Association for Information Systems

AIS Electronic Library (AISeL)

ICIS 2019 Proceedings

DLT, Blockchain and FinTech

Towards a Framework for Evaluation of Blockchain Implementations

Olga Labazova
University of Cologne, labazova@wiso.uni-koeln.de

Towards a Framework for Evaluation of Blockchain Implementations

Completed Research Paper

Olga Labazova
University of Cologne
Albertus-Magnus-Platz, 50923, Cologne, Germany
labazova@wiso.uni-koeln.de

Abstract

Organizations appear to implement blockchain solutions based on fear of missing out instead of a clear understanding of blockchain usefulness. Actually, 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 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.

Keywords: Blockchain, distributed ledger technology, Bitcoin

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, business value is collectively generated by nodes, and cooperation on intra- and inter-organizational levels is 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, Panayi and Chapelle, 2015; Schlegel, Zavolokina and Schwabe, 2018). Further, blockchain integration and the interconnection between nodes are not limited to one organization but require inter-organizational collaboration (Fridgen, Schweizer, Regner and Urbach, 2018; Oliveira 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 manuscript 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, March, Park and Ram, 2004). For data collection, we use the scientific literature that helps us to arrive at a set of blockchain evaluation factors. Based on IT artifacts 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 manuscript. Practitioners can use the framework to understand the main factors of success or failure of blockchain implementations beforehand.

We structure the manuscript 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.

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 1).

Public permissionless (Bitcoin) blockchains are fully decentralized blockchains where everyone can read, write, and validate information (Beck, Müller-Bloch and King, 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 finding (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 1. 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)

Table 1. Blockchain Types

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.

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, Egelund-mu, Henglein and Ross, 2017). Cross-organizational workflow management in a German bank case can run on blockchains (Fridgen, Radszuwill, Urbach and Utz, 2018). Besides, blockchain prototypes can reduce costs of know-your-customer verification processes and revolutionize loyalty programs (Wang, Luo and Xue, 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, Risius and Friis, 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; Hua et al., 2018; Lacity, 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, Müller-Bloch, Beck and Palmund, 2017). Other blockchain proofs-of-concept enable the automated transaction of real-world assets such as diamonds (Notheisen, Cholewa and Shanmugam, 2017; Loebbecke, Lueneborg and Niederle, 2018). For social businesses, blockchain is a basic technology of crowdlending platforms and social networking practices (Schweizer et al., 2017; Ciriello, Beck and Thatcher, 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 and Weinhardt, 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, Radszuwill, Rieger and Urbach, 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, Tan and Lim, 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, Schweizer, Regner and Urbach, 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, Miscione and Schwabe, 2018). For the detailed description, we refer to the original research projects.

Methodology

This study follows a Design Science Research approach that guides developing IT artifacts and their use in practice (Hevner et al., 2004; Peffes, Tuunanen, Rothenberger and Chatterjee, 2008). Developing IT artifacts 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 artifacts in the blockchain domain. To strengthen the quality of our artifact, we utilized DSR methodology for information systems research (Peffers et al., 2008), which comprises six steps: problem identification, objective definition, design and development, demonstration, evaluation, and communication (Figure 1).

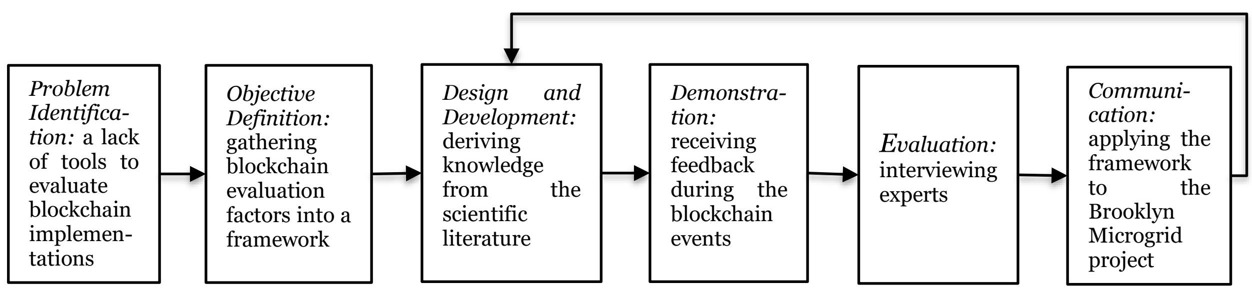

Figure 1. Methodology of Developing a Framework for Evaluation of Blockchain Implementations. Adopted from Peffers et al. (2008)

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

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.

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

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 manuscripts. 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 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).

Data Analysis. For data analysis, we applied open coding for initial categorization of blockchain concepts and axial coding for removal of overlapping concepts while iteratively testing the concepts against data (Strauss and Corbin, 1990). If available, we also coded the theoretical foundations that were used to delineate and structure interconnections between factors. Next, we aggregated the factors in broader categories that were derived from the analysis 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 found in the scientific texts from the literature review. 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 artifacts (Notheisen, Hawlitschek, et al., 2017). Afterwards, the four categories were aligned with four main evaluation steps that guide the evaluation of blockchain implementations.

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

Evaluation. To evaluate our results, we conducted a first set of interviews (seven semistructured 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 via 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 of 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 literature. Therefore, we asked the same experts for the phone or e-mail feedback on the new versions. All experts provided the feedback.

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 the secondary data.

A Framework for Evaluation of Blockchain Implementations

Figure 2 shows a framework for 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*.

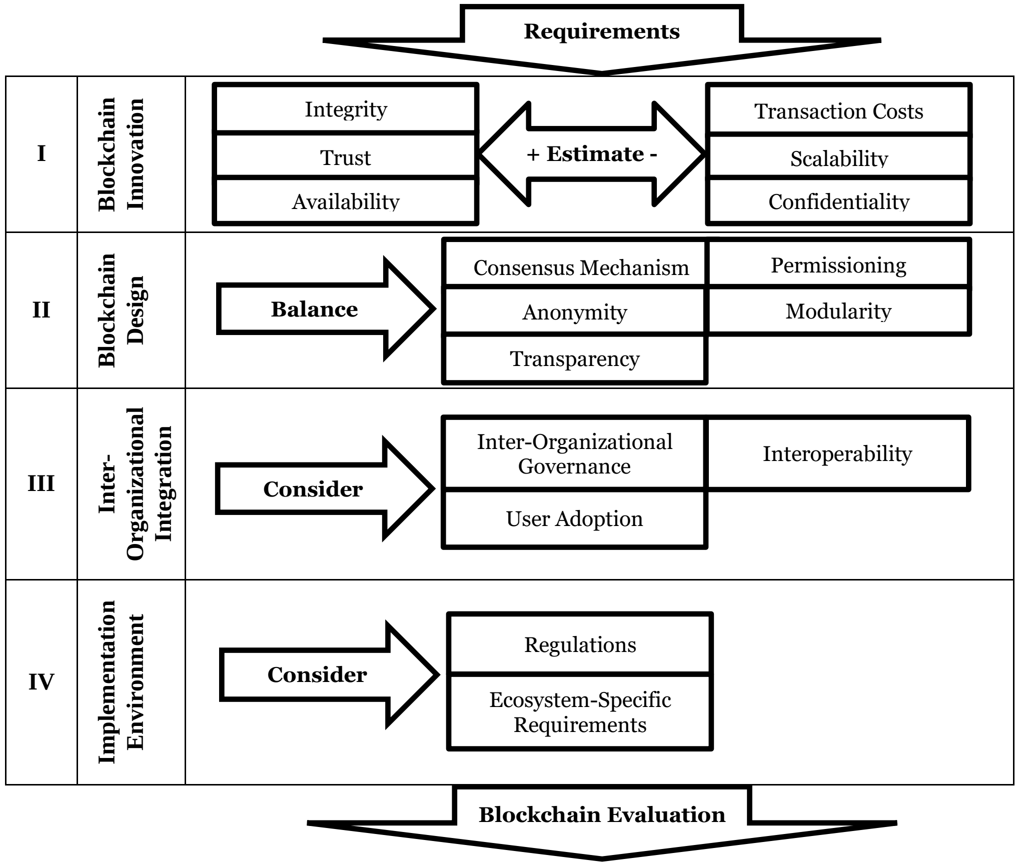

Figure 2. A Framework for Evaluation of Blockchain Implementations

Blockchain Innovation

First, an estimation of the blockchain suitability to 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, 2017). Implementations can benefit from 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 is a number of 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 as the probability of a system to be accessed when needed (Xu et al., 2017). In blockchain systems, availability is offered through data replication across nodes (Wüst and Gervais, 2017) 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, 2017).

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. In addition, 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 of time (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.

Blockchain Design

Blockchain designs aim to minimize losses and maximize benefits of blockchains according to project requirements. The first and main factor is **the 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 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 with respect to 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).

The anonymity of users assesses with what accuracy users can be matched to particular identities. For example, users are *pseudonymous* in case of Bitcoin and *anonymous* in 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 favor 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 of 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 with regard to 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).

The 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.

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. "I think, 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 own 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.

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. "I think 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, 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, Fedcoin, 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.

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.

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).

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, Rossi and Abbatemarco, 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 (Notheisen, Hawlitschek, et 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).

User adoption → confidentiality, integrity, transaction costs, 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).

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 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 individual participant. Confidentiality in a public system can be achieved using cryptographic techniques but typically comes at the cost of lower efficiency (Wüst and Gervais, 2017). Non-transparent data on blockchains is 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.

Regulations → interoperability: to exchange data between systems, it is necessary to consider compatibility and network externalities and use the same formats and semantics. "I do not think that the interoperability is an issue right now; also, I do not think that blockchains force to use data standards as much as possible. In the near future, the interoperability will emerge from the use cases affecting data standards" (I2).

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).

<u>Blockchain innovation.</u> 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 contradicts 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 clearly 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).

<u>Blockchain design.</u> 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.

<u>Inter-organizational integration.</u> 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).

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 of existing 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).

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, an 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 important factor and regulations of the energy sector are not supported peer-to-peer energy trading to consider the specific effect on interoperability.

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 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 mechanism* should be more suitable to maximize performance metrics of adopting blockchains (Mengelkamp et al., 2018). Also, *regulations should be developed on the national and inter-national levels*.

Discussion

The framework for evaluation of blockchain implementations comprises factors that are important to consider before blockchain projects begin. Factors are grouped in 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, permissioning, 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 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 manuscript 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 manuscript. Second, we do not go into technical specifics with respect to 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 the proposed concepts for the 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, Hawlitschek, et al., 2017).

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.

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.

References

Albrecht, S., Reichert, S., Schmid, J., Strüker, J., Neumann, D., and Fridgen, G. 2018. "Dynamics of

Blockchain Implementation - A Case Study from the Energy Sector," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, Waikoloa, Hawaii, USA, pp. 3527–3536.

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

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

Beck, R., Czepluch, S., Lollike, N. N., Malone, S. 2016. "Blockchain - The Gateway to Trust-Free Cryptographic Transactions," in *Proceedings of the 24th European Conference on Information Systems,* Istanbul, Turkey, pp. 1-14.

Ciriello, R. F., Beck R., and Thatcher, J. B. 2018. "The Paradoxical Effects of Blockchain Technology on Social Networking Practices," in *Proceedings of the 39th International Conference on Information Systems*, San Francisco, California, USA, pp. 1-19.

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I. … Juels, A. 2019. "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," *arXiv preprint (arXiv:1904.05234)*.

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

Fridgen, G., Radszuwill, S., Rieger, A., and Urbach, N. 2018. "A Solution in Search of a Problem: A Method for the Development of Blockchain Use Cases," in *Proceedings of the 24th Americas Conference on Information Systems*, New Orleans, Louisiana, USA, pp. 1-10.

Fridgen, G., Radszuwill, S., Urbach N., and Utz, L. 2018. "Cross-Organizational Workflow Management Using Blockchain Technology – Towards Applicability, Auditability, and Automation," in *Proceedings of the 51st Hawaii International Conference on System Sciences,* Waikoloa, Hawaii, USA, pp. 3507-3516.

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

Furlonger, D., and Valdes, R. 2017. *Practical Blockchain: A Gartner Trend Insight Report*. Retrieved from https://www.gartner.com/document/3628617?ref=solrAll&refval=182700378&qid=a89318613984fd5789d202a1f0d1f680.

Glaser, F. (2017). "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis," in *Proceedings of the 50th Hawaii International Conference on System Sciences,* Waikoloa, Hawaii, USA, pp. 1543–1552.

Glaser, F., and Bezzenberger, L. 2015. "Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems," in *Proceedings of the 23rd European Conference on Information Systems,* Münster, Germany, pp. 1–18.

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

Hua, S., Sun, J., Zhou, E., Nomura, Y., Laboratories, F., Pi, B., … Laboratories, F. 2018. "Apply blockchain technology to electric vehicle battery refueling," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, Waikoloa, Hawaii, USA, pp. 4494–4502.

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

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

Labazova, O., Dehling, T., and Sunyaev, A. 2019. "From Hype to Reality: A Taxonomy of Blockchain Applications," in *Proceedings of the 52nd Hawaii International Conference on System Sciences,* Waikoloa, Hawaii, USA, pp. 4556-4564.

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

Loebbecke, C., Lueneborg, L., and Niederle, D. 2018. "Blockchain Technology Impacting the Role of Trust in Transactions : Reflections in the Case of Trading Diamonds," in *Proceedings of the 26th European Conference on Information Systems*, Portsmouth, UK, pp. 1-11.

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini L., and Weinhardt, C. 2018. "Designing microgrid energy markets: A case study: The Brooklyn Microgrid," *Applied Energy* (210), pp. 870-880.

Naerland, K., Müller-Bloch, C., Beck, R., and Palmund, S. 2017. "Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments," in *Proceedings of the 38th International conference on information systems*, Seoul, South Korea, pp. 1–16.

Nakamoto, S. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Www.Bitcoin.Org*, pp. 1-9.

Notheisen, B., Cholewa, J. B., and Shanmugam, A. P. 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), pp. 425–440.

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

Oliveira, L., Zavolokina, L., Bauer, I., and Schwabe, G. 2018. "To Token or not to Token: Tools for Understanding Blockchain Tokens," in *Proceedings of the 39th International Conference on Information Systems,* San Francisco, California, USA, pp. 1-17.

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

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

Risius, M., and Spohrer, K. 2017. "A Blockchain Research Framework," *Business and Information Systems Engineering* (59:6), pp. 385-409.

Rückeshäuser, N. 2017. "Typology of Distributed Ledger Based Business Models Typology of Distributed Ledger Based Business Models," in *Proceedings of the 25th European Conference on Information Systems*, Guimarães, Portugal, pp. 2201-2217.

Salviotti, G., De Rossi, L. M., and Abbatemarco, N. 2018. "A Structured Framework to Assess the Business Application Landscape of Blockchain Technologies," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, Waikoloa, Hawaii, USA, pp. 3467–3476.

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

Schweizer, A., Bayreuth, U., Schlatt, V., Bayreuth, U., Urbach, N., and Fridgen, G. 2017. "Unchaining Social Businesses – Blockchain as the Basic Technology of a Crowdlending Platform," in *Proceedings of the 38th International conference on information systems*, Seoul, South Korea, pp. 1–21.

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

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

Tönnissen, S., and Teuteberg, F. 2018. "Towards a Taxonomy for Smart Contracts," in *Proceedings of the 26th European Conference on Information Systems,* Portsmouth, UK, pp. 1-14.

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

Wang, L., Luo, X. R., and Xue, B. 2018. "Too Good to Be True ? Understanding How Blockchain Revolutionizes Loyalty Programs," in *Proceedings of the 24th Americas Conference on Information Systems*, New Orleans, Louisiana, USA, pp. 1–10.

Wüst, K., and Gervais, A. 2017. "Do you need a Blockchain?," *IACR Cryptology EPrint Archive*, 1–7.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., … Rimba, P. 2017. "A Taxonomy of Blockchain-Based Systems for Architecture Design," in *Proceedings of the IEEE International Conference on Software Architecture,* pp. 243–252.

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

Ziolkowski, R., Miscione, G., and Schwabe, G. 2018. "Consensus through Blockchains: Exploring Governance across inter-organizational Settings," in *Proeedings of the 39th International Conference on Information Systems*, San Francisco, California, USA, pp. 1-17.

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 & 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 & King, 2018	X	X	X						X	X		X									
Beinke & Ngoc, 2018	X	X	X	X	X							X									
Bonneau et al., 2015	X		X	X	X	X	X	X							X						
Brenig, Schwarz & Rückeshäuser, 2016	X	X		X				X				X	X								
Chanson, Risius & 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 & 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 & Bezzenberger,2015	X	X		X	X		X	X							X	X					
Hawlitschek, Notheisen & 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 & 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			
Li et 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 & Spohrer, 2017	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X		X
Sadhya & Sadhya, 2018	X	X	X	X	X	X	X	X	X			X	X		X	X					
Salviotti, Rossi & Abbatemarco, 2018	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X			
Scholz & Stein, 2018	X	X	X	X	X	X	X	X	X	X		X		X	X	X	X	X		X	
Schlegel, Zavolokina & 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&Teuteberg,2018	X	X	X	X		X		X							X	X					
Tschorsch & 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 & 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

Appendix A. A Factor Matrix.