchain Governance

The most successful Blockchain systems will be those that adapt their governance to the organizational environments for business value creation (Kharitonov, 2017; Beck et al., 2018). Being introduced as a more or less decentralized data management solution, Blockchain systems evolve continuously and are aligned with different IT governance approaches. Beck et al. (2018) specify decision rights as a dimension of Blockchain centralization. Decision-making power can either be concentrated in few governing nodes or distributed equally among all nodes in the Blockchain network. Concerning accountabilities, they differ in their rights to monitor decisions on Blockchain systems, having the ability to adjust actions based on consequences incurred (Beck et al., 2018). In the same vein, different incentive schemes motivate agents to act within Blockchain systems for monetary or non-monetary rewards.

7.2.2. Theory of Co-evolution of Technologies and Applications

The theory of coevolution of technologies and application areas during industry emergence focuses on mechanisms of their continuous coevolution, which starts with a period of divergence and continues with a period of convergence (Grodal et al., 2015). The period of divergence is characterized by high diversity in technology to address emerging application requirements. Technologies evolve and fulfill more application requirements through continuous design recombination. Application areas are influenced by a pool of ready-made technological designs, which in turn satisfy groups of application requirements. The following period of convergence results in consensus among producers concerning efficient technological designs for mature application areas.

The Blockchain domain is currently at an early stage of industry emergence and is characterized by a high diversity of technological designs and potential application areas

(Lindman et al., 2017; Miscione et al., 2018; Schlegel, Zavolokina and Schwabe, 2018). A variety of consensus mechanisms (Karame, Androulaki and Capkun, 2012) and anonymity schemes (Reid and Harrigan, 2013) produce various experimental solutions that are largely unrelated or opaque to emerging Blockchain application cases (Yli-Huumo et al., 2016). Nevertheless, the number of Blockchain application experiments is growing, leading to different Blockchain-based services, such as supply chain management (Glaser, 2017; Mendling et al., 2017), energy trading (Rutkin, 2016), or authentication services (Miscione et al., 2018). In turn, Blockchain application cases are not fully supported by ready-made technological solutions (Risius and Spohrer, 2017). So far, extant research on Blockchain systems yields isolated and unstructured concepts and offers only limited support for configuring Blockchain systems for application areas.

7.3. Research Approach

Our research approach for developing the Blockchain configuration process model comprises three consecutive steps (Figure 6). First, we explore Blockchain concepts and their relationships through taxonomy development based on literature, business reports, and instantiated decentralized applications (Nickerson et al., 2013). Second, we structure the findings in the form of the Blockchain configuration process model. Third, we illustrate the applicability of the Blockchain configuration process model on four Blockchain projects.

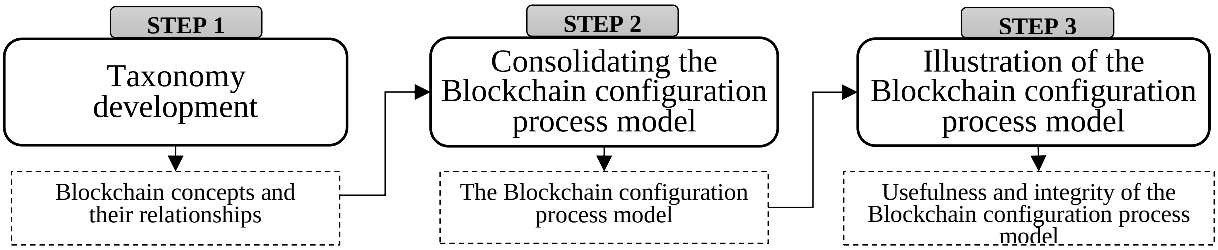

Figure 6. Research Approach. The Blockchain Configuration Process Model

7.3.1. Taxonomy Development

To organize extant knowledge on the Blockchain, we employed the taxonomy development method proposed by Nickerson et al. (2013), who define a taxonomy as a set of dimensions. Each dimension consists of “mutually exclusive and collectively exhaustive characteristics in a way that each object under consideration has one and only one character in every dimension” (Nickerson et al., 2013, p.5). The taxonomy development method proceeds in three stages. In the initial stage, metacharacteristics and ending conditions are defined according to the purposes of the taxonomy to be developed. In the main stage, the taxonomy is developed. Objects to be classified with the taxonomy (in this study, application cases, dimensions, and characteristics) are identified during inductive or deductive iterations. During inductive iterations, empirical cases are analyzed to determine dimensions and characteristics for the taxonomy. During deductive iterations, dimensions and characteristics are derived from the existing scientific knowledge base. In the final stage, the taxonomy is evaluated against ending conditions.

The taxonomy aims to derive and classify Blockchain application areas and dimensions driven by Blockchain characteristics. Therefore, we selected Blockchain characteristics (e.g., consensus mechanism, anonymity level) as a metacharacteristic. The metacharacteristics serve as the basis for the identification of further dimensions and characteristics.

We developed the taxonomy in four iterations. The first three iterations were inductive iterations, where we identified application cases to derive dimensions and characteristics. For each inductive iteration, we used different types of sources: scientific literature, business reviews, and white papers on Blockchain applications, respectively. The fourth iteration was a deductive iteration where we revised the taxonomy based on previous classifications of Blockchain systems. In the first iteration, we searched papers and articles in the web of science core collection[3] with the search string "Blockchain OR distributed ledger" on October 17, 2016, in title, abstract, and keywords, covering the whole period of publications (Webster and Watson, 2002; vom Brocke et al., 2009). The search returned fifty-one papers and articles. After screening the titles and abstracts, we discarded ten papers as non-Blockchain research and coded the forty-one remaining relevant papers and articles. In the first iteration, we identified six dimensions with fourteen characteristics and six application areas with ten application cases. The analysis of the existing scientific literature revealed detailed information on separate Blockchain characteristics (e.g., consensus mechanisms) or specific Blockchain application examples (e.g., energy markets, prediction platforms) but lacked comprehensiveness.

In the second iteration, we analyzed business reports, which provide less precise, but more comprehensive information. We investigated twenty business reports published by national agencies, consulting companies, and international institutions. We revised the taxonomy and added two dimensions, six characteristics, and one application case.

To fill the remaining gaps in the taxonomy, we reviewed eighty-six Blockchain systems and applications (e.g., Bitcoin, Ethereum, Hyperledger) in the third iteration. If possible, we used the applications; otherwise, we read available documentation and white papers. During the third iteration, we added four new application cases.

[3] Used indices: "Science Citation Index Expanded (1900-present), Social Sciences Citation Index (1900-present), Arts & Humanities Citation Index (1975-present), Conference Proceedings Citation Index- Science (1990-present), Conference Proceedings Citation Index- Social Science & Humanities (1990-present), Book Citation Index– Science (2005-present), Book Citation Index– Social Sciences & Humanities (2005-present), and Emerging Sources Citation Index (2015-present)"

The fourth iteration was deductive, where characteristics, dimensions, and application cases from fifteen previous classifications were derived. I have used all previous classifications to identify in extant literature until October 2018. This analysis showed that our taxonomy is consistent with extant Blockchain classifications.

All ending conditions proposed by Nickerson et al. (2013) were fulfilled after the fourth iteration. First, all found Blockchain application cases described in the existing scientific literature or business reports can be classified with the taxonomy. Second, each dimension is unique and mutually exclusive and each character is unique within its dimension. Third, all application cases were classified with a single characteristic for each dimension. Fourth, the taxonomy is concise - consists only of dimensions that classify application cases. Fifth, the taxonomy is robust - differentiates each application case from all others. Sixth, the taxonomy is explanatory, comprehensive, and extensible - highlights the main features of each application case and can be extended when new application cases arise.

7.3.2. Consolidation of the Findings

Based on the taxonomy development, we synthesized the findings into a process model for Blockchain configurations. The model captures characteristics and application areas that are pertinent to Blockchain systems. Specifically, the model is structured by four dimensions, which are distinct by their semantic features and reciprocal relationships: (1) Blockchain governance, (2) Blockchain application area, (3) Blockchain properties, and (4) Blockchain deployment. To synthesize Blockchain concepts and investigate their relationships, we coded the data using three types of coding schemes, open coding, axial coding, and selective coding[4] (Strauss and Corbin, 1990). We applied open coding for the initial categorization of Blockchain concepts; axial coding for removal of overlapping concepts while iteratively testing the Blockchain concepts against the data, and selective coding to identify the relationships between concepts. One researcher coded the sources three times (November 2016, April 2017, November 2017) and another researcher validated the results after each iteration (Strauss, 1987). Disputes were resolved in group discussions.

7.4. The Blockchain Configuration Process Model

Based on a set of known requirements of a Blockchain project (i.e., Blockchain governance, Blockchain application area), the Blockchain configuration process model (Figure

[4] Open coding is a process for grouping categories and subcategories (Strauss & Corbin, 1990, p.12). Axial coding is a process for testing "that categories are related to their subcategories, and the relationships against data" (Strauss & Corbin, 1990, p.13). Selective coding is a process "by which all categories are unified around a 'core' category, and categories that need further explication are filled-in with descriptive details" (Strauss & Corbin, 1990, p.14).

7) supports configuration of Blockchain properties and selection of Blockchain deployment attributes (i.e., processing and settlement of transactions).

The Blockchain configuration process model proceeds in three steps. First, one chooses the suitable governance approach (decentralized, hybrid, or centralized) and the application area (i.e., financial transactions, enforcements, asset management, storage, communication, or ranking) that reflects the requirements of the Blockchain project. Examples of Blockchain applications are located at the intersection of Blockchain governance and application area. Second, the proposed model identifies appropriate Blockchain properties according to the selected application area (e.g., financial transactions). The Blockchain properties are token (equity, utility), customizability (no, fixed, custom), data type (logs, assets), and history retention (whole, updates). Third, the Blockchain configuration process model supports the Blockchain deployment (i.e., processing and settlement) according to the selected Blockchain governance approach (e.g., decentralized). The Blockchain deployment attributes comprise access (i.e., private, public), validation (i.e., permissioned, unpermissioned), consensus mechanism (i.e., proof-of-work, proof-of-stake, Practical Byzantine Fault Tolerance, self-developed consensus mechanism), and the anonymity level (i.e., anonymous, pseudonymous, identifiable).

After finishing the three steps, the Blockchain configuration process model terminates. For complex Blockchain projects that include different Blockchain capabilities, the process can be reiterated.

I. CHOOSE THE BLOCKCHAIN GOVERNANCE. CHOOSE THE APPLICATION AREA.

Application Area \ Blockchain Governance	Decentralized	Hybrid	Centralized
Financial Transactions	Cryptocurrencies; Wealth Storage; Micro-Payments	Cross-Border and Micro-Inter-Organizational Payments	Central-Issued Financial Instruments
Enforcements	Enforcements between Individuals	Inter-organizational Enforcements	Central-Issued Enforcements
Asset Management	Authentication; Ownership; Audit Trails; Access Management	Inter-organizational Asset Management	Enterprise Asset Management
Storage	Decentralized Storage	Not Explored for Blockchain Systems	
Communication	Messengers; IoT Communication		
Ranking	Reputation; Rating		

II. CHOOSE THE BLOCKCHAIN PROPERTIES FOR THE APPLICATION AREA

Application Area \ Blockchain Properties	Token	Customizability	Data Type	History Retention
Financial Transaction	Equity	No	Logs	Whole
Enforcement	Utility	Custom	Logs	Whole
Asset Management	Utility	Fixed	Logs	Whole
Storage	Utility	Fixed	Assets	Updates
Communication	Utility	Fixed	Assets	Whole
Ranking	Utility	Fixed	Logs	Updates

III. CHOOSE THE BLOCKCHAIN DEPLOYMENT ATTRIBUTES FOR THE BLOCKCHAIN GOVERNANCE

Blockchain Governance \ Blockchain Deployment	Access	Validation	Consensus Mechanism	Anonymity Level
Decentralized	Public	Unpermissioned	Proof-of-Work/ Proof-of-Stake	Anonymous/ Pseudonymous
Hybrid	Private	Unpermissioned	Practical Byzantine Fault Tolerance	Identifiable
Centralized	Private	Permissioned	Self-Developed Consensus	Identifiable

Figure 7. The Blockchain Configuration Process Model

7.4.1. Blockchain Governance

The Blockchain configuration process model accounts for different approaches to IT governance—a decentralized, hybrid, and centralized (Brown and Grant, 2005). A *decentralized* approach to Blockchain governance implies that all nodes in the network have decision rights and accountability rights. Bitcoin is an example of Blockchains with decentralized governance. In the Bitcoin network, all participants hold the right to decide on the correct functioning of the system, whereas transparency of the data on Blockchains allows all actors to monitor decisions (Nakamoto, 2008). Collectively governed companies or startups often require decentralized Blockchain governance to spread decision rights and accountabilities among all actors in the network to reduce the network overload.

Blockchains that are governed by a *hybrid* governance approach allow only authenticated and predefined users to monitor decisions. However, once a node is a part of the network, participation in decision-making requires no additional permissions. Ripple is an example of a Blockchain with hybrid governance. In the Ripple network, predefined nodes are trusted organizations that deal directly with each other to support a peer-to-peer financial settlement system (Walsh et al., 2016). A hybrid approach to Blockchain governance is useful for inter-organizational collaboration, where Blockchains keep the network closed to ensure the confidentiality of the information, whereas the decision rights are distributed among all nodes in the network.

A *centralized* approach to Blockchain governance supports Blockchains where nodes (usually only a small number of nodes) that have been authorized to validate transactions require additional authorization to have decision rights. An example of systems with centralized Blockchain governance is IBM (Hyperledger) Blockchains, which support regulatory and supervisory nodes to monitor the system (Hyperledger Architecture Working Group, 2017). Centralized Blockchain governance is useful to support enterprise business projects, where a predefined number of users in the network, usually semi-trusted organizations or individuals, can monitor decisions while only a few nodes have rights to validate transactions.

7.4.2. Blockchain Application Areas

The taxonomy yields six Blockchain application areas, which comprise a total of fourteen application cases. Application areas group application cases with similar semantic features, for instance, usage scenarios, and with similar combinations of Blockchain configurations. The first application area is *financial transactions*, which captures application cases concerned with money transfer and exchange. Anonymous and conventional cryptocurrencies, wealth storage, and micro-payments utilize Blockchains with decentralized governance (e.g., Bitcoin, Prime coin, Name coin, Zcash, Dark coin). Inter-organizational cross-border and micro-financial transactions employ a hybrid approach to Blockchain governance (e.g., Ripple, Stellar). Central-issued financial instruments are deployed on Blockchains with centralized governance. For instance, RSCoin and Fed coin projects (Koning, 2016) may allow federal states to independently launch coins.

The second application area of Blockchains is *enforcement*. Enforcements ensure compliance with laws, regulations, rules, standards, or social norms through application logic (Beck et al., 2018). Blockchain-based enforcements between individuals can, for instance, be developed on the Ethereum platform, which supports a decentralized approach to Blockchain governance. Inter-organizational enforcements usually employ Blockchains with hybrid governance, such as Ripple Codius, which allows executing enforcements between predefined organizations. Blockchains with centralized governance can be useful for the deployment of centrally issued enforcements (e.g., R3 Corda). For example, UK Barclays Bank built a prototype on the R3 Corda platform that translates legal contracts into smart contracts, where all involved parties can monitor (but not decide) on amendments to the original smart contracts (Walsh et al., 2016).

The third application area is *asset management* and concerned with management tasks such as authentication, know your customer services, luxury goods provenance, and control of business assets. The management of off-chain registered assets usually requires decentralized governance of Blockchains. For example, a user can prove the ownership or verify the origin of an asset by keeping their labels on the Bitcoin Blockchain (e.g., Colored Coins). To keep the information confidential, inter-organizational asset management (e.g., Ever ledger) applies hybrid Blockchain governance. For enterprises, Blockchains with centralized governance may be suitable for managing inter-organizational assets. For example, Maersk and IBM introduce Trade Lens, a platform for real-time access to shipping data and shipping documents that utilizes a Hyperledger-based Blockchain.

The fourth application area is *storage* and is concerned with keeping digital assets, such as certificates or music and video files, on Blockchains (Kishigami et al., 2015). Blockchain-based decentralized storage is implemented on Blockchains with decentralized governance because it requires a high number of nodes to distribute the transaction load of the network. For instance, the Storj project leverages shading to split encrypted data (Wilkinson et al., 2014). Blockchains with hybrid and centralized governance seem inappropriate for Blockchain-based storage, because of extensive resource requirements for Blockchain deployment and the availability of effective alternative solutions, such as decentralized storage services (Salviotti et al., 2018).

The fifth application area is *communication*. Messaging and IoT communication can be realized on Blockchains with decentralized governance because the content is intended for mass communication (e.g., Whisper; Unger et al., 2015). Communication systems based on Blockchains with hybrid and centralized governance do not create additional value compared to peer-to-peer messengers such as Telehash, which are used by many decentralized services (e.g., IBM Adept).

The sixth application area is *ranking* with a single application case. Global reputation & rating (e.g., Dennis and Owenson, 2016) is supported by Blockchains with decentralized governance and allows several untrusted participants to create Blockchain-based reputations. Blockchains with hybrid and centralized governance seem inappropriate for ranking, because of the availability of alternative solutions, for example, ranking based on peer-to-peer systems such as Gnutella (Salviotti et al., 2018).

7.4.3. Blockchain Properties

Blockchain properties allow for the configuration of Blockchains according to application areas. We identify four important Blockchain properties. *Token* specify how transactions processed by a Blockchain are represented. Equity tokens capture the transfer of value between parties (e.g., Alice transfers 1 Bitcoin to Bob). Utility tokens are more elaborate and contain more extensive data and application logic. *Customizability* captures a Blockchain's ability to process application logic. No customizability indicates that the Blockchain cannot handle application logic. Fixed customizability supports built-in configurations. If customizability is custom, Blockchains support the processing of application logic provided by users. *Data type* focuses on the type of data shared between Blockchain users. Logs imply an exchange of logs of executed transactions. Digital assets mean that the whole digital assets such as documents, messages, and video or music files, are exchanged. *History retention* ascertains whether the whole Blockchain, starting with a genesis block or only its recent updates is kept and distributed between nodes.

The choice of Blockchain properties depends on Blockchain application areas. Everything that is primarily used for *financial transactions* is based on equity tokens. Financial transactions require no customizability. For example, the Bitcoin scripting language is purposefully not Turing-complete (Walsh et al., 2016). Blockchains for financial transactions exchange logs of executed financial transactions and keep the whole transaction history (Nakamoto, 2008).

Enforcements are based on utility tokens (e.g., company stock ownership) (Beck et al., 2018). Enforcements are customized by smart contracts, which are executed across participants in the Blockchain network (Peters, Panayi and Chapelle, 2015). Enforcements exchange logs of smart contracts and retrieve the whole history of logs for security reasons.

Asset management is based on utility tokens (e.g., data access). Fixed customizability allows users to use built-in configurations. Executed actions under the assets are represented by logs (e.g., access to assets, asset changes), which are continuously kept on the Blockchain.

Blockchain-based *storage* is supported by utility tokens and provides for fixed customizability of Blockchains. Storage Blockchains keep digital assets. To improve the scalability of Blockchains, only recent updates of assets are stored. Users are more interested in the current state of the assets and not in their changes over time.

Communication employs utility tokens, fixed customizability of Blockchains, and the exchange of digital assets in the form of text messages. Blockchains keep the whole communication history (Pureswaran, Panikkar, Nair and Brody, 2015; IBM Adept). However, application cases are far from the production stage.

Ranking uses utility tokens and allows for fixed customizability. Blockchains exchange logs of actions, usually reputation or rating scores, and keeps only recent updates of the transaction history, because outdated votes are not necessary for calculating reputation or rating and can be safely removed from Blockchains (Dennis and Owenson, 2016).

7.4.4. Blockchain Deployment

Blockchain deployment attributes depend on Blockchain governance. We identified four Blockchain deployment attributes. *Access* represents the ability to read and submit data on a Blockchain (Beck et al., 2018). Private access makes a Blockchain available for reading and submitting data only to authorized users. Public access allows everyone to read data from and submit data to a Blockchain. *Validation* indicates different mechanisms for validating transactions on a Blockchain. Permissioned validation means that only authorized users validate transactions and participate in consensus findings. If validation is unpermissioned, all users in the network validate transactions. The *consensus mechanism* is concerned with mechanisms for reaching consensus on Blockchain updates. Proof-of-work requires validating notes to spend resources (or work), usually processor time or storage space. Proof-of-stake requires users to prove the ownership of tokens to establish their stake in the Blockchain. Practical Byzantine Fault Tolerance requires agreement by the majority of validating nodes (2/3 of validating nodes) for transaction validation. Self-developed consensus mechanisms usually include several highly trusted nodes for achieving system-level agreements. *Anonymity level* assesses with what accuracy users can be matched to particular identities. If the characteristic is anonymous, users do not have to provide any identifying information to work with a Blockchain. If the characteristic is pseudonymous, users have to work under a pseudonym. Blockchains with the characteristic identifiable ask for or automatically collect personally identifiable information such as email addresses or IP addresses.

A *decentralized* approach to Blockchain governance implies public access to Blockchains, which allows all participants in the network to monitor transactions. Unpermissioned validation invites all participants to participate in consensus finding. Proof-of-work or proof-of-stake consensus mechanisms ensure the correct functioning of the Blockchain system in a network with a large number of untrusted nodes. Blockchains with decentralized governance support the anonymity and pseudonymity of users.

A *hybrid* approach to Blockchain governance requires private access to Blockchains that makes a Blockchain only available to authorized users. However, unpermissioned validation requires all users in the Blockchain network to participate in consensus finding. The Blockchain network consists of a small number of trusted nodes that make it possible to use energy-efficient but communication-heavy Practical Byzantine Fault Tolerance as a consensus mechanism. Blockchains with hybrid governance frequently ask for name, surname, and email address (e.g., Hyperledger, Ripple) to make users identifiable.

In Blockchains with *centralized* governance, private access allows only authorized users to monitor transactions. Permissioned validation allows only authorized users to validate transactions and participate in consensus finding. Often validating nodes find consensus-based on resource-saving, self-developed mechanisms. Nodes in private permissioned Blockchains must be identifiable and trusted.

7.5. Four Blockchain Projects

We illustrate the applicability and usefulness of the Blockchain configuration process model on four Blockchain projects: (1) DB System & IBM (public mobility), (2) Lit Sonar (academic literature tool), (3) dSCM Tool (data sharing between factories), and (4) Blockchain4openscience.org (portal for researchers).

We selected different types of Blockchain projects that exhibit three different Blockchain governance approaches (i.e., centralized, hybrid, and decentralized) and different application areas to demonstrate its analytical capabilities for identifying common and dissimilar configurations. We conducted four open-ended, semi-structured interviews with leading researchers, solution architects, or leading developers in September and October 2018. Interviews lasted between 46 and 85 minutes with an average duration of 58 minutes. The interviews were transcribed and coded using NVivo software. During the interviews, interviewees applied the Blockchain configuration process model to their projects and discussed the usefulness of the Blockchain configuration process model, Blockchain concepts, and their relationships according to their Blockchain project. Besides, we used secondary data sources to triangulate data and understand the relationship between Blockchain concepts and actual use. We gathered 229 pages of interview transcriptions and secondary data (Table 11).

Table 11. Project-by-Project Evaluation. Data Collection

№	Project	Interviews			Secondary Data	
		Interviewee	**Time (min.)**	**Pages**	**Sources**	**Number of pages**
1	DB Systel & IBM: Public Mobility	IBM Solution Architect	46	9	ibm.com, hyperledger.com, Hyperledger white papers	120
3	dSCM Tool	Leading Developer	51	11	ethereum.org, scientific sources	53
4	Lit Sonar	Leading Researcher	85	15	litsonar.com, scientific sources	33
5	Blockchain 4openscience.org	Leading Researcher	48	9	blockchain4openscience.com, scientific sources	23
Overall			230	58	Overall	229

We demonstrate how the choice of Blockchain governance, application area, Blockchain properties, and Blockchain deployment are consistent and interrelated (Table 12).

Table 12. Overview of Blockchain Projects

№	Project	Blockchain Governance	Application Area	Blockchain Properties	Blockchain Deployment
1	DB Systel & IBM: Public Mobility	Centralized	Financial Transactions	Equity token, fixed customizability, logs, whole history retention	Private access, permissioned validation, Practical Byzantine Fault Tolerance, identifiable nodes
2	dSCM Tool	Hybrid	Communication	Utility & equity tokens, custom customizability, logs, whole history retention	Public & private access, unpermissioned & permissioned validation, proof-of-work, pseudonymous nodes
3	Lit Sonar	Decentralized	Storage	Utility tokens, fixed customizability, digital assets, recent updates	Public access, unpermissioned validation, proof-of-existence, pseudonymous nodes
4	Blockchain4openscience		Ranking	Utility tokens, fixed customizability, logs exchange, whole history retention	Public access, validation is not defined, consequence-based consensus, identifiable nodes

7.5.1. DB Systel & IBM: Public Mobility

DB Systel GmbH (Frankfurt, Germany) is a digital research and innovation business unit within the Deutsche Bahn Group, one of the largest global mobility and logistics companies in Europe (IBM, 2018). As a strategic partnership between IBM and Deutsche Bahn, DB Systel GmbH helps to develop a public mobility solution using Blockchain.

7.5.1.1. **DB Systel & IBM: Public Mobility. Blockchain Governance**

The Blockchain is centrally governed by IBM. The interviewed IBM solution architect stated: *"IBM does not have its Blockchain implementation. We have built-in IBM add-ons for the governance of the Blockchain network on top of Hyperledger open source licenses*."

7.5.1.2. **DB Systel & IBM: Public Mobility. Blockchain Application Area**

The primary focus of the application is financial transactions. DB Systel GmbH wants to provide a single ticket for journeys with different mobility providers. The application enables mobility providers to check the validity of tickets and reimburses them for services rendered in a transparent and immutable way.

7.5.1.3. **DB Systel & IBM: Public Mobility. Blockchain Properties**

Tokens in the application represent tickets. Accordingly, they can be considered equity tokens since their main purpose is to represent the monetary value of the ticket. Tokens offering additional features were not considered by the project. The financial transactions are not customized. However, additional business logic is enforced by smart contracts integrated into the architecture and triggered by ticketing transactions (IBM, 2018). Hence, the application offers fixed customizability. The Blockchain logs all transactions performed with the application. The interviewed IBM solution architect confirmed: "We build solutions of having transactions where the data is small and does not contain, for example, the process-sensitive data." The application stores *the whole transaction history* to keep a record of all transactions performed on the system. The interviewed IBM solution architect specified: "*If you want to have a Blockchain for years and if your asset is critical, then you need the history*."

7.5.1.4. **DB Systel & IBM: Public Mobility. Blockchain Deployment**

The approach to Blockchain governance (i.e., centralized governance) reveals the following Blockchain deployment attributes. Access to the Blockchain is private and available only for authorized users. Mobility providers have an additional (*permissioned*) authentication for being validating members in the Blockchain network and get the split of the revenue. The interviewed IBM solution architect explained: "Users register to an application. Parties, who provide services for the tickets have to be participants in the *Blockchain, or to trust one of the participants*". A variant of Practical Byzantine Fault Tolerance is employed as a consensus mechanism. The IBM solution architect confirmed: "As you are working with private-permissioned *Blockchain, you can do other consensus protocols, which allow you to be simple and more efficient invalidation*." Users are identifiable within the application. The interviewed IBM solution architect specified: "*IBM provides Blockchain for business, for business means that we are looking for a way to have Blockchains with identities*."

7.5.2. dSCM Tool

The dSCM tool is a part of a larger project that aims to provide data sharing in federation clouds between different factories in supply chain management networks, which record and store data from sensors. Each factory and supplier have access to the data in different stages of aggregation.

7.5.2.1. dSCM Tool. Blockchain Governance

The system employs a hybrid *Blockchain governance* approach. The system is built on the public Ethereum Blockchain so that transactions are visible to the general public. The leading developer confirmed: "We rather focus on the level of openness than the level of trust. If we want to have a higher level of trust, we just would set up the network in a different way, with some auditing or monitoring mechanisms". However, the system also integrates the HAWK protocol to delegate sensitive smart contracts to managers. Managers are third-parties that all participants in the respective smart contract trust. Hence, the governance approach constitutes a hybrid form where the Ethereum's decentralized governance approach is extended with an additional layer to maintain the confidentiality of sensitive information.

7.5.2.2. dSCM Tool. Blockchain Application Area

The Blockchain application area is communication. The focus of the system is to enable communication and transparent data exchange between the factories in the supply chain network.

7.5.2.3. dSCM Tool. Blockchain Properties

Utility tokens are employed because the system has to track interactions beyond simple value transactions. However, equity tokens are used as well to pay for smart contract execution. The leading developer explained: *"We use both tokens, equity tokens because of this gas, and utility tokens, because of additional features that are offered, like storing text or smart contracts inside."* The system provides users with an integrated development environment for arbitrary smart contracts to realize additional built-in business logic. Hence, customizability is custom. The system keeps *logs of executed actions* and holds *the whole history* of the actions for security reasons.

7.5.2.4. dSCM Tool. Blockchain Deployment

The tool employs the Ethereum platform because it allows for fast deployment of a proof of concept. Ethereum supports public access to the data on the Blockchain and *unpermissioned validation*. The consensus mechanism is the most challenging part to select while deploying Blockchains. The leading developer stated: *"I have no idea about the consensus mechanism that would be the best. I just stayed with proof-of-work."* The nodes in the system are organizations that want to protect sensitive information from competitors in the network. Currently, the developers are exploring how to keep the parties involved in interactions and the content of transactions confidential from third-parties. To this end, security technologies like mixers or the HAWK protocol are employed.

7.5.3. Lit Sonar

The Lit Sonar project aims to establish a repository for open science/open access publications. Aims of the project are to make open access publications and data sets available to the general public and to ensure their authenticity.

7.5.3.1. LitSonar. Blockchain Governance

The project is going to use a public unpermissioned Blockchain to assure high availability and integrity by allowing for as many validating nodes as possible. Hence, the governance approach is decentralized.

7.5.3.2. LitSonar. Blockchain Application Area

As the infrastructure for open *storage*[5] of the scientific data, the project considers using Blockchain. The leading researcher confirmed: "*Storage is the biggest issue for the project. We believe that Blockchain might be the best option to implement an infrastructure that allows everyone to access knowledge.*" The Blockchain will most likely serve as a trust anchor and facilitator for access management. The Interplanetary File System is currently considered as a decentralized storage medium.

7.5.3.3. LitSonar. Blockchain Properties

The application employs utility tokens because representing scientific literature requires more information than simple transactions transferring monetary values. Customizability is fixed since users are allowed to execute fixed features (e.g., data selection, commenting, and uploading). The Blockchain exchanges digital assets. The system will capture only recent updates of the assets to avoid effort for management of outdated information.

[5] The project is at an early stage and struggles with the technical issues (e.g., scalability) to store more than a pointer to the data but the actual data. The project is working on these issues.

7.5.3.4. LitSonar. Blockchain Deployment

The project requires public access to the Blockchain data. The leading researcher explained: “It (the application) will be one big database where everyone can publish everything.” The system employs *unpermissioned validation* to enable any interested party to contribute to the system. However, scientific libraries are the most likely candidates for operating validating nodes. The considered consensus mechanism is proof-of-existence, a proof-of-work algorithm that builds on the provision of storage capacities instead of computational resources. The leading researcher stated: “You need a working *Blockchain that allows you to make proof-of-existence, giving timestamps for documents to search these verified indexes, which contain verified documents.”* Users are pseudonymous. The leading researcher explained: “Anonymity cannot establish links between papers and users, while identifiability creates privacy concerns.”

7.5.4. Blockchain4openscience.org

The open-source project Blockchain4openscience.org aims to represent extended information about research and researchers—their scholarly works, research interests, and affiliations.

7.5.4.1. Blockchain4openscience.org. Blockchain Governance

The project uses a public unpermissioned Blockchain because everyone should have the right to create and monitor ledgers of the scientific reputation. Accordingly, the governance is decentralized.

7.5.4.2. Blockchain4openscience.org. Blockchain Application Area

Blockchain4openscience.org implements Blockchains for open science in collaboration with openvivo.org, an existing social platform for managing scientific reputation. The project uses various reward mechanisms for the scientific works to generate a scientific reputation (Garcia, Lopez and Conlon, 2018). The leading researcher explained: “Once you have links where data is stored, you can facilitate the mechanism to reach the data and establish relationships across data. By doing that, you generate tokens that are stored in a wallet of the scientific reputation”.

7.5.4.3. Blockchain4openscience.org. Blockchain Properties

The project selected a utility token to avoid generating an economy around data. The leading researcher explained: “*The reputation-based Blockchain; the incentive is not money.”* The Blockchain should support fixed events such as token generation and rely on *the whole* *history* of the transactions[6]. The exchanged data is *logged*, while the real data is stored off-chain. The leading researcher confirmed: *"Yes, right now we are experimenting with IPFS, where we have the actual things for the Blockchain that are represented with a hash."*

7.5.4.4. Blockchain4openscience.org. Blockchain Deployment

Access to Blockchain should be public. The leading researcher explained: "*You have all the assets and basically what you want is to make the data available and public."* The project team had not decided on an approach for transaction validation. The system uses *consequence-based consensus,* which is based on certificated quoting. The users in the system are fully *identifiable* because anonymity does not support managing reputation. Besides, the project uses Open Researcher and Contributor ID (ORCID).

7.6. Discussion

7.6.1. Principal Findings

Based on a method for taxonomy development for deriving Blockchain system characteristics and dimensions (Nickerson et al., 2013), the Blockchain configuration process model represents an analytical tool to assists with the selection and configuration of Blockchain systems based on known requirements (i.e., Blockchain governance, Blockchain application area). The proposed model is particularly useful for decision-makers to derive insights before initiating the development of a Blockchain project, and allows the classification of alternative Blockchain configurations to identify performance differences. In this study, we derived four groups of relationships between Blockchain concepts, which assist with the development of

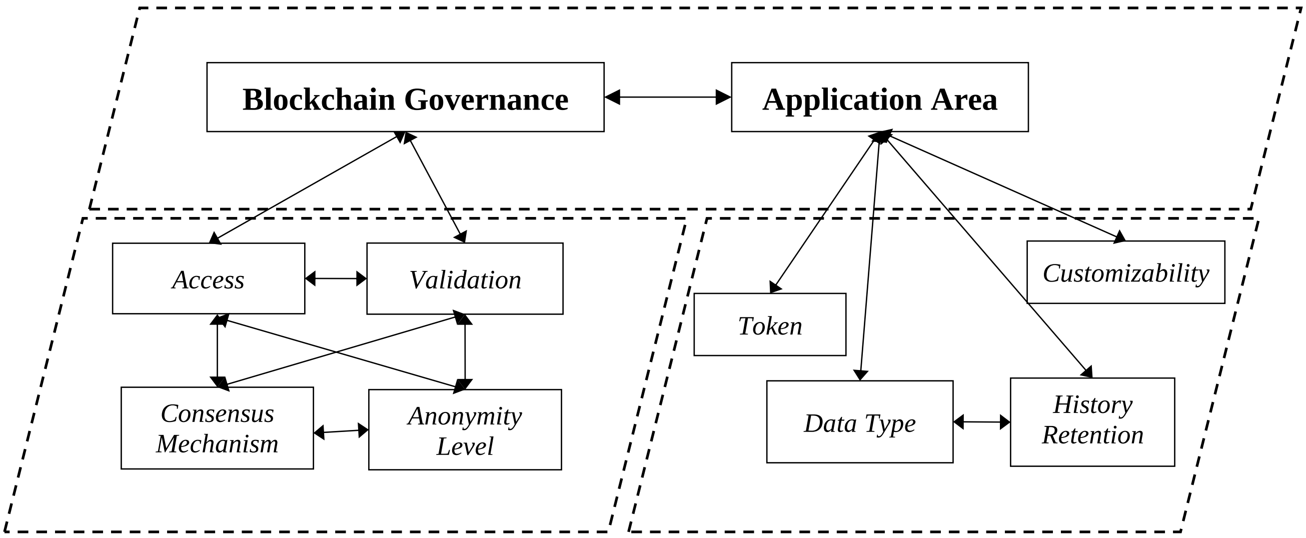

Figure 8. Overview of Blockchain Concepts and their Relationships

[6] The concept of rolling Blockchain was introduced. To keep recent updates, the miners should add a checkpoint to a block, in which all blocks older than some point in time can be safely removed (Dennis and Owenson, 2016).

Blockchain-based systems and consolidates extant knowledge on the Blockchain domain (Figure 8).

7.6.1.1. Relationships between Blockchain Governance and Application Areas

Our exploratory study revealed the interdependencies between Blockchain governance and Blockchain application areas. First, not all Blockchain governance approaches are well suited for all application areas. For instance, the application areas financial transactions, enforcement, and asset management can benefit from all three Blockchain governance approaches. However, application areas such as communication system, decentralized storage, and ranking should be performed on Blockchains with a decentralized governance approach, because operating such systems is resource-intensive and more effective solutions all already available if lesser degrees of centralization is satisfactory (e.g., ranking portals operated by a third party).

7.6.1.2. Relationships between Application Areas and Blockchain Properties

The findings suggest that Blockchain properties (i.e., token, customizability, data type, and history retention) have reciprocal relationships with application areas. To illustrate, equity tokens support financial transactions, while other application areas require tokens with more functionality; thus, they employ utility tokens. Customizability is not required for financial transactions since all required operations can be specified upfront. For enforcements are customizability is custom by design, because smart contracts must be specified. Other application areas employ customizability and provide users with built-in configuration options (e.g., a set of different types of transactions). *The data type* has the property logs for the application areas financial transactions, enforcements, data management, and ranking since only logs of executed actions are exchanged and stored. The application areas storage and communication keep digital assets directly in the Blockchain instead of logging state transitions. History retention is influenced by application areas and data type depending on sensitivity or volume stored in a Blockchain. If larger amounts of data are to be stored in a Blockchain, only recent updates can be retained to prevent the Blockchain from requiring too much storage space. Limited retention of transaction histories is also an option to alleviate confidentiality challenges.

7.6.1.3. Relationships between Blockchain Governance and Deployment

There are relationships between *Blockchain governance* and the attributes regarding *access* and *validation*. A decentralized Blockchain governance approach requires public access and unpermissioned validation because the network can be monitored and set up by all participating nodes. A hybrid Blockchain governance approach supports private access and unpermissioned validation because authorization is required for accessing sensitive data (see dSCM Tool). Lastly, centralized Blockchain governance requires private access to Blockchain systems, because the nodes need to be authorized to read data and perform permissioned validation (Hyperledger Architecture Working Group, 2017).

7.6.1.4. Relationships between Blockchain Deployment Attributes

To support efficiency, trade-offs between Blockchain deployment attributes should be considered. Combinations in the attributes of access and *validation* (public vs. private; permissioned vs. unpermissioned) determine the level of Blockchain decentralization (Walsh et al., 2016; Beck et al., 2018).

Combinations in the attributes of access and *validation* determine the *consensus mechanism* and the degree of anonymity. In Blockchains with public access and unpermissioned validation (e.g., Ethereum), the large number of untrusted nodes require proof-of-work or proof-of-stake consensus mechanisms. Blockchains with private access and unpermissioned validation have a smaller number of trusted nodes; hence, it is feasible to employ the energy-saving but communication-heavy Practical Byzantine Fault Tolerance algorithm. In Blockchain systems with private access and permissioned validation, highly trusted nodes participate in consensus finding based on self-developed rules. The degree of anonymity is influenced by access and validation type due to different requirements for authentication and authorization schemes; for instance, in a permissioned Blockchain users cannot be anonymous by design. Only Blockchain systems with public access and unpermissioned validation (e.g., Ethereum) support anonymity or pseudonymity, because no authentication is required.

Moreover, consensus mechanisms and the degree of anonymity influence each other. Proof-of-work and proof-of-stake support anonymous and pseudonymous nodes. On the other hand, Practical Byzantine Fault Tolerance and self-developed consensus mechanisms/rules require the identification of users to ensure control and trust in private Blockchain systems.

7.6.2. Theoretical Contributions

This study contributes to research in four ways. First, our findings contribute to the theory of IT governance in the context of Blockchain systems based on three IT governance approaches. Decentralized Blockchain governance is suitable for collectively governed companies or startups to spread decision rights and accountabilities among all actors (i.e., nodes) in the network. Hybrid Blockchain governance is useful for inter-organizational collaboration to ensure confidentiality while sharing decision rights among all nodes in the network. Lastly, a centralized Blockchain governance approach is useful to support enterprise business projects where a predefined number of users can monitor decisions while only validating nodes have decision rights.

Second, previous research on Blockchain proposes concepts of interest to computer science (Glaser and Bezzenberger, 2015; Walsh et al., 2016; Yli-Huumo et al., 2016; Bartoletti and Pompianu, 2017) and business applications related concepts (Salviotti et al., 2018), but falls short in exploring their relationships. Our study bridges prior research by offering clearer conceptualizations for the identified concepts and their relationships. As such, the identified relationships (i.e., governance, application areas, properties, and deployment) bridge knowledge gaps between computer science and the socio-economic literature on the Blockchain.

Third, the identified Blockchain properties (i.e., token, customizability, data type, and history retention) are important attributes for configuring Blockchain systems, which, however, have received only a little attention in the literature.

Last, we establish an overview of Blockchain application cases and more abstract Blockchain application areas. Application areas group application cases with similar characteristics (e.g., usage scenarios) and similar combinations of Blockchain characteristics.

7.6.3. Practical Contributions

Our research contributes to practice in three ways. First, our proposed Blockchain configuration process model guides the design of Blockchain-based information systems before development. The model establishes an overview of best practices for Blockchain applications and organizes them according to their configurations. This is particularly useful for practitioners to identify promising Blockchain projects and assess risks before their implementations.

Second, we highlight the hybrid governance approach, besides the widely-known decentralized or centralized ones. For many application cases, organizations may consider Blockchain implementations with hybrid governance that store information in a more confidential but still more decentralized fashion (e.g., Ethereum with the Hawk framework).

Third, we provide an overview of application cases and areas beyond the financial sector, which is still the focus of the majority of current Blockchain projects. For example, the entertainment industry may use Blockchain-based data management to monitor the use of media content for billing purposes and to prevent copyright infringements.

7.6.4. Limitations

This study is not without limitations. First, due to our focus on Blockchain governance (Beck et al., 2018) and coevolution of technology and application areas (Grodal et al., 2015), we do not consider other socio-economic concepts; therefore, Blockchain concepts and their relationships can be enriched with different socio-economic concepts.

Second, the identified application areas do not directly capture more complex services such as prediction markets or crowdsourcing platforms; instead, we decided to break complex application cases down into the basic functionalities that can be performed by Blockchains.

Third, we identified several application areas proposed in scientific and business sources, which would be invalid within the scope of the Blockchain configuration process model (e.g., private Blockchains that use proof-of-work consensus mechanism and, thus, unnecessarily waste resources). Such examples were purposefully disregarded for the design of the Blockchain configuration process model because they seem unreasonable for commercial use.

7.6.5. Future Research

There are three promising areas for future research. First, exploratory research could replicate our three-step research approach with different scientific and business sources to falsify or corroborate our findings. Besides, the identification of further Blockchain configurations and application areas would broaden the applicability of the Blockchain configuration process model. For example, the addition of a dimension data structure with the two characteristics blocks and graph would make the Blockchain configuration process model also applicable to ledgers based on directed acyclic graphs (e.g., Otte, de Vos and Pouwelse, 2017) that may replace certain Blockchain architectures in the future for some application cases, for example, in the internet-of-things with its scarce resources.

Second, research focused on other socio-economic concepts, for example, market regulations in different countries or implementation and management strategies of Blockchain-based information systems will be useful to contextualize the Blockchain configuration process model for different industries and domains. For example, interoperability of Blockchain-based systems and other information systems is constrained by industry-specific or country-specific data protection regulations such as HIPAA in healthcare (Mercuri, 2004; Sunyaev, Leimeister, Schweiger and Krcmar, 2008) or the GDPR in the European Union (The European Parliament and The European Council, 2016). Third, studies in different industry contexts would allow development measurements and performance indicators that are pertinent to Blockchain systems. This, in turn, would reduce the existing uncertainty about the real business value of Blockchain systems (Notheisen, Hawlitschek et al., 2017).

7.7. Conclusion

Blockchain is an emerging technology with largely untapped potential for the enhancement of many aspects in the information systems domain. Currently, research streams on Blockchain remain largely disconnected, which prevents further development of Blockchain industries and hinders the integration of Blockchain-based information systems into the business landscape. Based on the theory of IT governance and the theory of coevolution of technologies and application areas during industry emergence (Grodal et al., 2015), our work consolidates knowledge on Blockchain governance, application areas, Blockchain properties, and Blockchain deployment attributes in the form of the Blockchain configuration process model. This research contributes to the literature by clarifying the concept of Blockchain governance, a summary of generic Blockchain application areas, and highlighting new concepts that complement existing Blockchain literature. Overall, the Blockchain configuration process model captures Blockchain capabilities based on the current state of knowledge on the Blockchain. Simultaneously, it serves as a foundation for future research exploring Blockchain integrations into the business landscape.

8. Towards a Framework for Evaluation of Blockchain Implementations

Table 13. Bibliographical Information for Paper 4

Title	Towards a Framework for Evaluation of Blockchain Implementations
Authors	(1) Olga Labazova, University of Cologne
Outlet	International Conference on Information Systems
Publication Type	Conference Proceedings
Publication Year	2019
VHB-JOURQUAL3	A
Publication Status	Published

Abstract. Organizations appear to implement Blockchain solutions based on fear of missing out instead of a clear understanding of Blockchain usefulness. Ninety percent of current Blockchain projects do not need a Blockchain to meet their requirements. Therefore, we employ a Design Science Research approach to develop a framework for the evaluation of Blockchain implementations. The framework incorporates common factors of Blockchain decisions, including Blockchain innovation, Blockchain design, inter-organizational integration, and implementation environment. We contribute to the scientific literature by structuring previous research efforts in a four-step framework, which provides a fruitful ground for future conceptual

and empirical studies. For practitioners, the framework is useful to identify Blockchain projects that facilitate purposeful Blockchain adoption.

8.1. Introduction

Blockchain is an intriguing technology that promises to transform agreements, processes, businesses, and financial models into digital code that is stored and shared in immutable, distributed ledgers, and identified and validated by cryptographic signatures (Beck et al., 2016). Blockchain may redefine companies and economies by relying on distributed networks of users, which can change enterprise architectures and affect the ways companies generate value. At least one innovative Blockchain-based business is expected to be worth $10 billion by 2022 and the value may grow to $3.1 trillion by 2030 (Furlonger and Valdes, 2017).

Organizations have an interest in Blockchains to reduce costs, accelerate existing processes, facilitate data exchange with partners, and achieve new revenue sources. However, current Blockchain implementations are often motivated by fear of missing out instead of an understanding of Blockchain usefulness (Furlonger and Valdes, 2017). As with many projects based on new technologies, Blockchain projects are motivated by political problems within organizations (e.g., how to satisfy a chief executive officer) or aim to improve the image of a company. The long-term business value of Blockchains often remains an afterthought. As a result, ninety percent of current Blockchain projects either do not need Blockchains to meet their requirements or result in Blockchain solutions not suitable for implementation in their current IT infrastructure (Furlonger and Valdes, 2017).

Blockchain design components and business outcomes differ from traditional technologies and business models because the infrastructure is decentralized and relies on peer-to-peer information exchange, the business value is collectively generated by nodes, and cooperation on intra- and inter-organizational levels are required to fully leverage the technology (Beck and Müller-Bloch, 2017). For Blockchains to be implemented in existing ecosystems, many factors of IT infrastructure, inter-organizational governance, and societal interactions should be considered simultaneously (Glaser, 2017). For example, the application of Blockchains requires the consideration of technical Blockchain limitations (e.g., delay in recording transactions) and performance metrics of different Blockchain designs (Walsh et al., 2016; Xu et al., 2017). At the same time, the requirements of interoperability of Blockchains with other systems, user behavior, and regulations can affect the outcomes of Blockchain projects (Peters et al., 2015; Schlegel et al., 2018). The absence of a holistic framework to evaluate Blockchain implementations leads to misunderstandings of the core purposes of

Blockchains, mismatches between Blockchain design components, failures in interoperability with existing IT solutions, and confusions regarding future visions of technology (Furlonger and Valdes, 2017).

In the context of this debate, the objective of the paper is to gather technical and managerial knowledge of Blockchains and operationalize them in a framework for evaluation of Blockchain implementations. We answer the research question: *What are the common factors of Blockchain decisions to evaluate Blockchain implementations and how do these factors interconnect with each other?*

This study follows a Design Science Research (DSR) approach (Hevner et al., 2004). For data collection, we use the scientific literature that helps us to arrive at a set of Blockchain evaluation factors. Based on IT artefacts in the Blockchain domain, we organize the resulting factors in a framework for evaluation of Blockchain implementations with four semantic categories: Blockchain innovation, Blockchain design, inter-organizational integration, and implementation environment. We evaluate the framework by interviewing experts and showcase the applicability of the framework on the Brooklyn Microgrid project (Lacity, 2018; Mengelkamp et al., 2018).

The study contributes to the scientific literature by synthesizing and operationalizing previous research efforts in a framework for evaluation of Blockchain implementations. Besides, the framework by itself is a contribution of the paper. Practitioners can use the framework to understand the main factors of success or failure of Blockchain implementations beforehand.

We structure the paper as follows. We start with a Blockchain background and highlight the importance of DSR for the Blockchain domain. Next, we outline our DSR methodology. Then, we present the developed framework. Further, we showcase the applicability of the framework on the Brooklyn Microgrid project. Then, we discuss principal findings, implications for theory and practice, limitations of our study, and areas for future research. We conclude the paper with a brief outline.

8.2. Blockchain Background

Blockchain was introduced by Satoshi Nakamoto in 2008 as the Bitcoin Blockchain — a common transparent, global, and openly-accessible asset ledger that keeps the history of financial transactions between members of a decentralized peer-to-peer network (Nakamoto, 2008). Over time, other Blockchain types emerged that differ in approaches to Blockchain governance (Table 14).

Public permissionless (Bitcoin) Blockchains are fully decentralized Blockchains where everyone can read, write, and validate information (Beck et al., 2018). Such Blockchains are useful for applications with a large number of untrusted participants where no restriction on access and no authentication for validation are required. Public permissionless Blockchains require proof-of-work consensus mechanisms or proof-of-stake consensus mechanisms to achieve agreements on system updates. Application examples are cryptocurrencies, where participants do not have to trust each other but the Blockchain itself (Nakamoto, 2008).

Public permissioned Blockchains are more centralized Blockchains, where only authenticated and pre-defined users can read and write transactions. However, all nodes in the network participate in consensus finding. Participants determine consensus mechanisms. Organizations consortia (e.g., Ripple) are examples of public permissioned Blockchains, where pre-defined nodes in the network are trustful organizations and deal directly with each other to support a peer-to-peer transaction exchange (Walsh et al., 2016).

Private permissioned Blockchains are fully centralized Blockchains where access authorization does not entail validation permissions, which require additional authorization rights usually given only to a small number of nodes. The nodes that have been authorized to read the data, also need to be authorized to broadcast transactions. In private permissioned Blockchains, several highly trusted nodes participate in consensus findings (e.g., practical Byzantine fault tolerance) based on resource-saving. Usually, enterprises employ private permissioned Blockchains (e.g., Hyperledger) for their implementations.

Private permissionless Blockchains are not applicable. Applications are not identified (Beck et al., 2018).

Table 14. Existing Blockchain Types

Blockchain Types	Description	Applications
Public Permissionless Blockchains	Everyone can read, write, and validate the information. The consensus is enforced by proof-of-work or proof-of-stake. Users are usually anonymous and pseudonymous.	Cryptocurrencies (Bitcoin)
Public Permissioned Blockchains	Only authenticated and pre-defined users can read and write transactions. All nodes participate in consensus finding. Identifiable nodes determine consensus mechanisms.	Organizational consortia (Ripple, R3)
Private Permissioned Blockchains	Access authorization does not entail validation permissions, which require additional authorization rights given to several nodes. Consensus (e.g., practical Byzantine fault tolerance) is enforced by trustful nodes.	Enterprise projects (Hyperledger)

Taxonomies and topologies classify other Blockchain design components including tokens, oracles, and programming languages. For the sake of brevity, we refer to Glaser and Bezzenberger (2015), Xu et al., (2017), Oliveira, Zavolokina, Bauer and Schwabe (2018), Tönnissen and Teuteberg (2018), and Labazova et al., (2019) for a more elaborated description of Blockchain design components.

8.3. Design Science Research in the Blockchain Domain

In the last years, interest in Blockchain moved far beyond Bitcoin. The financial sector and other sectors investigate Blockchain proofs-of-concept prototypes. For example, a Blockchain prototype for financial transactions can replace a trust-based coffee shop payment solution (Beck et al., 2016). Automatic execution of Blockchain-based financial contracts can move from natural languages towards formal languages of smart contracts (Elsman et al., 2017). Cross-organizational workflow management in a German bank case can run on Blockchains (Fridgen et al., 2018). Besides, Blockchain prototypes can reduce costs of know-your-customer verification processes and revolutionize loyalty programs (Wang et al., 2018). In the public sector, Blockchain prototypes aim to overcome the double taxation of investors on dividend payment and move land records from paper to Blockchain (Hyvärinen et al., 2017). Public healthcare can benefit from managing medical records on Blockchains, improve precision healthcare, and audit the healthcare value chain to improve patient outcomes. For the energy sector, the most investigated implementation is an electric vehicle and their integration into microgrids (Albrecht et al., 2018; Beinke et al., 2018; Mengelkamp et al., 2018). Logistic explores the prototype to turn central documents in shipping (e.g., the Bill of Lading) into smart contracts on Blockchains (Naerland et al., 2017). Other Blockchain proofs-of-concept enable the automated transaction of real-world assets such as diamonds (Loebbecke et al., 2018). For social businesses, Blockchain is a basic technology of crowdlending platforms and social networking practices (Schweizer et al., 2017; Ciriello et al., 2018).

Different from particular proofs-of-concept, conceptual frameworks guide the integration of Blockchain implementations in industries and markets. The core idea of the proposed frameworks is the focus on multiple layers of Blockchain technology and its environment (Glaser, 2017). For example, the Blockchain market engineering approach introduces macro elements of Blockchain-based platforms and surrounding factors (e.g., legal, social and economic constraints) that is a basic macro layer for the infrastructure layer (Notheisen, Hawlitschek et al., 2017). The infrastructure layer implements the Blockchain protocol that specifies the basic elements of Blockchain system designs including distributed database, consensus mechanism, and cryptographic protocol. The infrastructure layer, in its turn, influences application logic of implementations and is the foundation of the microeconomic design. Based on these realized applications, one can analyze the social factors and individual user behavior in decentralized networks.

Other process-based tools investigate dynamics of Blockchain implementation (Beck and Müller-Bloch, 2017; Albrecht et al., 2018) or propose methods for developing Blockchain use cases (Fridgen et al., 2018). Topologies and classifications of the Blockchain-related concepts (e.g., cryptocurrencies) investigate the factors of the affected markets, such as the potential for disruption and competitive pressure (Kazan et al., 2014). Ontologies and typologies of Blockchain business networks formalize the concepts and properties to describe the integral parts of Blockchain business models and values (Rückeshäuser, 2017; Seebacher, 2018). Managerial studies derive sets of business factors for implementing Blockchains (Lacity, 2018; Mengelkamp et al., 2018). Also, there are classifications of new Blockchain-caused phenomena, for example, Tokenomics (Fridgen et al., 2018; Oliveira et al., 2018). Different frameworks of governance in the Blockchain economy and decentralized autonomous organizations (DAO) arouse interest (Beck et al., 2018; Ziolkowski et al., 2018). For the detailed description, we refer to the original research projects.

8.4. Methodology

This study follows a Design Science Research approach that guides developing IT artefacts and their use in practice (Hevner et al., 2004; Peffes, Tuunanen, Rothenberger and Chatterjee, 2008). Developing IT artefacts should be relevant to the domain of interest and grounded in the previous knowledge base, while the design and evaluation of the solution happen iteratively. To develop a framework for evaluation of Blockchain implementations, we achieved relevance with investigating shortcomings of Blockchain implementations and rigor with knowledge of Blockchain technology, best practice of real-world Blockchain implementations, and IT artefacts in the Blockchain domain. To strengthen the quality of our artefact, we utilized DSR methodology for information systems research (Peffers et al., 2008),

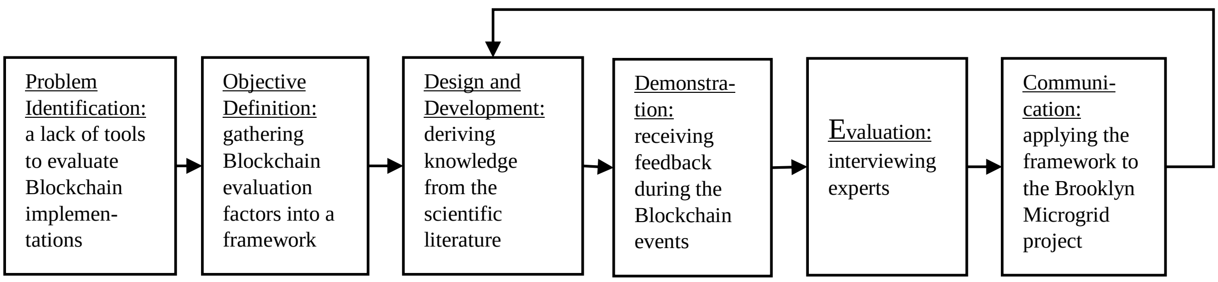

Figure 9. Methodology. The Framework for Evaluation of Blockchain Implementations

which comprises six steps: problem identification, objective definition, design and development, demonstration, evaluation, and communication (Figure 9).

8.4.1. Problem Identification

The Blockchain domain is at an early stage of development and is concerned with a lack of defined tools to guide the evaluation of Blockchain implementations. That results in a high number of unsuccessful Blockchain implementations (Labazova et al., 2019).

8.4.2. Objective Definition

To explore the potential use of our framework, we asked experts in casual talks whether the solution is needed. The authors systematically attended thematic Blockchain events to come up with the objectives of the solution.

8.4.3. Design and Development

We iteratively designed and refined our solution based on incoming data.

8.4.3.1. Data Collection

We conducted a literature review to uncover the Blockchain evaluation factors in previous research. We searched for peer-reviewed journal articles and conference proceedings (e.g., taxonomies, frameworks) on Blockchain and related topics (e.g., distributed ledger) to identify important aspects of Blockchains. We searched with the search string ("Blockchain" OR "distributed ledger") AND ("framework" OR "taxonom*" OR "topolog*") on March 1st, 2018, in title, abstract, and keywords, covering the whole period of publications. We read the abstracts of the articles and focused on articles that describe the factors for Blockchain design and adoption. Next, we performed a backward search to identify relevant papers. Further, we systematically updated our search after March 1st, 2018 with a search string "Blockchain" OR "distributed ledger" for the journals and conferences affiliated by the Association of Information Systems to follow the rapidly developed Blockchain knowledge base. Overall, we identified fifty-one conference papers and journal articles relevant to the factors of Blockchain implementations and DSR tools in the Blockchain domain (Appendix A).

8.4.3.2. Data Analysis

For data analysis, we first applied open coding for the initial categorization of Blockchain concepts and then axial coding for removal of overlapping concepts while iteratively testing the concepts against data (Strauss and Corbin, 1990). We also coded the theoretical foundations that were used to delineate and structure interconnections between factors. Next, we aggregated the factors in broader categories and counted the number of papers and expert statements on the Blockchain evaluation factors and their interconnections

(Appendix A). Interconnections between concepts were identified based on the semantic influence of one concept on another. Interconnections reported in scientific texts and interviews were coded along with descriptive information, such as the text excerpts from which interconnections were derived. One researcher coded the sources twice in spring/summer 2018 and winter/spring 2019 for the initial coding and validation of the results (Strauss and Corbin, 1990). Disputes were resolved in discussions.

Finally, we translated the data into a framework for evaluation of Blockchain implementations by semantically grouping the factors in four categories—Blockchain innovation, Blockchain design, inter-organizational integration, and implementation environment. The groups arose in semantic similarities and are based on related artefacts (Notheisen et al., 2017). Afterwards, the four categories were aligned with four main evaluation steps that guide the evaluation of Blockchain implementations.

8.4.4. Demonstration

We demonstrated the developed framework during the scientific conferences, consortiums, and other thematic events with a Blockchain-friendly audience.

8.4.5. Evaluation

To evaluate our results, we conducted a first set of interviews (seven semi-structured interviews) in April and May 2018. We searched for experts in different fields including computer science, finance, and social sciences because our results cover broad aspects of Blockchains. Interviews were held face-to-face, via Skype, and telephone and lasted on average 74 minutes. Interviewees have an average work experience of eight years and were on average engaged in three Blockchain projects. We used the interview guide. We initially discussed with interviewees the factors suitable for evaluation Blockchain implementations and, then, we showed the first versions of the developed framework. The interviewers followed the framework while consequently discussing the proposed Blockchain evaluation factors and their interconnection. The interviews were transcribed and coded using NVivo software. Overall, we gathered ninety-eight pages of interview transcriptions.

After, we revised the framework according to the interviews and the new scientific literature. Therefore, we asked the same experts for phone or e-mail feedback on the new versions. All experts provided the following feedback.

8.4.6. Communication

We communicated the developed framework back to the knowledge base by showing the applicability of the framework on a randomly chosen Blockchain implementation.

Randomization ensures a generalized abstraction of the framework, which should evaluate any Blockchain implementation. For these purposes, we had a hat with the titles of known Blockchain projects. The first author took out the piece of paper, which stated: "the Brooklyn Microgrid" (Albrecht et al., 2018; Lacity, 2018; Mengelkamp et al., 2018). Afterwards, we screened the secondary sources of the Brooklyn microgrid project available online including the project website, published scientific papers, and other sources. Overall, we investigated more than 100 pages of secondary data.

8.5. The Framework for Evaluation of Blockchain Implementations

Figure 10 shows a framework for evaluation of Blockchain implementations. The framework uses the requirements of the implementations as and inputs to provide users with an evaluation of Blockchain implementations as an output. The framework does so by guiding the user through four steps: *Blockchain innovation, Blockchain design, inter-organizational integration*, and *implementation environment.*

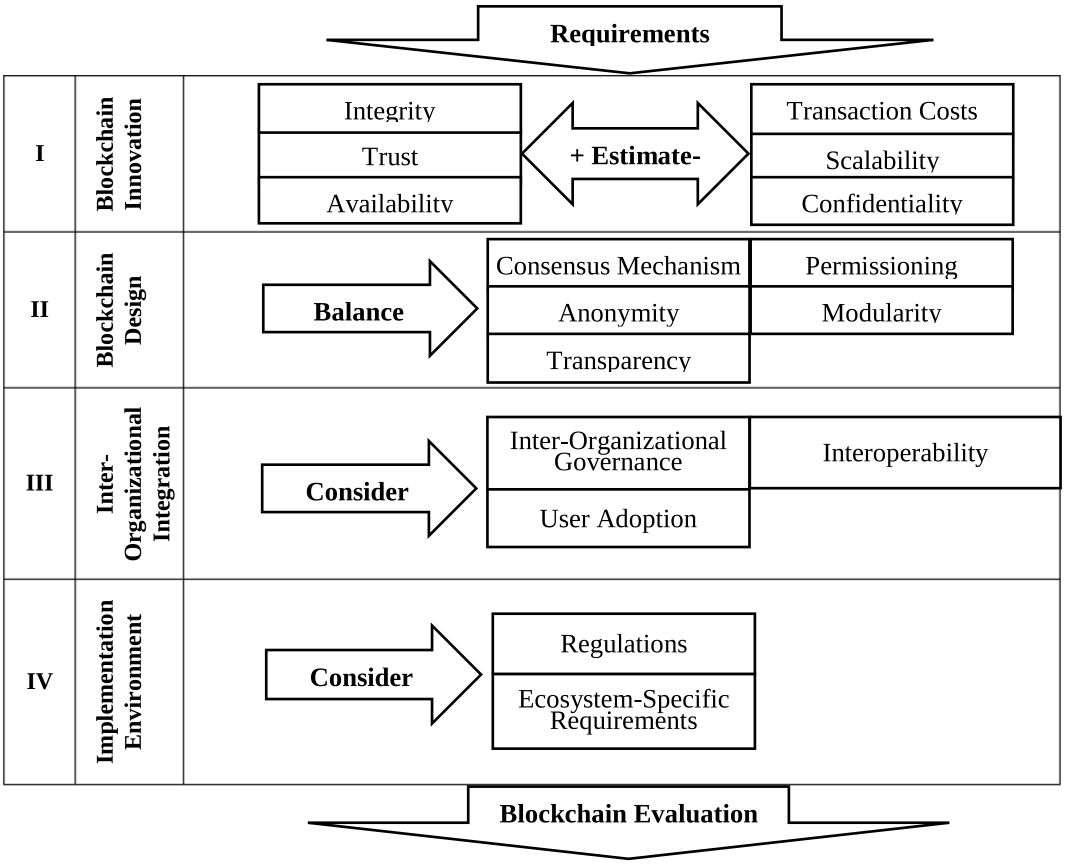

Figure 10. The Framework for Evaluation of Blockchain Implementations

8.5.1. Blockchain Innovation

First, an estimation of the Blockchain's suitability for implementations is required. The category Blockchain suitability includes six factors that represent benefits or challenges for the specific Blockchain implementations.

Integrity ensures that information is protected from unauthorized modifications, that is, its original state is preserved (Wüst and Gervais, 2018). Implementations can benefit from the data integrity of Blockchains to audit the validity and prove the immutability of an entire history of transactions that are consistent between nodes in the network (Glaser, 2017). Increased *network protection against fraud* is achieved through the removal of any central point of failure and increasing the number of nodes. To be attacked, a malicious actor requires 51% of the network power (Yli-Huumo et al., 2016), which is difficult to achieve in large networks with a high number of competitive nodes. Immutability of the ledger can support implementations that require storage of data off-chain (e.g., to verify that data in a cloud remains unchanged). However, there are several ways to manipulate Blockchains, for example, using arbitrage bots, who exploit inefficiencies in decentralized networks, paying high transaction fees, and optimizing network latency (Daian et al., 2019).

Blockchains can provide **trust** in a network of selfish and possibly corrupt agents by replacing any central managing point with cryptographic proofs (Nakamoto, 2008). Smart contracts provide additional functionality to Blockchain transactions by ensuring that pre-defined agreements between users are kept without the need of intermediaries (e.g., lawyers). Smart contracts can be useful to enforce policies, for example, "triggering smart contracts that prevent everyone from sharing a damaging file" (I2).

Availability measures the probability of a system being accessed when needed (Xu et al., 2017). In Blockchain systems, availability is offered through data replication across nodes (Wüst and Gervais, 2018) that decreases "the probability that every node is shut off and the data is gone" (I7). In centralized systems, availability is generally achieved through replication on different physical servers and backups, which is a more expensive solution for most implementations (Wüst and Gervais, 2018).

Blockchain execution relies on **transaction costs** (or fees) in the form of tokens that represent internet-based value (Glaser and Bezzenberger, 2015) to reward nodes for the processing of transactions. *Token commoditization* refers to mapping tokens with assets so that Blockchain transactions may be used in a variety of different contexts. If tokens are not used as assets, there is no common language to integrate Blockchains into organizational workflows and with other systems (I5). There are two predominant types of tokens that have different levels of commoditization: *equity tokens* and *utility tokens*. Equity tokens are in the form of coins (e.g., Bitcoin) and aim for high commoditization. Utility tokens are not monetized and represent more specific assets (e.g., parts of a company). As Blockchains operate in closed networks (Glaser, 2017), tokens are subject to *the volatility of costs* because token (e.g., cryptocurrency) markets can change fast and dramatically. Besides, one should have the possibility to withdraw tokens from the system.

Scalability refers to the ability of Blockchains to handle an increasing amount of workload. The network size of Blockchains needs to be scalable enough to satisfy the demands of the implementation environment. For example, Blockchains for electronic medical records should scale to allow all stakeholders to participate in the Blockchain-based information exchange. Throughput is the number of transactions that can be successfully delivered and validated over the network in a fixed period (Yli-Huumo et al., 2016). When the frequency of transactions in Blockchain increases, the throughput of the Blockchain network needs to be capable of validating submitted transactions with minimum latency. Transaction size represents the amount of data stored in a single transaction. The number of transactions included in each block is limited by the bandwidth of nodes participating in the network (e.g., bandwidth per Bitcoin block is one megabyte) and the defined block size (for Bitcoin, on average 500 transactions in one block) (Xu et al., 2017). *Latency* is the time between submission and secure integration of a transaction into a Blockchain after a certain number of subsequent blocks. For Bitcoin, latency is near one hour with a 10-minute block interval and confirmation after 6 blocks; for Ethereum, it is close to three minutes with a 14-second block interval and confirmation after 12 blocks (Xu et al., 2017).

Confidentiality is defined as the protection of information from unintended disclosure. Data encryption provides for confidentiality on Blockchains. For example, in the Bitcoin network, all transactions are publicly visible and user confidentiality can be damaged. Though, Monero and Zcash employ advanced cryptographic constructions to protect the confidentiality of users.

8.5.2. Blockchain Design

Blockchain designs aim to minimize losses and maximize the benefits of Blockchains according to project requirements. The first and main factor is **consensus mechanism** which ensures that only valid and unique transactions are added to Blockchains (Walsh et al., 2016). There are three predominant consensus mechanisms. *Proof-of-work* requires resources from a miner (e.g., processing time) to produce a computationally difficult piece of data. *(Delegated) proof-of-stake* distributes the ability to create a new block depending on the user’s stake in the system. Practical Byzantine fault tolerance gathers individual decisions made by trusted nodes in a network that together determine system-level agreements. "This consensus part is the hardest one when design Blockchain because that will impact everything else. You make the ground decision here concerning the consensus mechanism, and it is hard to change it later. The right choice of consensus is to move from thinking about design to thinking about implementation" (I2).

Anonymity of users assesses with what accuracy users can be matched to particular identities. For example, users are pseudonymous in the case of Bitcoin and anonymous in the case of Zcash, while in business Blockchain networks users are often identifiable (e.g., Hyperledger). The anonymity of users is considered according to project requirements. "If you are thinking about existing Blockchains for clinical data, they favour anonymity. But if you are thinking in terms of a pharmaceutical company, you need to de-anonymize users at some point" (I2).

Transparency represents whether information or data on Blockchains can be accessible (Yli-Huumo et al., 2016). The *transparency of the Blockchain network* provides a degree of control to end-users concerning the software they run. In some scenarios, involved processors can operate as black boxes and do not reveal the way they came to specific results (e.g., Oracles): the operations are processed off-chain and the outcomes are published on-chains. However, this contradicts the original understanding of how Blockchains function. Transparency of transactions represents a degree of openness of data on Blockchains. Public Blockchains have no restrictions on reading Blockchain data; private Blockchains limit access to Blockchain data to predefined users (Walsh et al., 2016). If the transparency of transactions is public, anyone can extract the transaction history and retrieve sensitive information (Walsh et al., 2016). For example, for sharing economies, transparency can predict signals and, therefore, predict the economy; for "clinical records, the transparency is harmful because one has to comply with the law first" (I2).

Permissioning identifies whether all users can participate in the network or the participation is restricted to a small community. Permissioned Blockchains restrict transaction processing to predefined nodes, while *permissionless* Blockchains have no restrictions on identities of validating nodes (Walsh et al., 2016). For implementations, differences arise when the solutions target external communication with customers (e.g., online services) or Blockchains are used to manage inter-and intra-organizational processes (e.g., supply chain management).

Modularity of Blockchains may be necessary to separate different types of transactions stored on a Blockchain to reduce the complexity of the system or improve scalability. Side-chains enable assets to be transferred between multiple Blockchains. This gives users access to new systems using the assets they already own (Xu et al., 2017). By reusing assets, these systems can interoperate with each other, avoiding liquidity shortages and market fluctuations. Some data should not be stored on Blockchains and during the project, on-chain-off-chain decisions should be made. To support off-chain decisions, other storage systems are needed (e.g., interplanetary file system). For mobile devices, the concept of lightweight nodes versus *full nodes* can be considered. Full nodes have a copy of the whole transaction history and this history must be downloaded. Lightweight nodes verify transactions using simplified payment verification methods that download only the headers of all blocks on the Blockchain. Full nodes support lightweight nodes by allowing them to connect and transmit transactions to the network and by notifying lightweight nodes when a transaction affects them.

8.5.3. Inter-Organizational Integration

Inter-organizational governance assesses whether Blockchain capabilities enhance inter-organizational competitiveness (Beck et al., 2018). *Vision*, *strategies,* and *tactics* can differ for or be influenced by Blockchains because of its inter-organizational nature. For example, open-source strategies require granting universal access to development rights. Business value depends on specific use cases. Other *project-specific characteristics* (e.g., project size) can influence Blockchain adoption. It is necessary to consider switching costs that accrue through Blockchain adoption. However, these research directions are in their infancy and attention should be focused on how governance is different for or influenced by Blockchains versus other IT solutions.

Interactions of users are at the core of Blockchains, and **user adoption** of Blockchains requires attention. “It is thought that the organizational impact is just the social structure of people, who produce value” (I1). User adoption is driven by the hype around Blockchains and ignorance in terms of technical knowledge and implications that Blockchains might have. “In the future people will start to realize that Blockchain was a good idea for some things whether a very bad idea for all the other things, like Facebook” (I1). User adoption of Blockchains can depend on usability (quality of being easy to use to fulfill a specified task effectively), which is currently still an issue for Blockchains. For example, the Bitcoin API for developing services is difficult to use (Yli-Huumo et al., 2016). *Technology acceptance* and related constructs, such as ease of use and usefulness, cultural and age differences, as well as concepts from the broader adoption literature, such as technology acceptance theory and unified technology acceptance theory, can provide additional insights to assess user adoption. An important question is whether extant theories on user adoption will also hold for Blockchain technologies.

Interoperability is defined as interoperability between Blockchains, and interoperability of Blockchains with other systems. Interoperability *between Blockchains* is tightly coupled with interoperability of tokens. A Blockchain platform (e.g., Ethereum) that uses its currency makes it hard to be interoperable with other platforms. If one is in a Blockchain network and uses its tokens, it inflates the value of the tokens. “The worst thing that can happen in five years that only Ethereum is used because the whole point of Blockchain is no single central point and it is caused failure” (I2). Interoperability *between Blockchains and other systems* should emerge naturally when you comply with data standards.

8.5.4. Implementation Environment

Blockchains should comply with regulations and other requirements in the implementation environment. Compliance of Blockchains with current **regulations** is the greatest barrier. Data standards have not yet been proposed to deal with Blockchains. “It is thought that governments and regulators, in general, are very far behind in terms of data on Blockchains and data market-driven economies” (I2). An issue seen with Blockchains is that it has a cryptographic layer which may allow for obfuscation of actions that happen on Blockchains. Only several governments have imposed regulations of Blockchains, for example, in Singapore, China, Japan, and South Korea regulations of cryptocurrency markets were implemented.

Ecosystem-specific requirements may lead to differences in Blockchain suitability of markets and industries. Ecosystem self-sufficiency characterizes closed systems where value exchanges happen without external interactions (Glaser, 2017). To achieve high ecosystem self-sufficiency, the cooperation of customers and value providers within an ecosystem is required. Institutionalization captures to what degree Blockchains are embedded in social structures, for instance, who issues the value (e.g., central banks or community currency issuers). “In some cases, you need to have a closed Blockchain, for instance, Fed coin, if federal states decide to launch coins on their own to bypass banks and skip up some taxes” (I2). Other economic constraints including the potential to disrupt an industry or to distribute market power and competitive pressure can be considered together with related theories (e.g., theories of competition and market performance) to further inform Blockchain implementations.

8.5.5. Selected Interconnections between the Factors

Developers and Blockchain integrators also need to consider interconnections between the factors while evaluating Blockchain implementations. We found 48 interconnections between factors, however, we only discussed those which were mentioned more than two times. Overall, trade-offs between all factors should be considered specifically for each implementation.

8.5.5.1. Consensus Mechanism, Modularity → Integrity, Scalability

The consensus mechanism is closely related to integrity and scalability issues, and an estimation of their trade-offs is necessary. Different consensus mechanisms have different latencies associated with transaction confirmations (Walsh et al., 2016) and need to arrange transaction speed against an appropriate level of integrity (Risius and Spohrer, 2017; Xu et al., 2017). Blockchains are not suitable for high-frequency transactions but ensure high data integrity when proof-of-work is used as a consensus mechanism (Albrecht et al., 2018). However, Blockchains with consensus mechanisms such as proof-of-stake and practical Byzantine fault tolerance achieve higher scalability but are less secure regarding unauthorized modifications of data. The usage of multiple, connected Blockchains improves scalability (e.g., sharding). Multiple chains are used for specific tasks and types of transactions, where all chains are linked with the main Blockchain. These multiple chains can build a Blockchain ecosystem based on the main Blockchain to reduce transaction load on the main chain (Xu et al., 2017). However, "if we put more data on-chain, the integrity of data would increase" (I5).

8.5.5.2. Consensus Mechanism, Anonymity, Transparency, Permissioning

There are trade-offs between these four factors of Blockchain design. Whereas 96% of permissionless Blockchains use proof-of-work or proof-of-stake consensus mechanisms (Salviotti et al., 2018), permissioned Blockchains generally use lightweight consensus mechanisms, for example, practical Byzantine fault tolerance (Risius and Spohrer, 2017; Salviotti et al., 2018). In permissionless and public networks, users act under pseudonyms or are anonymous, while in permissioned and private networks all users are identified (Notheisenet al., 2017; Salviotti et al., 2018). In permissionless Blockchains all transactions are publicly viewable, creating full transparency of the network; permissioned Blockchains can sacrifice transparency of information (Risius and Spohrer, 2017; Albrecht et al., 2018).

8.5.5.3. User Adoption → Confidentiality, Integrity, Transaction Costs, and Scalability

The fear of being identifiable and linked to transactions in a fully transparent network keeps users from adopting Blockchains. Information about integrity breaches of Blockchains (e.g., money losses) can prevent adoption because in most cases "people trust in Blockchain by itself" (I5) without an understanding of the technical functioning. Integrity-related issues could also be moderated by cultural or age-related differences (Risius and Spohrer, 2017). If data integrity is not strong, then people will be less inclined to adopt Blockchains, "if it is kind of secure this increases the user acceptance" (I3). Costs and volatility in the transaction currency can constrain the adoption and utilization (Risius and Spohrer, 2017). Scalability issues (e.g., latency) can constrain the Blockchain utilization and determine end-user adoption (Risius and Spohrer, 2017).

8.5.5.4. Confidentiality → Transparency

Confidentiality is connected to transparency in a way that the more data transparency exists, the less confidentiality of users can be guaranteed (I2, I8). A fully transparent system allows anyone to see data on the Blockchain and no confidentiality is provided. Otherwise, a fully private system provides no transparency. However, a system can still provide significant confidentiality-guarantees while making processes of state transitions transparent. For example, a distributed ledger can provide public verifiability of its overall state without leaking information about the state of each participant. Confidentiality in a public system can be achieved using cryptographic techniques but typically comes at the cost of lower efficiency (Wüst and Gervais, 2018). Non-transparent data on Blockchains are necessary to protect confidential information. For example, confidentiality issues in Bitcoin Blockchain led to the development of Zcash, a cryptocurrency that encrypts all data on transactions including transaction value.

8.5.5.5. Regulations → Interoperability

To exchange data between systems, it is necessary to consider compatibility and network externalities and use the same formats and semantics. "It is not thought that interoperability is an issue right now; also, it is not thought that Blockchains forced to use data standards as much as possible. Shortly, the interoperability will emerge from the use cases affecting data standards" (I2).

8.6. Applicability of the Framework: The Brooklyn Microgrid

The Brooklyn Microgrid is a project of LO3 Energy startup that develops a Blockchain-based microgrid energy market in Brooklyn, New York. The project aims to enable network members to trade locally generated energy with the neighbors in a peer-to-peer manner (Lacity, 2018).

8.6.1. The Brooklyn Microgrid. Blockchain Innovation

First, a Blockchain-based microgrid energy market benefits from eliminating trusted third parties, centralized utility companies that manage energy platforms. Therefore, the usage of Blockchain technology for electricity transactions makes microgrids more efficient by creating trust between the involved agents (Mengelkamp et al., 2018). Second, the Brooklyn area is vulnerable to grid failures caused by repetitive natural disasters. The decentralized infrastructure of Blockchain allows a local microgrid to be available if the main utility grid is offline "so you have a safe place to charge your phone, get food or send out emails to let people know you are okay" (Lacity, 2018, p. 203).

Despite the envisioned benefits, Blockchain systems are energy-consuming in case of transaction costs that contradict the sustainability principles of microgrid energy markets (Mengelkamp et al., 2018). Besides, the developed Blockchain-based prototype has a dissatisfactory low transaction speed, i.e., scalability (Lacity, 2018).

The factors of integrity and *confidentiality* were not discussed in the available sources of the Brooklyn microgrid project. We assume that these factors have secondary importance. However, in other literature on peer-to-peer energy trading, the integrity of transactions and confidentiality of users in the Blockchain network is better comparing to centralized trading platforms (Mengelkamp et al., 2018).

8.6.2. The Brooklyn Microgrid. Blockchain Design

To provide decentralized infrastructure with high availability, LO3 Energy's first proof-of-concept was based on a standard Ethereum Blockchain (Lacity, 2018). Ethereum Blockchain is a *public permissionless Blockchain* that utilizes *proof-of-work* or *proof-of-stake* to reach consensus on the system updates and allows for *pseudonymous* users in the network.

8.6.3. The Brooklyn Microgrid. Inter-Organizational Integration

Decentralized Blockchain inter-organizational governance is suitable for ensuring a reliable balance of energy generation and consumption in the microgrid network (Mengelkamp et al., 2018). Moreover, the Brooklyn Microgrid's business model is characterized by a closed ecosystem that generates value inside of the community (Glaser, 2017). Because users can keep profits from energy trading within the community, the adoption of the network by market participants happens in a user-friendly and comprehensive way (Mengelkamp et al., 2018). Regarding interoperability, a secure connection from the market participants' energy devices and Blockchain is necessary. Also, interoperability between the main physical grid and Blockchain-based virtual microgrid should be established. Because energy is a physical good, energy flow problems might arise during the transmission on constrained grids (Mengelkamp et al., 2018).

8.6.4. The Brooklyn Microgrid. Implementation Environment

Current regulations of the energy sector do not allow to run local peer-to-peer energy markets in most countries and, hence, is the biggest bottleneck (Lacity, 2018; Mengelkamp et al., 2018). The Brooklyn Microgrid project in cooperation with Con Edison, Inc. is working on the legalization of a peer-to-peer local microgrid energy trading (Mengelkamp et al., 2018). Other ecosystem-specific requirements concern a lack of ability to exist in wholesale markets to react in real-time to the volatile and intermittent generation from decentralized microgrids. Furthermore, market prices are often determined on a national level which does not reflect balancing demand and supply of local energy (Mengelkamp et al., 2018).

8.6.5. The Brooklyn Microgrid. Interconnections

Instead of using computationally costly consensus, identity mechanisms use the simple verification of the agent's identity mechanisms (*consensus mechanism, anonymity* → *transaction costs*). If only trusted community members participate in the market, and identity-based consensus mechanism can be sufficiently secure (*consensus mechanism* → *anonymity*). Self-interested rational market participants maximize their revenue and minimize their energy costs (*user adoption* → *transaction costs*). There is no specific information about interconnections *confidentiality* → *transparency* and *regulations* → *interoperability* because the confidentiality of users was not mentioned as an important factor and regulations of the energy sector are not supported peer-to-peer energy trading to consider the specific effect on interoperability.

8.6.6. The Brooklyn Microgrid. Evaluation Outcome

The evaluation shows that the Brooklyn Microgrid project benefits from Blockchain by establishing trust without centralized utility companies and increased availability of the network. Therefore, an Ethereum public permissionless Blockchain satisfies these requirements. However, the Ethereum Blockchain has challenges such as transaction costs and scalability of the network because of the employed proof-of-work consensus mechanism. Further, inter-organizational integration of Blockchain supports decentralized governance of the peer-to-peer local energy trading together with closed value generation of the business model. Thus, users are motivated to participate in the network. However, the interoperability of the users' devices with Blockchain and the Blockchain with the main physical grid is challenging. The main bottleneck is regulations that do not allow to trade energy on the local markets. Therefore, computationally efficient *Blockchains with different consensus mechanisms* should be more suitable to maximize performance metrics of adopting Blockchains (Mengelkamp et al., 2018). Also, *regulations should be developed on the national and international levels*.

8.7. Discussion

The framework for evaluation of Blockchain implementations comprises factors that are important to consider before Blockchain projects begin. Factors are grouped into four semantic categories Blockchain suitability, Blockchain design, inter-organizational integration, and implementation environment. First, the benefits of implementing Blockchains—integrity, trust, and availability—and challenges—transaction costs, scalability, and confidentiality—should be estimated and contrasted with project requirements. Second, five Blockchain design components—consensus mechanism, anonymity, transparency and modularity—can be combined into diverse Blockchain designs to maximize benefits and minimize challenges. Third, Blockchain-based systems need to be integrated into organizational processes, which requires consideration of governance, user adoption, and interoperability of Blockchains and other information systems. Fourth, Blockchains should fit into their implementation environment including compliance with regulations and other ecosystem-specific requirements (e.g., competitive pressure).

This research contributes to the scientific knowledge base in four ways. First, previous research on Blockchain proposes computer-science (Glaser and Bezzenberger, 2015; Walsh et al., 2016), user-related, and organization-related factors (Glaser, 2017; Salviotti et al., 2018) but falls short in considering their mutual impact. Our study complements previous research by offering clear conceptualizations for the identified Blockchain evaluation factors and their interconnections. The identified factors bridge the gap between extant technology-centered and organizational-focused research on Blockchains and serve as a foundation for the further synthesis of the findings. Second, we proposed an integrative framework for the evaluation of Blockchain implementations. The framework synthesizes expert insights about the development of Blockchain-based systems and their implementation in organizational and environmental contexts. Third, the overview of extant research can accelerate future conceptual studies on Blockchain adoption (e.g., case studies, expert interviews, and Delphi studies) in different industries that may identify new interconnections between factors not addressed in extant literature. Fourth, further analysis of theoretical and empirical findings in different industries will allow for the development of Blockchain measurements and performance indicators, which will be useful to reduce the prevailing uncertainty about the business value of Blockchains.

Our research contributes to practice by providing a comprehensive combination of factors that can influence the outcomes of implementations. We have proposed an integrative framework to evaluate Blockchain implementations that is useful for practitioners to gain knowledge about the main factors before the projects begin. For example, our study highlights other Blockchain designs, besides the widely-known public Blockchains, that are useful if public Blockchains are unfeasible. For many projects, businesses should consider the implementation of private Blockchains that store information more predictable and confidential than public Blockchains. Private Blockchains lose the advantages of completely decentralized networks; still, they keep up-to-date data with an immutable history of changes that is available for all members of the network. Moreover, the framework can support project management by providing insights on the required expertise of project teams and purposeful key performance indicators of Blockchain projects.

This study is not without limitations. First, we focus on Blockchains as one type of a distributed ledger where the continuous transaction history is kept in blocks. Other types of distributed ledgers, for example, directed acyclic graphs (IOTA) are out of the scope of the study. Second, we do not go into technical specifics concerning Blockchain factors. For example, our discussion of integrity could go into more details on cryptographic algorithms. Cryptographic algorithms also should be exchanged or strengthened with increasing processing power available to attackers or as soon as exploits are discovered. However, this seems appropriate as our goal was to provide a holistic overview of factors that can guide projects, which consider Blockchain adoptions.

Future research could replicate our research approach with additional scientific or industry data to falsify or corroborate our findings. The identification of additional Blockchain evaluation factors would broaden the applicability of the developed framework. Further, future research could elaborate on the proposed concepts for specific industries, markets, and countries. Studies in different industry contexts would allow to development of measurements and performance indicators that are pertinent for Blockchain systems. This, in turn, would reduce the existing uncertainty about the real business value of Blockchain systems (Notheisen et al., 2017).

8.8. Conclusion

Blockchain is an emerging technology with largely untapped potential. Currently, knowledge of Blockchain remains largely disparate, which hinders the integration of Blockchain-based systems into organizations. Our work consolidates research on technical, inter-organizational, and environmental perspectives of Blockchain in the form of a framework for evaluation of Blockchain implementations. The framework accounts for Blockchain evaluation factors that are grouped into four categories, Blockchain suitability, Blockchain design, inter-organizational integration, and implementation environment. This research contributes to the scientific knowledge base by synthesizing information on Blockchain evaluation factors and highlighting their interconnections. It complements the scientific literature on Blockchain classifications and Blockchain integration frameworks, i.e., DSR in the Blockchain domain. Overall, the framework for evaluation of Blockchain implementations captures the current state of knowledge on Blockchain aspects and their interconnections; simultaneously, it serves as a foundation for future theoretical and empirical research exploring how to integrate Blockchain into industries and markets.

8.9. Acknowledgements

We would like to thank Alexander Herwix (University of Cologne), Tobias Dehling (Karlsruhe Institute of Technology), Niclas Kannengießer (Karlsruhe Institute of Technology), Benedikt Notheisen (Karlsruhe Institute of Technology), Alexander Garcia (Graz University of Technology), and Ali Sunyaev (Karlsruhe Institute of Technology) for the helpful comments on earlier versions of this work.

9. Discussion

This dissertation project aims to bridge the gap between technical and managerial knowledge of Blockchain that allows successful Blockchain system design and implementation. I identified the scope of Blockchain applications and introduced guidelines to make purposeful decisions of Blockchain implementations. The dissertation covers different perspectives of Blockchain investigation and adoption, i.e., technical, application, organizational, and combinational or multi-level. There are four principal findings.

First, I consolidated the knowledge of Blockchain technical configurations through the development of a taxonomy. I limited the scope of purposeful Blockchain applications by connecting technical Blockchain characteristics across a range of foundational application cases. The findings show that Blockchain application areas are at different maturity levels. Financial transactions constitute the most mature application area. Smart contracts received attention because of the idea to execute agreements on Blockchains. Data management gains momentum because of emerging enterprise applications. Storage, communication, and ranking on Blockchains are less prevalent. Besides, Blockchain applications vary in technical configurations (e.g., reading access, writing access, main consensus mechanism, anonymity level, event handling, data exchange type, encryption, and history retention).

Second, I considered the design patterns of smart contracts that represent the application logic of Blockchain systems. I found the defined standards and introduced them in the form of sixteen design patterns of Blockchain smart contracts. Besides, a pattern language examines and summarizes the relationships between smart contract design patterns.

Third, guidance was offered for transforming initial conceptions of Blockchain ideas into working system prototypes. I introduced a Blockchain configuration process model, a tool to assists with the configuration of Blockchain properties and Blockchain deployment attributes based on a set of known requirements of a Blockchain project (i.e., Blockchain governance, Blockchain application area). Three groups of relationships between Blockchain concepts were derived: interdependencies between Blockchain governance and Blockchain application areas, relationships between application areas and Blockchain properties (i.e., token, customizability, data type, and history retention), and relationships between Blockchain governance and Blockchain deployment (i.e., access and validation).

Fourth, the factors of Blockchain decisions have a multi-level nature. The factors can be grouped into four semantic categories: Blockchain suitability, Blockchain design, inter-organizational integration, and implementation environment. I introduced the factors in the form of the framework for the evaluation of Blockchain implementations.

9.1. Research Contribution

This research contributes to the scientific knowledge base in four ways. First, the findings contribute to the theory of IT governance in the context of Blockchain systems. Accordingly, this paper defined the concept of Blockchain governance based on three IT governance approaches. Decentralized Blockchain governance is suitable for collectively governed companies or startups to spread decision rights and accountabilities among all actors (i.e., nodes) in the network. Hybrid Blockchain governance is useful for inter-organizational collaboration to ensure confidentiality while sharing decision rights among all nodes in the network. Lastly, a centralized Blockchain governance approach is useful to support enterprise business projects where a predefined number of users can monitor decisions while only validating nodes have decision rights.

Second, the allocation of Blockchain application cases based on technical Blockchain characteristics reduced the hype around Blockchain application possibilities. Classification of application areas that, along with semantic differences, is based on technical characteristics, made the identification of application areas more meaningful.

Third, the study bridges prior research by offering clearer conceptualizations for the identified concepts and their relationships. As such, the identified relationships (i.e., governance, application areas, properties, and deployment) bridge knowledge gaps between computer science and the socio-economic literature on Blockchain systems.

Fourth, it proposed artefacts that reveal new insights on the development of Blockchain-based systems and their further implementation in the organizational context. I identified additional technical dimensions of importance in the Blockchain domain. Therefore, technical research can go beyond the Bitcoin Blockchain and focus on other areas, for example, the development of a Blockchain-based protocol for data transmission in healthcare.

9.2. Practical Contribution

This research contributes to practice in three ways. First, I introduced a comprehensive combination of factors that can influence the outcomes of Blockchain projects. This might be useful for practitioners to identify the more promising Blockchain projects and assess risks during Blockchain implementation. Moreover, the factors can support project management by providing insights on the required expertise of project teams and purposeful key performance indicators of Blockchain projects.

Second, it was presented with further evidence that Blockchains are not only applicable to the financial sector, which is the focus of the majority of Blockchain projects but also for other promising areas. Thus, other industries can use Blockchain advantages for resolving their challenges. For example, in the media industry, Blockchain-based data management may be useful to monitor the use of media content to prevent copyright infringements.

Third, the insights highlight other Blockchain types, besides the widely-known public Blockchain, that is useful if public Blockchains are unfeasible. For many application cases, businesses should consider the implementation of private Blockchains that store information more reliably and confidentially than public Blockchains. Private Blockchains lose the advantages of completely decentralized networks; still, they keep up-to-date data with an immutable history of changes that is available for all members of the network. Further, it highlighted the hybrid governance approach, which stores information in a more confidential but still more decentralized fashion.

9.3. Limitations

This study is not without limitations. First, this project does not go into detail concerning Blockchain concepts. For example, security can be further detailed on encryption algorithms, while encryption algorithms should be exchanged or strengthened with increasing processing power available to attackers or as soon as exploits are discovered. However, this seems appropriate as my goal was to provide a holistic overview of factors that can guide projects, which consider Blockchain adoptions.

Second, I could not identify application areas that may emerge in the future. The rapidly evolving nature of the Blockchain domain will necessitate an extension of the artefacts with new application cases and information in general.

Fourth, I focus on Blockchains as one type of a distributed ledger where the continuous transaction history is kept in blocks. Other types of distributed ledgers, for example, directed acyclic graphs (IOTA) are out of the scope of the dissertation.

9.4. Future Research

There are four promising areas for future research. First, research that replicates my research approach with more or different scientific and business sources will be useful to falsify or corroborate my findings. The identification of further Blockchain concepts would broaden the applicability of the integrative artefacts.

Second, research focused on other socio-economic concepts, for example, market regulations in different countries or implementation and management strategies of Blockchain-based information systems will be useful to contextualize the findings for different industries and domains. For example, the interoperability of Blockchain-based systems and other information systems is constrained by industry-specific or country-specific data protection regulations such as HIPAA in healthcare (Mercuri, 2004) or the GDPR in the European Union.

Third, the studies in different industry contexts would allow developing measurements and performance indicators that are pertinent to Blockchain systems. This, in turn, would reduce the existing uncertainty about the real business value of Blockchain systems.

10. Conclusions

Blockchain is an emerging technology with largely untapped potential. Currently, research streams on Blockchain remain largely disparate, which hinders the integration of Blockchain-based systems into organizations. This dissertation project consolidates knowledge on system, organizational, and environmental perspectives of Blockchain and their combination in the form of four artefacts, which guide Blockchain projects and facilitate purposeful

Blockchain adoption. This research contributes to the scientific knowledge base by bridging knowledge gaps between computer science and socio-economic research. Overall, the dissertation project captures the current state of knowledge on Blockchain aspects. Simultaneously, it serves as a foundation for future theoretical and empirical research exploring the Blockchain domain.

Appendix A. A Factor Matrix

Blockchain Evaluation Factors / ***References***	Blockchain Innovation						Blockchain Design					Inter-Organizational Integration			Implementation Environment		Interconnections				
	Integrity	Trust	Availability	Transaction Costs	Scalability	Confidentiality	Consensus Mechanism	Anonymity	Transparency	Permissioning	Modularity	Inter-Organizational Governance	User Adoption	Interoperability	Regulations	Ecosystem-Specific Requirements	Consensus Mechanism, Modularity → Integrity, Scalability, Transaction Costs	Consensus Mechanism → Anonymity → Transparency → Permissioning	User Adoption → Confidentiality, Integrity, Transaction Costs, Scalability	Confidentiality → Transparency	Regulations → Interoperability
Albrecht et al., 2018	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X		X	X
Andersen and Bogusz, 2017	X		X					X													
Beck & Müller-Bloch, 2017	X	X		X	X				X	X		X			X						
Beck et al., 2016	X	X	X	X	X		X		X	X	X		X	X			X				
Beck, Müller-Bloch and King, 2018	X	X	X						X	X		X									
Beinke and Ngoc, 2018	X	X	X	X	X							X									
Bonneau et al., 2015	X		X	X	X	X	X	X							X						
Brenig, Schwarz and Rückeshäuser, 2016	X	X		X				X				X	X								
Chanson, Risius and Wortmann, 2018		X		X				X							X						
Ciriello, Beck and Thatcher, 2018	X	X	X	X		X	X	X	X	X		X	X		X	X		X		X	
Diniz et al., 2016		X		X	X				X	X		X	X	X	X						
Elsman et al., 2017	X	X	X	X	X	X	X	X	X	X					X	X	X	X			
Fridgen, Lockl, et al., 2018	X		X									X				X					
Fridgen, Schweizer et al., 2018		X	X	X	X							X	X	X	X	X					X
Fridgen et al., 2018	X	X	X	X	X				X	X				X	X	X					X
Friedlmaier, Tumasjan and Welpe, 2016	X	X	X	X	X		X		X	X		X		X	X						
Glaser, 2017		X	X	X	X		X			X		X	X		X	X					
Glaser and Bezzenberger,2015	X	X		X	X		X	X							X	X					
Hawlitschek, Notheisen and Teubner, 2018	X	X	X	X	X	X	X	X	X	X		X		X	X	X	X	X			
Holotiuk& Moormann,2018		X		X	X	X						X	X		X			X			
Hua et al., 2018	X	X	X	X	X	X	X	X	X	X							X	X			
Hyvärinen et al., 2017	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X		X			
Kaul, Storey and Woo, 2018	X	X	X			X	X		X			X			X						
Kazan et al., 2014	X								X			X	X								
Lacity, 2018	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X		X			
Liet al., 2018	X	X	X		X			X		X			X		X						

	Mendling et al., 2018	X	X																			
	Mendling et al., 2017	X	X	X	X	X	X	X	X				X	X	X	X	X		X			
	Morisse, 2015	X				X		X	X	X	X			X								
	Moyano and Ross, 2017	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X			
	Naerland et al., 2017	X	X	X	X	X	X	X	X	X	X		X	X				X	X			
	Nofer et al., 2017	X	X	X	X	X	X	X	X	X	X		X	X			X		X			
	Notheisen et al., 2017	X	X	X	X	X	X	X	X	X	X		X	X		X	X		X			
	Notheisen, Cholewa & Shanmugam, 2017	X	X	X	X	X	X	X	X	X	X	X					X	X	X			
	Oliveira et al., 2018	X	X					X		X	X		X	X				X				
	Rückeshäuser, 2017	X		X	X	X		X		X	X		X				X	X	X			
	Risius and Spohrer, 2017	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X		X
	Sadhya and Sadhya, 2018	X	X	X	X	X	X	X	X	X			X	X		X	X					
	Salviotti, Ross and Abbatemarco, 2018	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X			
	Scholz and Stein, 2018	X	X	X	X	X	X	X	X	X	X		X		X	X	X	X	X		X	
	Schlegel, Zavolokina and Schwabe, 2018	X	X	X	X	X		X	X					X		X						
	Schweizer et al., 2017	X	X	X	X	X	X	X	X	X	X			X		X	X	X	X			
	Seebacher, 2018	X	X	X			X	X	X	X	X		X	X			X	X				
	Tönnissen and Teuteberg,2018	X	X	X	X		X		X							X	X					
	Tschorsch and Scheuermann, 2016	X		X	X	X	X	X	X													
	Walsh et al., 2016	X		X		X		X	X	X	X	X	X		X	X						
	Wang, Luo and Xue, 2018	X	X	X	X	X		X					X	X								
	Wörner et al., 2016	X	X	X	X			X	X	X	X	X	X	X	X	X	X					
	Xu et al., 2017	X	X	X	X	X	X	X	X	X	X	X	X		X	X		X	X			
	Yli-Huumo et al., 2016	X	X	X	X	X	X	X	X		X		X	X								
	Ziolkowski et al., 2018	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X		
Counting		**46**	**43**	**41**	**40**	**38**	**26**	**36**	**34**	**33**	**33**	**7**	**35**	**29**	**18**	**32**	**25**	**17**	**21**	**2**	**3**	**4**
Evaluation	Interviewee 1		X						X			X	X	X	X	X		X				
	Interviewee 2	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Interviewee 3	X	X	X		X		X	X	X	X	X	X	X	X	X	X	X	X	X		
	Interviewee 4	X	X									X	X		X							
	Interviewee 5	X	X	X	X	X	X					X	X		X		X	X	X	X	X	X
	Interviewee 6	X		X	X	X		X		X	X		X	X		X		X	X			
	Interviewee 7	X		X	X	X	X	X	X	X	X	X		X	X	X	X		X	X	X	
Counting		**6**	**4**	**5**	**4**	**5**	**3**	**4**	**4**	**4**	**4**	**6**	**6**	**5**	**6**	**5**	**4**	**5**	**5**	**4**	**3**	**2**
The Brooklyn Microgrid		X+	X+	X+	X-	X-	X+	X+	X+	X+	X+	N/A	X+	X+	X-	X-	X-	X+	X+	X+	N/A	N/A

Bibliography

Albrecht, S., S. Reichert, J. Schmid, J. Strüker, D. Neumann and G. Fridgen. (2018). "Dynamics of Blockchain Implementation - A Case Study from the Energy Sector." In: *51st Hawai International Conference on System Sciences* (pp. 3527–3536). Waikoloa, Hawaii, USA.

Andersen, J. and C. Bogusz. (2017). "Patterns of Self-Organising in the Bitcoin Online Community: Code Forking as Organising in Digital Infrastructure." In: *38th International Conference on Information Systems (ICIS 2017)* (pp. 1–20). Seoul, South Korea.

Avital, M., J. L. King, R. Beck, M. Ross I. and R. Teigland. (2016). "Jumping on the Blockchain Bandwagon : Lessons of the Past and Outlook to the Future Panel." In: *37th International Conference on Information Systems (ICIS 2016)* (pp. 1–6). Dublin, Ireland.

Azaria, A., A. Ekblaw, T. Vieira and A. Lippman. (2016). "MedRec: Using Blockchain for Medical Data Access and Permission Management." In: *2nd International Conference on Open and Big Data (OBD 2016)* (pp. 25–30). Vienna, Austria.

Bartoletti, M. and L. Pompianu. (2017). "An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns." In: *21st International Conference on Financial Cryptography and Data Security (FC 2017)* (pp. 494–509). Sliema, Malta.

Baskerville, R. and J. Pries-Heje. (2010). "Explanatory Design Theory." *Business & Information Systems Engineering, 2*(5), 271–282.

Beck, K. and W. Cunningham. (1987). Using Pattern Languages for Object-Oriented Programs. *OOPSLA-87 workshop on the Specification and Design for Object-Oriented Programming*. Orlando, USA.

Beck, R., M. Avital, M. Ross I. and J. B. Thatcher. (2017). "Blockchain Technology in Business and Information Systems Research." *Business & Information Systems Engineering, 59*(6), 381–384.

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

Beck, R., C. Müller-Bloch and J. L. King. (2018). "Governance in the Blockchain Economy: A Framework and Research Agenda." *Journal of the Association for Information Systems, 19*(10), 1020–1034.

Beck, R., J. Stenum Czepluch, N. Lollike and S. Malone. (2016). "Blockchain - The Gateway to Trust-Free Cryptographic Transactions." In: *24th European Conference on Information Systems (ECIS 2016)* (pp. 1–14). Istanbul, Turkey.

Beinke, J. H., D. Nguyen Ngoc and F. Teuteberg. (2018). "Towards a Business Model Taxonomy of Startups in the Finance Sector using Blockchain." In: *39th International Conference on Information Systems (ICIS 2018)* (pp. 1–9). San Francisco, USA.

Beinke, J. H., D. Nguyer and F. Teuteberg. (2018). "Towards a Business Model Taxonomy of Startups in the Finance Sector using Blockchain." In: *26th European Conference on Information Systems (ECIS 2018)* (pp. 1–17). Portsmouth, UK.

Bloom, B. (2001). "Bloom ' s Taxonomy." *ReVision*, 1–6.

Bogner, A., M. Chanson and A. Meeuw. (2016). "A Decentralised Sharing App Running a Smart Contract on the Ethereum Blockchain." In: *6th International Conference on the Internet of*

Things (IoT 2016) (pp. 177–178). Stuttgart, Germany.

Böhm, M., J. Weking, F. Fortunat, S. Müller, I. Welpe and H. Krcmar. (2017). "The Business Model DNA: Towards an Approach for Predicting Business Model Success." In: *13th International Conference on Wirtschaftsinformatik (WI2017)* (pp. 1006–1020). St. Gallen, Switzerland.

Bonneau, J., A. Miller, J. Clark, A. Narayanan, J. A. Kroll and E. W. Felten. (2015). "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies." *IEEE Symposium on Security and Privacy*, 104–121.

Borchers, J. O. (1999). "Electronic Books: Definition, Genres, Interaction Design Patterns." In: *Conference on Human Factors in Computing Systems. CHI99 Workshop: Designing Electronic Books* (pp. 1–8). Pittsburgh, USA.

Boynton, A. C. and R. W. Zmud. (1987). "Information Technology Planning in the 1990s: Directions for Practice and Research." *MIS Quarterly*, *11*(1), 59–71.

Brenig, C., J. Schwarz and N. Rückeshäuser. (2016). "Value of Decentralized Consensus Systems - Evaluation Framework." In: *24th European Conference on Information Systems (ECIS 2016)* (pp. 1–18). Istanbul, Turkey.

Brown, A. and G. Grant. (2005). "Framing the Frameworks: A Review of IT Governance Research." *Communications of the Association for Information Systems*, *15*(1), 696–712.

Brown, C. and S. Magill. (1994). "Alignment of the IS Functions with the Enterprise: Toward a Model of Antecedents." *MIS Quarterly*, *18*(4), 371–403.

Buterin, V. (2014). "A Next-Generation Smart Contract and Decentralized Application Platform." *Etherum*, *3*(37), 1–36.

Chanson, M., M. Risius and F. Wortmann. (2018). "Initial Coin Offerings (ICOs): An Introduction to the Novel Funding Mechanism Based on Blockchain Technology." In: *24th Americas Conference on Information Systems (AMCIS 2018)* (pp. 1–5). New Orleans, USA.

Chapman, J., R. Garratt, S. Hendry, A. Mccormack and W. Mcmahon. (2017). *Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet? Bank of Canada Financial System Review*.

Chen, Y. and C. Bellavitis. (2020). "Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models." *Journal of Business Venturing Insights*, *13*(1), 1–8.

Christidis, K. and M. Devetsikiotis. (2016). "Blockchains and Smart Contracts for the Internet of Things." *IEEE Access*, *4*(1), 2292–2303.

Ciriello, R., R. Beck and J. B. Thatcher. (2018). "The Paradoxical Effects of Blockchain Technology on Social Networking Practices." In: *39th International Conference on Information Systems (ICIS 2018)* (pp. 1–17). San Francisco, USA.

Constantinides, P., O. Henfridsson and G. G. Parker. (2018). "Introduction—Platforms and Infrastructures in the Digital Age." *Information Systems Research*, *29*(2), 381–400.

Daian, P., S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, … A. Juels. (2019). "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges." *ArXiv Preprint*, *1904*(05234), 1–23.

Darwin, C. (2009). "The Origin of Species (1859)." In: *Foundations of Psychological Thought:*

A History of Psychology. (pp. 320–336).

Davidson, S., P. De Filipp I. and J. Potts. (2016). "Economics of Blockchain." *SSRN Electronic Journal*, *17*(3), 1–23.

Dennis, R. and G. Owenson. (2016). "Rep on the Roll: A Peer to Peer Reputation System Based on a Rolling Blockchain." *International Journal of Digital Society*, *7*(1), 1123–1134.

Diniz, E. H., E. S. Siqueira and E. Van Heck. (2016). "Taxonomy for Understanding Digital Community Currencies: Digital Payment Platforms and Virtual Community Feelings." In: *SIG GlobDev Ninth Annual Workshop* (pp. 1–25). Dublin, Ireland.

Du, W., S. L. Pan, D. E. Leidner and W. Ying. (2019). "Affordances, Experimentation and Actualization of FinTech: A Blockchain Implementation Study." *Journal of Strategic Information Systems*, *28*(1), 50–65.

Eberhardt, J. and S. Tai. (2017). "On or off the Blockchain? Insights on off-Chaining Computation and Data." In: *European Conference on Service-Oriented and Cloud Computing (ESOCC 2017)* (pp. 3–15). Oslo, Norway.

Elsman, M., B. Egelund-mu, F. Henglein and O. Ross. (2017). "Automated Execution of Financial Contracts on Blockchains." *Business & Information Systems Engineering*, *59*(6), 457–467.

Ergin, H., E. Syrian I. and J. Gray. (2016). "Design Pattern-Oriented Development of Model Transformations." *Computer Languages, Systems and Structures*, *46*(1), 106–139.

Fabian, B., T. Ermakova and U. Sander. (2016). "Anonymity in Bitcoin – The Users' Perspective." In: *37th International Conference on Information Systems (ICIS 2016)* (pp. 1–12). Dublin, Irland.

Fridgen, G., J. Lockl, S. Radszuwill, A. Rieger, A. Schweizer and N. Urbach. (2018). "A Solution in Search of a Problem: A Method for the Development of Blockchain Use Cases." In: *24th Americas Conference on Information Systems (AMCIS 2018)* (pp. 1–10). New Orleans, USA.

Fridgen, G., S. Radszuwill, A. Rieger and N. Urbach. (2018). "A Blockchain Use Cases Development Method A Solution in Search of a Problem : A Method for the Development of Blockchain Use Cases." In: *Twenty-fourth Americas Conference on Information Systems* (pp. 1–10).

Fridgen, G., S. Radszuwill, N. Urbach and L. Utz. (2018). "Cross-Organizational Workflow Management Using Blockchain Technology – Towards Applicability, Auditability, and Automation." In: *51st Hawai I. International Conference on System Sciences (HICSS 2018)* (pp. 3507–3516). Waikoloa, Hawaii, USA.

Fridgen, G., A. Schweizer, F. Regner and N. Urbach. (2018). "Don't Slip on the ICO- A Taxonomy for a Blockchain-enabled Form of Crowdfunding." In: *26th European Conference on Information Systems (ECIS 2018)* (pp. 1–17). Portsmouth, UK.

Friedlmaier, M., A. Tumasjan and I. M. Welpe. (2018). "Disrupting Industries with Blockchain: The Industry, Venture Capital Funding, and Regional Distribution of Blockchain Ventures." In: *51st Hawai I. International Conference on System Sciences (HICSS 2018)* (pp. 3517–3526). Waikoloa, Hawaii, USA.

Furlonger, D. and R. Valdes. (2017). *Practical Blockchain: A Gartner Trend Insight Report*. *Gartner Research*. Retrieved from https://www.gartner.com

Gamma, E., R. Helm, R. Johnson and J. Vlissides. (1993). "Design Patterns: Abstraction and Reuse of Object-Oriented Design." In: *ECOOP '93 - Object-Oriented Programming* (pp. 1–21). Kaiserslautern, Germany.

Garcia, A., F. Lopez and M. Conlon. (2018). "Thinking of a Blockchain for VIVO."

Giancaspro, M. (2017). "Is a "Smart Contract" really a Smart Idea? Insights from a Legal Perspective." *Computer Law and Security Review*, *33*(6), 825–835.

Gibbs, T. and S. Yordchim. (2014). "Thai Perception of Litecoin Value." *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, *8*(8), 2613–2615.

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* (pp. 1543–1552). Waikoloa, Hawaii, USA.

Glaser, F. and L. Bezzenberger. (2015). "Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems." In: *23rd European Conference on Information Systems (ECIS 2015)* (pp. 1–18). Münster, Germany.

Glass, R. L. and I. Vessey. (1995). "Contemporary Application-Domain Taxonomies." *IEEE Software*, *12*(4), 63–76.

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

Grodal, S., A. Gotsopoulos and F. Suarez. (2015). "The Coevolution of Technologies and Categories during Industry Emergence." *Academy of Management Review*, *40*(3), 423–445.

Hahn, A., R. Singh, C. C. Liu and S. Chen. (2017). "Smart Contract-Based Campus Demonstration of Decentralized Transactive Energy Auctions." In: *8th Conference on Innovative Smart Grid Technologies (ISGT 2017)* (pp. 1–5). Arlington, USA.

Hans, R., H. Zuber, A. Rizk and R. Steinmetz. (2017). "Blockchain and Smart Contracts: Disruptive Technologies for the Insurance Market." In: *23rd Americas Conference on Information Systems (AMCIS 2017)* (pp. 1–10). Boston, USA.

Hawlitschek, F., B. Notheisen and T. Teubner. (2018). "The Limits of Trust-Free Systems: A Literature Review on Blockchain Technology and Trust in the Sharing Economy." *Electronic Commerce Research and Applications*, *29*, 50–63.

Hevner, A. R. (2007). "A Three Cycle View of Design Science Research." *Scandinavian Journal of Information Systems*, *19*(2), 87–92.

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

Higgins, S. (2015). "Factom Partners With Honduras Government on Blockchain Tech Trial." *CoinDesk*, pp. 1–3.

Holotiuk, F. and J. Moormann. (2018). "Organizational Adoption of Digital Innovation: The Case of Blockchain Technology." In: *26th European Conference on Information Systems (ECIS 2018)* (pp. 1–17). Portsmouth, UK.

Hua, S., E. Zhou, B. Pi, J. Sun, Y. Nomura and H. Kurihara. (2018). "Apply Blockchain Technology to Electric Vehicle Battery Refueling." In: *51st Hawaii International Conference* *on System Sciences (HICSS 2018)* (pp. 4494–4502). Waikoloa, Hawaii, USA.

Huang, B., Z. Liu, J. Chen, A. Liu, Q. Liu and Q. He. (2017). "Behavior Pattern Clustering in Blockchain Networks." *Multimedia Tools and Applications*, *76*(19), 20099–20110.

Hyperledger Architecture Working Group. (2017). *Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus* (Vol. 1). Hyperledger.org.

Hyvärinen, H., M. Risius and G. Friis. (2017). "A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services." *Business and Information Systems Engineering*, *59*(6), 441–456.

Iansiti, M. and K. R. Lakhani. (2017). *The truth about blockchain*. *Harvard Business Review*.

IBM. (2018). "DB Systel and IBM: Public Mobility."

Kannengießer, N., S. Lins, T. Dehling and A. Sunyaev. (2019). "What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs." In: *52nd Hawaii International Conference on System Sciences (HICSS 2019)* (pp. 7069–7078). Waikoloa, Hawaii, USA.

Karame, G. O., E. Androulak and S. Capkun. (2012). "Double-Spending Fast Payments in Bitcoin." In: *ACM Conference on Computer and Communications Security (CCS 2012)* (pp. 906–917). New York, USA.

Karame, G. O., E. Androulaki, M. Roeschlin, A. Gervais and S. Čapkun. (2015). "Misbehavior in Bitcoin: A Study of Double-Spending and Accountability." *ACM Transactions on Information and System Security (TISSEC)*, *18*(1), 1–32.

Kaul, M., V. Storey and C. Woo. (2018). "Feasibility of Blockchain Applications." In: *24th Americas Conference on Information Systems (AMCIS 2018)* (p. 1). New Orleans, USA.

Kazan, E., C. Tan and E. Lim. (2015). "Value Creation in Cryptocurrency Networks: Towards A Taxonomy of Digital Business Models for Bitcoin Companies." In: *19th Pacific Asia Conference on Information Systems (PACIS 2015)* (pp. 1–34). Singapore.

Kazan, E., C. Tan and E. T. K. Lim. (2014). "Towards a Framework of Digital Platform Disruption: A Comparative Study of Centralized & Decentralized Digital Payment Providers." In: *25th Australasian Conference on Information Systems (ACIS 2014)* (pp. 1–10). Auckland, New Zealand.

Khan, M. A. and K. Salah. (2018). "IoT Security: Review, Blockchain Solutions, and Open Challenges." *Future Generation Computer Systems*, *82*(1), 395–411.

Kharitonov, A. (2017). "A Framework for Strategic Intra- and Inter-Organizational Adoption of Blockchain Technology." *SSRN Electronic Journal*, 1–6.

Kirpes, B. and C. Becker. (2018). "Processing Electric Vehicle Charging Transactions in a Blockchain-based Information System." In: *24th Americas Conference on Information Systems (AMCIS 2018)* (pp. 1–5). New Orleans, USA.

Kishigami, J., S. Fujimura, H. Watanabe, A. Nakadaira and A. Akutsu. (2015). "The Blockchain-Based Digital Content Distribution System." In: *5th International Conference on Big Data & Cloud Computing (BDC 2015)* (pp. 187–190). Dalian, China.

Koning, J. P. (2016). *Fedcoin: A Central Bank-Issued Cryptocurrency*. *R3 Report*.

Kuo, T. T., H. E. Kim and L. Ohno-Machado. (2017). "Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications." *Journal of the American*

Medical Informatics Association, *24*(6), 1211–1220.

Labazova, O., T. Dehling and A. Sunyaev. (2019). “From Hype to Reality: A Taxonomy of Blockchain Applications.” In: *52nd Hawaii International Conference on System Sciences (HICSS 2019)* (pp. 4555–4564). Waikoloa, Hawaii, USA.

Lacity, M. C. (2018). “Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality.” *MIS Quarterly Executive*, *17*(3), 201–222.

Lamberti, F., V. Gatteschi, C. Demartini, C. Pranteda and V. Santamaria. (2018). “To Blockchain or Not to Blockchain: That Is the Question.” *IT Professional*, *20*(1), 62–74.

Laurillau, Y. (2013). “IOWAState: Models and Design Patterns for Identity-Aware User Interfaces Based on State Machines.” In: *5th ACM SIGCHI Symposium on Engineering Interactive Computing Systems (EICS 2013)* (pp. 59–68). London, UK: Association for Computing Machinery, New York, USA.

Li, Y., T. Marrie-Bienvenue, A. Perron-Brault, X. Wang and G. Paré. (2018). “Blockchain Technology in Business Organizations: A Scoping Review.” In: *51st Hawaii International Conference on System Sciences* (pp. 4474–4483). Waikoloa, Hawaii, USA.

Lin, I.-C. and T.-C. Liao. (2017). “A Survey of Blockchain Security Issues and Challenges.” *International Journal of Network Security*, *1919*(55), 653–65901.

Lindman, J., V. K. Tuunainen and M. Rossi. (2017). “Opportunities and Risks of Blockchain Technologies – a Research Agenda.” In: *50th Hawaii International Conference on System Sciences (HICSS 2017)* (pp. 1533–1542). Waikoloa, Hawaii, USA.

Lischke, M. and B. Fabian. (2016). “Analyzing the Bitcoin Network: The First Four Years.” *Future Internet*, *8*(1), 1–7.

Liu, Y., Q. Lu, X. Xu, L. Zhu and H. Yao. (2018). “Applying Design Patterns in Smart Contracts: A Case Study on a Blockchain-Based Traceability Application.” In: *2nd International Conference on Blockchain (ICBC 2018)* (pp. 92–106). San Diego, USA.

Loebbecke, C., L. Lueneborg and D. Niederle. (2018). “Blockchain Technology Impacting the Role of Trust in Transactions: Reflections in the Case of Trading Diamonds.” In: *26th European Conference on Information Systems (ECIS 2018)* (pp. 1–11). Portsmouth, UK.

Madhusudan, A., I. Symeonidis, M. A. Mustafa, R. Zhang and B. Preneel. (2019). “SC2Share: Smart Contract for Secure Car Sharing.” In: *5th International Conference on Information Systems Security and Privacy (ICISSP 2019)* (pp. 163–171). Prague, Czech Republic.

Maher, D. P. (2018). “On Software Standards and Solutions for a Trusted Internet of Things.” In: *51st Hawaii International Conference on System Sciences (HICSS 2018)* (pp. 5666–5675). Waikoloa, Hawaii, USA.

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

Mendling, J., G. Decker, H. A. Reijers, R. Hull and I. Weber. (2018). “How Do Machine Learning, Robotic Process Automation, and Blockchains Affect the Human Factor in Business Process Management?” *Communications of the Association for Information Systems*, *43*(1), 297–320.

Mendling, J., I. Weber, W. van der Aalst, J. vom Brocke, C. Cabanillas, F. Daniel, … L. Zhu. (2017). “Blockchains for Business Process Management - Challenges and Opportunities.”

ACM Transactions on Management Information Systems, *9*(1), 1–16.

Mengelkamp, E., J. Gärttner, K. Rock, S. Kessler, L. Orsini and C. Weinhardt. (2018). "Designing Microgrid Energy Markets: A Case Study: The Brooklyn Microgrid." *Applied Energy*, *210*(1), 870–880.

Mercuri, R. T. (2004). "The HIPAA-Potamus in Health Care Data Security." *Communications of the ACM*, *47*(7), 25–28.

Miscione, G., R. Ziolkowski, L. Zavolokina and G. Schwabe. (2018). "Tribal Governance: The Business of Blockchain Authentication." In: *51st Hawaii International Conference on System Sciences (HICSS 2018)* (pp. 4484–4493). Waikoloa, Hawaii, USA.

Möhring, M., B. Keller, R. Schmidt and J. Schulz. (2018). "Empirical Insights in the Current Development of Smart Contracts." In: *22nd Pacific Asia Conference on Information Systems (PACIS 2018)* (pp. 146–154). Yokohama, Japan.

Morabito, V. (2017). "Smart Contracts and Licensing." In: *Business Innovation Through Blockchain* (pp. 101–124). Springer, Cham.

Morisse, M. (2015). "Cryptocurrencies and Bitcoin: Charting the Research Landscape." In: *21st Americas Conference on Information Systems (AMCIS 2015)* (pp. 1–16). Fajardo, Puerto Rico.

Mrosek, R., T. Dehling and A. Sunyaev. (2015). "Taxonomy of Health IT and Medication Adherence." *Health Policy and Technology*, *4*(3), 215–224.

Naerland, K., C. Müller-Bloch, R. Beck and S. Palmund. (2017). "Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments." In: *38th International Conference on Information Systems (ICIS 2017)* (pp. 1–16). Seoul, South Korea.

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." *Www.Bitcoin.Org*.

Nickerson, R. C., U. Varshney and J. Muntermann. (2013). "A Method for Taxonomy Development and its Application in Information Systems." *European Journal of Information Systems*, *22*(3), 336–359.

Nizamuddin, N., H. Hasan, K. Salah and R. Iqbal. (2019). "Blockchain-Based Framework for Protecting Author Royalty of Digital Assets." *Arabian Journal for Science and Engineering*, *44*(4), 3849–3866.

Nofer, M., P. Gomber, O. Hinz and D. Schiereck. (2017). "Blockchain - A Disruptive Technology." *Business & Information Systems Engineering*, *59*(3), 183–187.

Notheisen, B., J. B. Cholewa and A. P. Shanmugam. (2017). "Trading Real-World Assets on Blockchain: An Application of Trust-Free Transaction Systems in the Market for Lemons." *Business and Information Systems Engineering*, *59*(6), 425–440.

Notheisen, B., F. Hawlitschek and C. Weinhardt. (2017). "Breaking Down the Blockchain Hype – Towards a Blockchain Market Engineering Approach." In: *25th European Conference on Information Systems (ECIS 2017)* (pp. 1062–1080). Guimarães, Portugal.

Oliveira, L., L. Zavolokina, I. Bauer and G. Schwabe. (2018). "To Token or not to Token: Tools for Understanding Blockchain Tokens." In: *39th International Conference on Information Systems (ICIS 2018)* (pp. 1–17). San Francisco, USA.

Ølnes, S. (2016). "Beyond Bitcoin Enabling Smart Government Using Blockchain Technology." In: *15th International Conference on Electronic Government (EGOV 2019)* (pp. 253–264). Guimarães, Portugal.

Otte, P., M. de Vos and J. Pouwelse. (2020). "TrustChain: A Sybil-Resistant Scalable Blockchain." *Future Generation Computer Systems*, *107*, 770–780.

Parra Moyano, J. and O. Ross. (2017). "KYC Optimization Using Distributed Ledger Technology." *Business and Information Systems Engineering*, *59*(6), 411–423.

Pedersen, A., M. Risius and R. Beck. (2019). "A Ten-Step Decision Path to Determine When to Use Blockchain Technologies." *MIS Quarterly Executive*, *18*(2), 99–115.

Peffers, K., T. Tuunanen, M. A. Rothenberger and S. Chatterjee. (2007). "A-Design Science Research Methodology for Information Systems Research." *Journal of Management Information Systems*, *24*(3), 45–77.

Peffers, K., T. Tuunanen, M. A. Rothenberger and S. Chatterjee. (2008). "A-Design Science Research Methodology for Information Systems Research." *Journal of Management Information Systems*, *24*(3), 45–77.

Peters, G., E. Panay I. and A. Chapelle. (2015). "Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective." *Journal of Financial Perspectives*, *3*(3), 1–46.

Pongnumkul, S., C. Siripanpornchana and S. Thajchayapong. (2017). "Performance Analysis of Private Blockchain Platforms in Varying Workloads." In: *26th International Conference on Computer Communications and Networks (ICCCN 2017)* (pp. 1–6). Vancouver, Canada.

Pries-Heje, J., R. Baskerville and J. Venable. (2008). "Strategies for Design Science Research Evaluation." In: *16th European Conference on Information Systems (ECIS 2008)* (pp. 1–13). Galway, Ireland.

Pureswaran, V., S. Panikkar, S. Nair and P. Brody. (2015). *Empowering the Edge: Practical Insights on a Decentralized Internet of Things*. *IBM Institute of Business Value* (Vol. 17).

Quinan, J. and C. Alexander. (1977). *A Pattern Language: Towns, Buildings, Construction*. *Oxford university press*.

Ray, G., W. Muhanna and J. Barney. (2005). "Information Technology and the Performance of the Customer Service Process: A Resource-Based Analysis." *MIS Quarterly*, *29*(4), 625–652.

Reid, F. and M. Harrigan. (2013). "An Analysis of Anonymity in the Bitcoin System." In: *Security and Privacy in Social Networks* (pp. 197–223). Springer, New York.

Risius, M. and K. Spohrer. (2017). "A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There." *Business and Information Systems Engineering*, *59*(6), 385–409.

Rockart, J. F. (1988). "The Line Takes the Leadership - IS Management in a Wired Society." *Sloan Management Review*, 1–26.

Rückeshäuser, N. (2017). "Typology of Distributed Ledger Based Business Models Typology of Distributed Ledger Based Business Models." *Twenty-Fifth European Conference on Information Systems*.

Ruj, S., M. S. Rahman, A. Basu and S. Kiyomoto. (2018). "BlockStore: A Secure Decentralized

Storage Framework on Blockchain." In: *32nd International Conference on Advanced Information Networking and Applications (AINA 2018)* (pp. 1096–1103). Cracow, Poland.

Rutkin, A. (2016). "Blockchain Aids Solar Sales." *New Scientist*, *231*(3088), 1–22.

Sadhya, V. and H. Sadhya. (2018). "Barriers to Adoption of Blockchain Technology." In: *24th Americas Conference on Information Systems (AMCIS 2018)* (pp. 1–10). New Orleans, USA.

Salviotti, G., L. M. de Ross I. and N. Abbatemarco. (2018). "A Structured Framework to Assess the Business Application Landscape of Blockchain Technologies." In: *51st Hawaii International Conference on System Sciences (HICSS 2018)* (pp. 3467–3476). Waikoloa, Hawaii, USA.

Savelyev, A. (2017). "Contract Law 2.0: Smart Contracts as the Beginning of End of Classic Contract Law." *Information and Communications Technology Law*, *26*(2), 116–134.

Schlegel, M., L. Zavolokina and G. Schwabe. (2018). "Blockchain Technologies from the Consumers' Perspective: What Is There and Why Should Who Care?" In: *51st Hawaii International Conference on System Sciences (HICSS 2018)* (pp. 3477–3486). Waikoloa, Hawaii, USA.

Schneider, S., J. Lansing, F. Gao and A. Sunyaev. (2014). "A Taxonomic Perspective on Certification Schemes: Development of a Taxonomy for Cloud Service Certification Criteria." In: *47th Hawaii International Conference on System Sciences (HICSS 2014)* (pp. 4998–5007). Waikoloa, Hawaii, USA.

Schollmeier, R. (2001). "A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications." In: *1st International Conference on Peer-to-Peer Computing (IEEE 2001)* (pp. 101–102). Linkoping, Sweden.

Scholz, T. and V. Stein. (2018). "The Architecture of Blockchain Organization." In: *39th International Conference on Information Systems (ICIS 2018)* (pp. 1–17). San Francisco, USA.

Schrader, U. and T. Hennig-Thurau. (2009). "VHB-JOURQUAL2: Method, Results, and Implications of the German Academic Association for Business Research's Journal Ranking." *Business Research*, *2*(2), 180–204.

Schwarz, A. and R. Hirschheim. (2003). "An extended platform logic perspective of IT governance: Managing perceptions and activities of IT." *Journal of Strategic Information Systems*, *12*(2), 129–166.

Schweizer, A., V. Schlatt, N. Urbach and G. Fridgen. (2017). "Unchaining Social Businesses–Blockchain as the Basic Technology of a Crowdlending Platform." In: *38th International Conference on Information Systems (ICIS 2017)* (pp. 1–21). Seoul, South Korea.

Seebacher, S. (2018). "A Model-driven Approach for the Description of Blockchain Business Networks." In: *51st Hawaii International Conference on System Sciences (HICSS 2018)* (pp. 3487–3496). Waikoloa, Hawaii, USA.

Sharples, M. and J. Domingue. (2016). "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward." In: *European Conference on Technology Enhanced Learning (EC-TEL 2016)* (pp. 490–496). Lyon, France.

Singh, S. and N. Singh. (2016). "Blockchain: Future of Financial and Cyber Security." In: *2nd International Conference on Contemporary Computing and Informatics (IC3I2016)* (pp. 463–467). Noida, India.

Strauss, A. and J. Corbin. (1990). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Sage Publications, Inc.

Strauss, A. L. (1987). *Qualitative Analysis for Social Scientists*. *Cambridge University Press* (Vol. 1). Cambridge University Press.

Sunyaev, A., J. M. Leimeister, A. Schweiger and H. Krcmar. (2008). "IT-Standards and Standardization Approaches in Healthcare." In: *Encyclopedia of Healthcare Information Systems* (pp. 813–820). Medical Information Science Reference, New York.

Swan, M. (2015a). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc.

Swan, M. (2015b). "Blockchain Thinking: The Brain as a Decentralized Autonomous Corporation." *IEEE Technology and Society Magazine*, *34*(4), 41–52.

Szabo, N. (1997). "Formalizing and Securing Relationships on Public Networks." *First Monday, 2*(9).

Tallon, P. (2007). "A Process-Oriented Perspective on the Alignment of Information Technology and Business Strategy." *Journal of Management Information Systems, 24*(3), 227–268.

Tapscott, D. and A. Tapscott. (2017). "How Blockchain Will Change Organizations." *MIT Sloan Management Review, 58*(2), 10–13.

The Economist. (2015). "The Trust Machine-The Promise of Blockchain," 2–4.

The European Parliament and The European Council. (2016). "General Data Protection Regulation." *Official Journal of the European Union, 14*(5), 20–30.

Tönnissen, S. and F. Teuteberg. (2018). "Towards a Taxonomy for Smart Contracts." In: *26th European Conference on Information Systems (ECIS 2018)* (pp. 1–15). Portsmouth, UK.

Trujillo, J. L., S. Fromhart and V. Srinivas. (2017). *Evolution of blockchain technology Insights from the GitHub platform*. *Deloitte Insights*.

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

Vom Brocke, J., A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, A. Cleven, K. Reimer. (2009). "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process." In: *17th European Conference on Information Systems (ECIS 2009)* (pp. 2206–2217). Verona, Italy.

Vukolić, M. (2017). "Rethinking Permissioned Blockchains." In: *1st ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC 2017)* (pp. 3–7). Abu Dhabi, UAE.

Walsh, C., P. O'Reilly, R. Gleasure, J. Feller, L. Shanping and J. Cristoforo. (2016). "New Kid on the Block: A Strategic Archetypes Approach to Understanding the Blockchain." In: *37th International Conference on Information Systems (ICIS 2016)* (pp. 1–12). Dublin, Irland.

Wang, L., X. R. Luo and B. Xue. (2018). "Too Good to Be True? Understanding How Blockchain Revolutionizes Loyalty Programs." In: *24th Americas Conference on Information Systems (AMCIS 2018)* (pp. 1–10). New Orleans, USA.

Watanabe, H., S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami. (2015). "Blockchain Contract: A Complete Consensus Using Blockchain." In: *4th Global Conference on Consumer Electronics (GCCE 2015)* (pp. 577–578). Ōsaka, Japan.

Webster, J. and R. T. Watson. (2002). "Analyzing the Past to Prepare for the Future: Writing a Literature Review." *MIS Quarterly*, *26*(2), 13–23.

Welpe, I., L. Zavolokina, H. Krcmar and P. Mehrwald. (2020). "Distributed Ledger Technology, Blockchain Minitrack." In: *53rd Hawaii International Conference on System Sciences (HICSS 2020)* (pp. 4021–4022). Wailea, Hawaii, USA.

Wiesche, M., M. C. Jurisch, P. W. Yetton and H. Krcmar. (2017). "Grounded Theory Methodology in Information Systems Research." *MIS Quarterly*, *41*(3), 685–701.

Wilkinson, S., T. Boshevski, J. Brandoff, J. Prestwich, G. Hall, P. Gerbes, C. Pollard. (2014). *Storj A Peer-to-Peer Cloud Storage Network*. *Storj.io*.

Winter, R., A. Gericke and T. Bucher. (2009). *Method versus Model - Two Sides of the Same Coin? Advances in Enterprise Engineering III*. Springer, Berlin, Heidelberg.

Wohrer, M. and U. Zdun. (2018). "Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solidity." In: *International Workshop on Blockchain Oriented Software Engineering (IWBOSE 2018)* (pp. 2–8). Campobasso, Italy.

Wörner, D., T. Von Bomhard, Y.-P. Schreier and D. Bilgeri. (2016). "The Bitcoin Ecosystem: Disruption beyond Financial Services?" In: *24th European Conference on Information Systems (ECIS 2016)* (pp. 1–16). Istanbul, Turkey.

Wüst, K. and A. Gervais. (2018). "Do You Need a Blockchain?" In: *1st Crypto Valley Conference on Blockchain Technology (CVCBT 2018)* (pp. 1–7). Zug, Switzerland.

Xu, X., C. Pautasso, L. Zhu, Q. Lu and I. Weber. (2018). "A Pattern Collection for Blockchain-Based Applications." In: *23rd European Conference on Pattern Languages of Programs (EuroPLoP 2018)* (pp. 1–20). Irsee, Germany.

Xu, X., I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, P. Rimba. (2017). "A Taxonomy of Blockchain-Based Systems for Architecture Design." In: *International Conference on Software Architecture (ICSA 2017)* (pp. 243–252). Gothenburg, Sweden.

Yli-Huumo, J., D. Ko, S. Choi, S. Park and K. Smolander. (2016). "Where is Current Research on Blockchain Technology?-A Systematic Review." *PLoS ONE*, *11*(10), 1–27.

Yuan, R., Y. Xia, H. Chen, B. Zang and J. Xie. (2018). "ShadowEth: Private Smart Contract on Public Blockchain." *Journal of Computer Science and Technology*, *33*(1), 542–556.

Zhang, C., R. Sharma and S. Wingreen. (2018). "Block-Chaining in Precision HealthCare: A Design Research Approach." In: *22nd Pacific Asia Conference on Information Systems (PACIS 2018)* (pp. 1–8). Yokohama, Japan.

Ziegeldorf, J. H., F. Grossmann, M. Henze, N. Inden and K. Wehrle. (2015). "CoinParty: Secure Multi-Party Mixing of Bitcoins." In: *5th ACM Conference on Data and Application Security and Privacy* (pp. 75–86). San Antonio, USA.

Ziolkowski, R., G. Miscione and G. Schwabe. (2018). "Consensus through Blockchains: Exploring Governance across Inter-Organizational Settings." In: *39th International Conference on Information Systems (ICIS 2018)* (pp. 1–17). San Francisco, USA.

Curriculum Vitae. Olga Labazova

Address	Overbeckstr. 67, 50823 Cologne, Germany
E-mail	labazova@wiso.uni-koeln.de
Phone	+49 163 7571378

RESEARCH POSITION AND INTERESTS

2016 – 2019	*PhD. Fellow in Information Systems,* Cologne Graduate School in Management, Economics and Social Sciences (CGS), University of Cologne, Cologne, Germany
Research Interests	Blockchain; Distribution Ledger Technology, Internet of Things, Business Process Management, Enterprise Architecture
2018	*Research Stay,* Institute of Applied Informatics and Formal Description Methods, Karlsruhe Institute of Technology, Karlsruhe, Germany

EDUCATION

2014 – 2016	*Master Degree in Business Informatics,* National Research University «Higher School of Economics», Moscow, Russia Graduation: 1.0
2010 – 2014	*Bachelor Degree in Business Informatics,* National Research University «Higher School of Economics», Moscow, Russia Graduation: 1.7

PROFESSIONAL EXPERIENCE

2019 – current	*Data Engineer,* AXA, Cologne, Germany
2014 – 2016	*Business Development Consultant,* Oracle Corporation, Moscow, Russia
2015 – 2016	*Analyst,* National Research University «Higher School of Economics», Moscow, Russia
2015 – 2015	*Research Assistant,* National Research University «Higher School of Economics», Moscow, Russia
2013 – 2014	*Junior Consultant,* SGS Project, Moscow, Russia
2013 – 2013	*Software Test Engineer,* S&T International, Moscow, Russia
2010 – 2013	*Computer Operator,* National Research University «Higher School of Economics», Moscow, Russia

SCHOLARSHIPS AND AWARDS

2016 – 2019	*CGS-Research Scholarship,* Cologne Graduate School in Management, Economics and Social Sciences, University of Cologne, Cologne, Germany
December 2017	*The Winner of Future Blockchain Hackathon,* Deutsche Telekom, Bonn, Germany
2015 – 2016	*Scholarship for Outstanding Academic Achievements,* National Research University «Higher School of Economics», Moscow, Russia
2013 – 2016	*Scholarship for Outstanding Achievements in Sport,* National Research University «Higher School of Economics», Moscow, Russia

PUBLICATIONS

2018	Labazova, O. "Exploring Blockchain Applications in Service Systems." In: *Doctoral Consortium, 9th International Conference on Exploring Service Science (IESS 2018)*. Karlsruhe, Germany.
2019	Labazova, O., T. Dehling, A. Sunyaev. "From Hype to Reality: A Taxonomy of Blockchain Applications." In: *52nd Hawaii International Conference on System Sciences (HICSS 2019)* (pp. 4555–4564). Waikoloa, Hawaii, USA (published).
2019	Labazova, O. "Towards a Framework for Evaluation of Blockchain Implementations." In: *40th International Conference on Information Systems (ICIS 2019)* (pp. 1-16). Munich, Germany (published).
2020	Klein, S., Prinz W., Gräther W., Labazova O. "Smart Contract Design Patterns to Assist Blockchain Conceptualization." In: *28th European Conference on Information Systems (ECIS 2020)*. Marrakech, Morocco (submitted, under review).
2020	Labazova, O., Kazan E., Dehling T., Tuunanen T., Sunyaev A. "Managing Blockchain Systems and Applications: A Process Model for Blockchain Configurations." *Electronic Markets* (revise & resubmit).

VOLUNTEERING

Reviewer	Academy of Management Annual Meeting
	Multikonferenz Wirtschaftsinformatik
	International Conference on Information Systems
	European Conference on Information Systems
Supervisor	Master & Bachelor Thesis
	The topics include but are not limited to Blockchain applications, Blockchain in healthcare, Blockchain for open science, smart contracts
Organizer	FORCE11-Blockchain Workshop Berlin 2017
Speaker	Conferences & Meetups & Workshops (e.g., Hack Share Berlin 2017, 3rd For Digital Blockchain Workshop Karlsruhe 2019)
Member	IFS-Mentoring: Mentoring Program for International Female Scholars, University of Cologne, Cologne, Germany
	Blockchain 4 Open Science

MISCELLANEOUS

Programming	C#, Java, Python
IT Software	SQL Server, Visual Studio, NoSQL DBs, MS Office (incl. Visio), Hyperledger, Ethereum, Oracle Applications, ARIS, Metasonic Suit, IBM Blue works live, Snowflake, Denodo, AWS.
Languages	English (fluent, IELTS, GMAT), German (intermediate), Russian (native)
Hobbies	Public Speaking and Leadership, (Scientific) Writing, Football, Martial Arts, Traveling, Classical Music, Classical/Modern Art

Cologne, February 2020. Olga Labazova