The Use of Distributed Ledger Technology in Compliance: A Review of the Current State of Research

Bachelor Thesis

by

Frederic von Normann

Degree Course: Industrial Engineering and Management

Matriculation Number: 1959246

Institute for Applied Informatics and Formal Description Methods (AIFB)

KIT Department of Economics and Management

Advisor:	Prof. Dr. Ali Sunyaev
Second Advisor:	Prof. Dr. Andreas Oberweis
Supervisor:	Malte Greulich M.Sc.
Submitted:	30. October 2019

Abstract

The third generation of Distributed Ledger Technology (DLT) allows advanced and various applications with Smart Contracts in an environment of interconnected organizations, external entities and real-world processes. Many organizations operate in such an environment and are engaged with compliance requirements, such as laws and regulation. This leads to a multitude of challenges for organizations. For the most part, organizations lack a general understanding of this emerging technology regarding the use in compliance. Therefore, we present in this work, based on a literature review, an overview what challenges DLT is able to address and what risks could emerge through the use of DLT in this area of application. Moreover, we differentiate the effects of single DLT characteristics addressing different compliance challenges and discuss important controversial aspects (e.g. integrity of data vs. GDPR requirements). We further discuss the suitability of the most common DLT designs, Ethereum and Hyperledger, in the context of compliance and provide a brief outlook on illustrative business use cases for DLT in compliance.

Table of Content

Abstract ..... **II**
List of Abbreviations ..... **IV**
List of Figures ..... **V**
List of Tables ..... **VI**
1. Introduction **1**
2. Background on Compliance and Distributed Ledger Technology **2**
2.1. Compliance 2
2.1.1. Definition Organizational Compliance 2
2.1.2. Challenges in Compliance 2
2.2. Distributed Ledger Technology 5
2.2.1. Definition DLT 5
2.2.2. Key Concepts 7
2.2.3. DLT Characteristics 11
3. Research Method **13**
3.1. Literature Search 13
3.2. Literature Analysis 14
4. Results of Literature Review **17**
4.1. Descriptive Results of Literature Search 17
4.2. DLT Concepts and Designs 17
4.3. DLT for Challenges in Compliance 19
4.4. Risks Through the Use of DLT 26
4.5. Business Use Cases of DLT in Compliance 29
5. Discussion **29**
6. Conclusion **37**
6.1. Limitations of this Work 38
6.2. Future Research 39
Appendix **40**
A. List of Relevant Literature with Reference Number 40
B. Concept Matrix C-1: DLT Concepts and Designs 41
C. Concept Matrix C-2: Challenges in Compliance 42
D. Concept Matrix C-2: Risks Through the Use of DLT 58
E. Concept Matrix C-3: Business Use Cases 64
References **66**
Declaration about the Thesis **73**

List of Abbreviations

ACM DL	Association for Computing Machinery Digital Library
AISeL	Association of Information Systems electronic Library
BFT	Byzantine Fault Tolerance
blockDAG	Block Directed Acyclic Graph
BPC	Business Process Compliance
BPM	Business Process Management
CBM	Circular Business Model
CIP	Critical Infrastructure Protection
DLT	Distributed Ledger Technology
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IEEE Xplore DL	Institute of Electrical and Electronics Engineers Digital Library
IFRS	International Financial Reporting Standards
IPFS	InterPlanetary File System
ISO	International Standard Organization
KYB	Know Your Business
KYC	Know Your Customer
MDO	Multi-Disciplinary Optimization
NERC	North American Electric Reliability Corporation
OLTP	Online Transaction Processing
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance
PoS	Proof of Stake
PoW	Proof of Work
TDAG	Transaction-based Directed Acyclic Graphs
TPA	Third-Party Auditor
TTP	Trusted Third Party

List of Figures

Figure 1: A Distributed Ledger in a P2P Network 6
Figure 2: Model of the Blockchain concept and structure with Merkle Tree..... 8
Figure 3: Hierarchical Structure of DLT (adapted from Kannengießer et al. 2019b, p. 4). 8
Figure 4: A hermeneutic framework for the literature review process consisting of two major hermeneutic circles (adapted from Boell & Cecez-Kecmanovic, 2014, p. 264). 14
Figure 5: Literature Search and Selection Process Model (adapted from Lins & Sunyaev, 2017, p. 6). 17

List of Tables

Table 1: DLT Properties (adapted from Kannengießer et al. 2019b, p. 12). 11
Table 2: DLT Characteristics part 1 (adapted from Kannengießer et al. 2019b, p. 13). 11
Table 3: DLT Characteristics part 2 (adapted from Kannengießer et al. 2019b, p. 13-14). 12
Table 4: DLT Characteristics part 3 (adapted from Kannengießer et al. 2019b, p. 14). 13
Table 5: Schematic of Concept Matrix C-1: DLT Concepts and DLT Designs. 15
Table 6: Schematic of Concept Matrix C-2: DLT Characteristics vs. Challenges and Risks. 16
Table 7: Schematic of Concept Matrix C-3: Business Use Cases 16
Table 8: Breakdown of Concept Matrix C-1: DLT Concepts and DLT Designs. 18
Table 9: Master Variables: Challenges in Compliance 20
Table 10: Breakdown of Concept Matrix C-2: Challenges in Compliance 22
Table 11: Breakdown of Concept Matrix C-2: Challenges in Compliance 23
Table 12: Breakdown of Concept Matrix C-2: Challenges in Compliance 24
Table 13: Breakdown of Concept Matrix C-2: Challenges in Compliance 25
Table 14: Master Variables: Risks through the use of DLT 26
Table 15: Breakdown of Concept Matrix C-2: Risks through the use of DLT 27
Table 16: Breakdown of Concept Matrix C-2: Risks through the use of DLT 28

1. Introduction

In 2008, Satoshi Nakamoto, a pseudonym for an unknow person or group, proposed a protocol for the cryptographic currency Bitcoin (Nakamoto, 2008). The rise of Bitcoin and the development of more elaborated functions in other cryptocurrencies has fueled research efforts aimed at transferring the underlying idea of DLT to other contexts. DLT is the superordinate concept of a distributed shared database in a Peer-to-Peer (P2P) network composed of a certain number of storage devices, so-called nodes (Suciu et al., 2018, p. 370). Each of these nodes holds a consistent replica of the ledger, which has to be agreed upon in a consensus mechanism (Suciu et al., 2018, p. 370).

This unique structure of DLT provides favorable characteristics for organizational compliance, such as the transparency and integrity of data. In organizational compliance, organizations must ensure that their business processes, operations and practices are in accordance with compliance requirements, such as laws, standards and business partner contracts (Sadiq & Governatori, 2015, p. 265). Organizations face numerous different challenges to fulfill the compliance requirements. At the current state organizations face high and increasing costs and efforts to fulfill the compliance requirements (English & Hammond, 2018, p. 5). Potential consequences of non-compliance are high fines as well as legal disputes and bad reputation (English & Hammond, 2018, pp. 14–31). Therefore, organizations seek to use DLT to address those challenges, though in practice, the problem for many organizations is the lack of understanding, what specific challenges of compliance DLT is able to address. Furthermore, the emerging risks through the usage of DLT need to be taken into account. Finally, it remains unclear in what potential business use cases DLT can address those compliance challenges.

Prior research regarding DLT in compliance focuses mainly on the development of DLT-based concepts to address only selected compliance challenges and proposing illustrative business use cases (e.g. Shbair, Steichen, Francois, and State (2018), Kaaniche and Laurent (2017)). Thus, the current state of research lacks an overview of the potentials of DLT for compliance. This thesis seeks to address this gap by answering the following research question:

RQ: What are the potentials and risks for the use of DLT for organizational compliance?

Therefore, the main objective of this thesis is presenting an overview of the potentials of DLT to address the challenges of organizational compliance. Furthermore, the main objective is presenting an overview of the risks that emerge through the use of DLT in this particular area of application. This implies the sub-objectives: What characteristics of DLT are the key factors addressing these challenges? What DLT concepts and designs are promoted in the current research? What are concrete business use cases of DLT in compliance? This provides the basis for further research into the presented DLT solutions, in order to develop more advanced prototypes for real world business environments.

The thesis is structured into the following chapters: In chapter 2, we first define the terms of compliance and derive from this the compliance challenges that organizations must address. Then, we give an introduction into DLT, the underlying concepts and characteristics to provide the required technical background for the subsequent literature analysis. Chapter 3 explains the applied research method, how we gathered and analyzed relevant literature. In chapter 4 we describe quantitatively the results regarding DLT concepts and designs, the relationship between DLT characteristics and compliance challenges as well as risks and finally business use cases. In chapter 5 we discuss those results accordingly. In the conclusion, we not only summarize the research, but also point out the limitations of our work and provide a brief outlook for further research.

2. Background on Compliance and Distributed Ledger Technology

2.1. Compliance

2.1.1. Definition Organizational Compliance

In organizational compliance, organizations must ensure that their business processes, operations and practice are in accordance with compliance requirements (Sadiq & Governatori, 2015, p. 265). Compliance requirements have different sources. There are national or international laws, such as the Sarbanes-Oxley Act, a reform of public company accounting in the USA (Sadiq & Governatori, 2015, p. 265) or the General Data Protection Regulation (GDPR), an EU law regulating data protection and privacy. Furthermore, compliance requirements also stem from standards and codes of practice (Sadiq & Governatori, 2015, p. 265). For instance, the International Organization for Standardization (ISO) 9000 norm defines a family of quality management system standards and the International Financial Reporting Standards (IFRS) defines global accounting standards. Ultimately, contractual partners determine in business partner contracts the requirements and penalty clauses of non-compliance (Sadiq & Governatori, 2015, p. 265). For simplicity reasons, the term compliance will stand for organizational compliance throughout the remainder of this thesis.

2.1.2. Challenges in Compliance

Organizations face numerous different challenges in fulfilling the compliance requirements. Some of these challenges are independent from the organizational structure and the industrial sector. Other challenges depend strongly on these and other factors. To reach a basis of comparison and to gain a better overview, we generalized the challenges and categorized them according to Meironke, Seyffarth, and Damarowsky (2019) into five categories: Legal, organizational, technical, economic and human-centered challenges. We adopted the categorization of Meironke et al. (2019), since they provide a broad

overview of challenges in compliance and a reasonable categorization. This will allow us to structure our analysis and locate those categories, where DLT has strong potentials.

Legal Challenges

Legal challenges contain the challenges that derive from the nature of compliance requirements itself. Organizations face these challenges independent of their organizational structure or industrial sector. Maintaining compliance is a dynamic and complex process, the challenge is to adapt to constant and rapid changes of compliance requirements (Khan et al., 2017, p. 30; Schäfer, Fettke, & Loos, 2012, p. 348). Furthermore, new and changing requirements overlap with other requirements and even come into conflict with them (Sadiq, 2011, p. 1). This increases the complexity and the need for sufficient guidelines and expertise to interpret and translate the requirements individually for an organization (Turetken, Elgammal, van den Heuvel, & Papazoglou, 2011).

Organizational Challenges

Organizations are confronted with organizational challenges in compliance that derive among other things from the organizational structure, industrial sector and business environment. The size of the organization, the multitude and dynamics of businesses that are incorporated, as well as the degree of global operations are key factors for the complexity of compliance processes (Fdhila, Rinderle-Ma, Knuplesch, & Reichert, 2015, p. 165; Sadiq, 2011, p. 1).This implies, for example, that in a cross-organizational business process an organization has to fulfill not only their internal local compliance requirements, but also the possibly divergent compliance requirements of an involved business partner (Knuplesch, Reichert, Fdhila, & Rinderle-Ma, 2013, pp. 146–147). The different legislations in every country and the divergent objectives of stakeholders of business partners intensify the complexity of compliance processes (Meironke et al., 2019, p. 1898).

Sadiq and Governatori (2015, pp. 266–267) distinguish three interrelated but distinct perspectives of the different organizational tasks and processes, namely corrective, detective and preventative. In the latter case, organizations should embed and validate compliance into the business model at design-time. This way, it is possible to identify compliance conflicts in a preventative manner (Schäfer et al., 2012, pp. 347–348). However, it is difficult to achieve "compliance by design" (Sadiq, Governatori, & Namiri, 2007, p. 150). Among other reasons, every business process needs to be mapped to the relevant compliance requirement and vice versa. The detective perspective includes two main approaches (Sadiq & Governatori, 2015, pp. 266–267). The first approach, the traditional retrospective reporting, ensures compliance through external or internal audits after runtime (Sadiq & Governatori, 2015, pp. 266–267). The second and more recent approach demands compliance already during runtime through automated detection (Sadiq & Governatori, 2015, pp. 266–267). This implies automated audits (Sadiq & Governatori, 2015, pp. 266–267), up-to-date compliance monitoring (Mylrea & Gourisetti, 2018, p. 71) and (financial) - risk monitoring (Parra Moyano & Ross, 2017, p. 412). Both approaches, and especially the

automated detection, require precise documentation and verification of assets, events, processes, contractual agreements, customer identity data, (financial) transactions and others. The high effort and amount of resources needed to collect, archive and process these records are immense (Hofman, Lemieux, Joo, & Batista, 2019). Additionally, the authenticity and integrity of these records need to be ensured (Abreu, Aparicio, & Costa, 2018, p. 1).

Corrective measures intervene if either new or changing compliance requirements impact the organization or if a compliance violation has been detected (Sadiq & Governatori, 2015, pp. 266–267). To find the origin of violations, the mapping of compliance requirements to their relevant business processes must be transparent and traceable (Meironke et al., 2019, p. 1898). Additional challenges include providing sufficient reporting channels for compliance violations (Singi, S, Kaulgud, & Podder, 2018, p. 132).

Technical Challenges

Technical challenges refer to the challenges of providing the necessary IT infrastructure and service to fulfill the compliance requirements. Organizations currently conduct many of the compliance processes manually, which is time-consuming and error-prone (Meironke et al., 2019, p. 1898). While organizations grow, enable new business collaborations, integrate new business segments and outsource others, the IT infrastructure gets more and more complex. Parallel, redundant and sometimes incompatible IT systems inside organizations and across organizations arise (P. Zhang, Walker, White, Schmidt, & Lenz, 2017, pp. 1–2). This leads to inconsistent data (Meironke et al., 2019, p. 1899), which is highly problematic for compliance tasks that rely on consistent data, such as auditing.

Organizations are often dependent on external service providers, which conduct compliance tasks, provide required IT tools or simply a cloud infrastructure. The centralization character of these service providers makes them a single-point-of-failure and organizations are forced to trust them (Liang et al., 2017, p. 474). As part of information governance, a major technical challenge for organizations is to provide the security and privacy of data. Compliance tasks, such as auditing, require the authenticity and integrity of data at all times (Kaaniche & Laurent, 2017, p. 3). Personal data is subjected to privacy regulations, such as the GDPR, which requires among other things transparent storage and usage of personal data as well as anonymity for the data owner (Schmelz, Fischer, Niemeier, Zhu, & Grechenig, 2018, p. 223).

Economic Challenges

Organizations face high and increasing costs for the provision of compliance, due to inefficient compliance processes, a low degree of automation as well as increased complex compliance requirements and business processes (Kühnel, 2017, pp. 2379–2380). Furthermore, many organizations lack data and measurement methods to evaluate the cost efficiency of compliance processes (Kühnel, 2017, p. 2383).

In addition to bad reputation, the financial consequences for being non-compliant can be drastic (English & Hammond, 2018, pp. 14–31). For example, a violation of the GDPR can result in a fine up to 20 million Euro or in the case of a business up to 4% of its total worldwide annual turnover (Schmelz et al., 2018, p. 223).

Human-centered Challenges

Although organizations instruct their personnel about compliance tasks and their significance, there still seems to be a lack of awareness and acceptance for compliance (Meironke et al., 2019, p. 1898). The lack of knowledge of compliance can lead to unconscious misconduct (Meironke et al., 2019, p. 1898), though, the biggest challenge remains conscious misconduct such as hiding, altering or faking records (Abreu et al., 2018, p. 4). Another challenge is that a lack of trust and conflicting interests between stakeholders impede the necessary exchange of compliance relevant data or the participation in a joint compliance task (Singi et al., 2018, p. 131).

2.2. Distributed Ledger Technology

2.2.1. Definition DLT

A distributed ledger is a database composed of a chronologically ordered list of transactions, which is replicated among a certain number of storage devices, so-called nodes (Suciu et al., 2018, p. 370). Although its most popular applications are crypto-currencies, such as Bitcoin or Ethereum, the transactions are not limited to monetary transfers and can be any exchange of data (Suciu et al., 2018, p. 370).

A database network is distinguished by two main factors: The level of decentralization and the level of distribution of storage location. If only one entity has full control over the database, it is referred to as a centralized network. This requires complete trust in the controlling entity from all participants. The opposite is a decentralized network, where the control is divided equally among the participants. A non-distributed database stores the data in only one location, whereas a distributed database stores consistent replica of the data in multiple locations.

To reach consistency of the data in a distributed ledger, all participants, respectively the nodes, need to agree to the current state and updates of the ledger (Suciu et al., 2018, p. 370). The nodes communicate in a P2P network, where each node is connected to a variable set of neighbors, to broadcast the data in multiple rounds of message exchanges (K. Zhang & Jacobsen, 2018, p. 1338). The owner of a node, who operates and controls the node, can be an individual, an organization or an external entity, such as a regulating authority. Figure 1 illustrates a distributed ledger in a P2P network.

While there are networks, where the participants can trust each other, the DLT is also suitable for partially or fully untrustworthy environments. In an untrustworthy environment, nodes can arbitrarily crash, be temporarily unreachable, or send malicious conflicting information to the network (Kannengießer, Lins, Dehling, & Sunyaev, 2019b, p. 3). This is referred to as the Byzantine Generals Problem (Lamport,

Shostak, & Pease, 1982, p. 382). Therefore, nodes take part in a consensus mechanism to come to an agreement over the update of the ledger (K. Zhang & Jacobsen, 2018, p. 1338). Since one can only append data to the ledger, it requires a large effort to modify or delete data retroactively, once it has been agreed upon by the network (Kannengießer, Lins, Dehling, & Sunyaev, 2019a, p. 7070). Thus, DLT provides a high degree of integrity, which guaranties an immutable record of the data (Kannengießer et al., 2019a, p. 7070). For the remainder of this thesis, we will only use the term 'integrity', when referring to immutability and tamper-resistances.

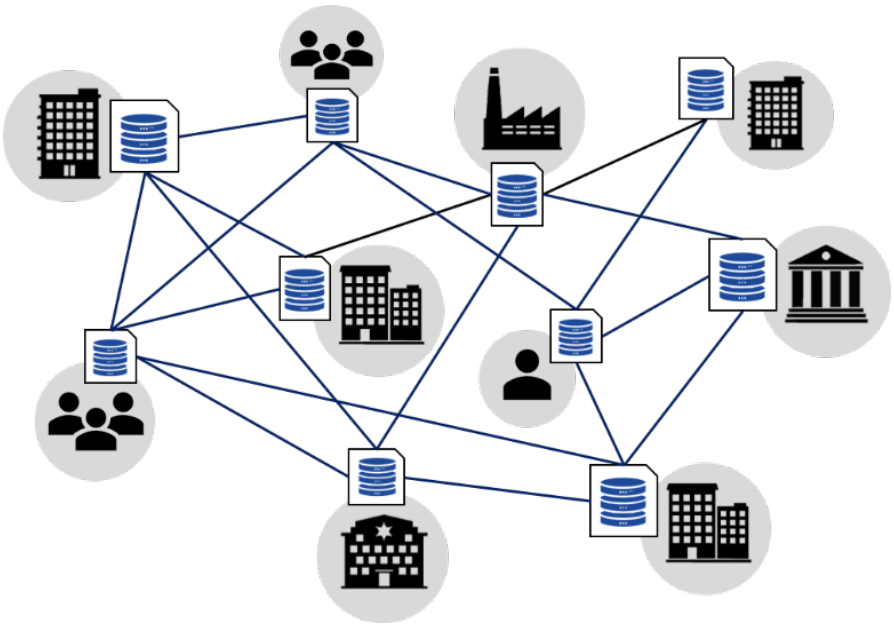

Figure 1: A Distributed Ledger in a P2P Network

In recent years, different concepts of the DLT with diverse designs have been developed to address different areas of applications in all fields of business (Casino, Dasaklis, & Patsakis, 2019). Three generations of DLT can be distinguished: DLT 1.0 for digital currency, DLT 2.0 for digital finance with the introduction of Smart Contracts (see chapter 2.2.2) by the Ethereum blockchain, and DLT 3.0 for digital society (Zhao, Fan, & Yan, 2016, p. 1). DLT 3.0 includes applications in areas beyond financial markets, such as government, health, science and Internet of Things (Casino et al., 2019, p. 56). Since DLT 3.0 applications interconnect entire industries and the public sector, it requires scalability and a dedicated DLT infrastructure (K. Zhang & Jacobsen, 2018, p. 1342). DLT in organizational compliance can be, depending on the scope of use case, distinguished as DLT 2.0 but predominantly as DLT 3.0. The Hyperledger project by the Linux foundation is a prominent example of DLT 3.0 (Androulaki et al., 2018).

2.2.2. Key Concepts

Hashing and Merkle Tree

Hash functions are mathematical algorithms that transform a given input of data of arbitrary length into an output of fixed length (Pilkington, 2016, p. 228). Cryptographic hash functions are one-way functions, thus it is extremely difficult to recreate the input data from the hash value of a given output (Pilkington, 2016, p. 228). Cryptographic hash functions are also deterministic, hence, an identical input transforms to the exact same hash value (Drescher, 2017, p. 72). Furthermore, they are pseudorandom, which means that the hash value changes unpredictably by any change of input (Drescher, 2017, pp. 72–73). Ultimately cryptographic hash functions are collision resistant so that the probability of receiving an identical hash value from different input data is extremely small (Drescher, 2017, pp. 72–73).

Based on Merkle (1990) a so-called Merkle tree is a binary hierarchical tree of hashes. Each leaf node holds the hash of a data input. Each of the internal non-leaf nodes transforms the hash values of their two child nodes to a new hash value. The final generated hash value is called the root. The Merkle tree allows for an efficient verification of the hashed data, since the hash value of the root changes, if the data of only one leaf node changes. Figure 2 illustrates the concept of a Merkle hash tree.

DLT Concepts and designs

DLT includes different DLT concepts, which are subclassified into different DLT designs. The DLT concept defines the basic data structure and functionality, in particular in the way the transactions are validated and stored (Kannengießer et al., 2019a, p. 7070). The most common DLT concept is Blockchain (Nakamoto, 2008), other DLT concepts are block directed acyclic graphs (blockDAG) and transaction-based directed acyclic graphs (TDAG).

A Blockchain, also called hashchain, consist of a sequence of blocks that are linked to form a chain (Kannengießer et al., 2019b, p. 4). A block in this context is the virtual storage object. The internal structure of a block various between different Blockchain designs (K. Zhang & Jacobsen, 2018, p. 1338). It commonly consists of a block header and a block body (Zheng, Xie, Dai, Chen, & Wang, 2017, p. 558). The block body contains the list of transactions and the block header contains the timestamp, a Merkle tree root hash of the transactions and the link to the previous block, which is the hash of the previous block header (Zheng et al., 2017, p. 558). Figure 2 illustrates this structure and concept of a Blockchain. In blockDAG blocks are linked to multiple parenting blocks in a direct acyclic graph, while in TDAG the transactions itself contain the link to previous transactions (Yeow, Gani, Ahmad, Rodrigues, & Ko, 2018, p. 1516). For a more detailed description of blockDAG and TDAG, we suggest the work of Yeow et al. (2018).

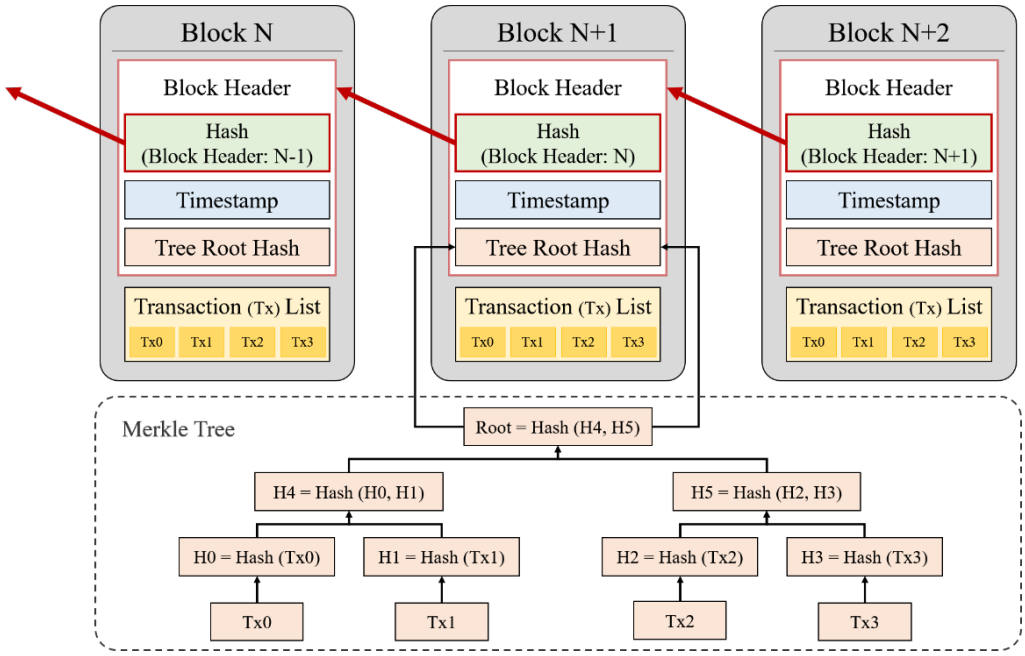

Figure 2: Model of the Blockchain concept and structure with Merkle Tree.

DLT concepts are further classified into DLT designs, that differ in their configuration of the DLT characteristics, which defines the suitability for an application (Kannengießer et al., 2019a, p. 7070). Characteristics are grouped in DLT properties. Ethereum and the Hyperledger framework Fabric are both examples for a Blockchain design, however they differ significantly in their configuration. IOTA is the most prominent example of a TDAG. Figure 3 visualizes the hierarchical structure of DLT.

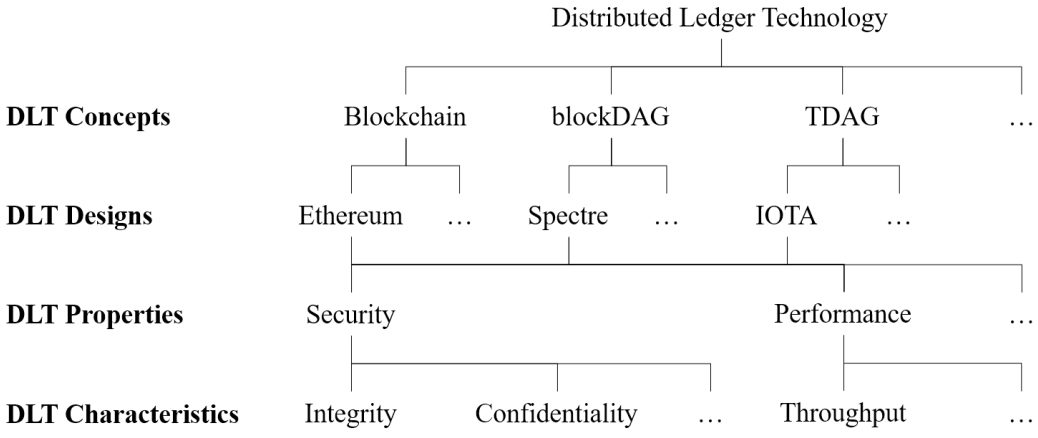

Figure 3: Hierarchical Structure of DLT (adapted from Kannengießer et al. 2019b, p. 4).

Configuration of DLT

There are two fundamental distinctions of a configuration of a DLT design: Private or public and permissioned or permissionless. The following definition is based on Axon, Goldsmith, and Creese (2018, p. 263). A public DLT has no access restrictions and anybody can join the network with a new node,

view the whole transaction record and submit new transactions. A private DLT has restricted access, and potential participants are individually granted permission for joining the network and submitting transactions. A permissionless DLT allows any participant to take part with their nodes in the validation and consensus process, while in a permissioned DLT a centralized entity controls which nodes are allowed to take part in the validation and consensus process.

Thus, the level of decentralization differs strongly between public and private as well as between permissionless and permissioned DLTs. Only public and permissionless DLTs are truly decentralized. Private, permissionless DLTs though are centralized due to the presence of the controlling entity (Zheng et al., 2017, p. 559). For instance, Hyperledger Fabric implements a membership service provider that manages the identities and the functional range of all nodes in the system (Androulaki et al., 2018, p. 8). A partially decentralized DLT constructed by different controlling entities, for example multiple organizations, is called a consortium DLT (Zheng et al., 2017, p. 559). Apart from the higher level of decentralization it has the characteristics of a private DLT.

Validation and Consensus

When a node wants to submit a transaction to the distributed ledger, it applies a digital signature with asymmetric cryptography to the transaction and broadcast it to the peer-to-peer network (Christidis & Devetsikiotis, 2016, p. 2293). The neighboring nodes validate the transaction and forward it further through the network until each node eventually received and validated the transaction (Christidis & Devetsikiotis, 2016, p. 2293). For example if a node wants to transfer an amount of cryptocurrency that exceeds its account balance, the transaction is discarded, since the account balance, (the ledger) is known to the entire network.

In the case of a Blockchain, multiple validated transactions are pooled and packaged into a timestamped candidate block (Christidis & Devetsikiotis, 2016, p. 2293). The consensus mechanism defines, which node generates the new block (Christidis & Devetsikiotis, 2016, p. 2294). In public Blockchains a node that takes part in this consensus process and which is often referred to as a miner, proposes the generated block back to the network (Christidis & Devetsikiotis, 2016, p. 2293). Every other node verifies the block by its hash reference to the parent block and by the transactions and finally update their distributed ledger to the new state (Christidis & Devetsikiotis, 2016, p. 2293).

Due to concurrency and network delays, multiple valid blocks may be generated simultaneously, so that multiple, possibly contradicting branches of the Blockchain occur (Saito & Yamada, 2016, p. 169). This phenomenon is called a fork, to resolve it, a fork resolution protocol dictates the new consistent state of the Blockchain (Kannengießer et al., 2019b, p. 4). For example, the Nakamoto Consensus protocol of Bitcoin selects the branch with the longest chain (Nakamoto, 2008). The most common consensus mechanism is Proof-of-Work (PoW), which requires a computational puzzle to be solved (K. Zhang & Jacobsen, 2018, p. 1339). This requires immense computational resources, which provides the desired

integrity of the blockchain (K. Zhang & Jacobsen, 2018, p. 1339). On the other hand, the high computational costs of the PoW mechanism are highly critical from an economical and environmental perspective (K. Zhang & Jacobsen, 2018, p. 1339). An alternative to PoW that requires less computational resources is Proof-of-Stake (PoS), where each participant's voting power is proportional to their amount of cryptocurrency in that system (Pass & Shi, 2017, p. 389).

In a private or consortium DLT, such as Hyperledger Fabric, an ordering service determines the next block, which prevents the possibility of a fork (K. Zhang & Jacobsen, 2018, p. 1339). The ordering service is either executed by a static central node or by periodically changing distributed nodes (K. Zhang & Jacobsen, 2018, p. 1339). Before the block is appended to the chain, all participating nodes need to verify the block and agree on the new state (Kannengießer et al., 2019b, p. 4). In the case of Hyperledger Fabric, the nodes execute a Practical Byzantine Fault Tolerance protocol (PBFT) to reach an agreement (K. Zhang & Jacobsen, 2018, p. 1339). To obtain further detailed technical information of the different consensus mechanism, we refer to the provided references.

Smart Contract

Smart Contracts are programmable scripts that allow for the execution of customized business logic on a distributed ledger (Glaser, 2017, p. 1546). DLTs of the first-generation support only a finite set of basic OP_CODEs, such as Bitcoin Script language, to specify the conditions of unlocking and accessing stored assets (Kannengießer et al., 2019b, p. 6). DLTs of the second and third generation support arbitrary, Turing-complete code in high level programming languages (Suciu et al., 2018, p. 370), such as Java, Python in Hyperledger and Solidity in Ethereum (Kannengießer et al., 2019b, p. 6).

Smart Contracts in Ethereum reside on the distributed ledger and are triggered by a transaction to their unique address or if defined conditions are met (Christidis & Devetsikiotis, 2016, p. 2296). For the execution of Turing complete Smart Contracts the Ethereum foundation provides the Ethereum Virtual Machine (EVM) that runs on every node in the network (Christidis & Devetsikiotis, 2016, p. 2296). The Hyperledger foundation provides different DLT frameworks that support Smart Contracts in a slightly different way. Each framework validates and executes the Smart Contract on a dedicated Smart Contract layer, before it is passed to the consensus layer (The Linux Foundation, 2018, p. 4). The different frameworks support various Smart Contract technologies and programming languages (The Linux Foundation, 2018, p. 8). The Smart Contract technology of Hyperledger Fabric is called Chaincode, but for the simplicity we will use for the rest of this work the term Smart Contract independently of the underlaying technological term. Smart Contracts are not only able to send and store any kind of data information on the distributed ledger, they are also able to retrieve data from external data sources, so-called oracles (Kannengießer et al., 2019b, p. 6). In case of Ethereum, once a Smart Contract is executed every node needs to execute the Smart Contract and update to the new state of the distributed ledger (Kannengießer et al., 2019b, p. 6). Hyperledger Fabric maintains confidentiality by only propagating the new state to all nodes, after selected trusted nodes have executed the Smart Contract (Androulaki et al., 2018, p. 4).

2.2.3. DLT Characteristics

The DLT design determines the DLT characteristics, such as scalability or level of decentralization. We adopted a comprehensive list of DLT characteristics and its descriptions from Kannengießer et al. (2019b, pp. 13–14). In their research, they aggregated similar DLT characteristics to DLT properties as master variables, which we also adopted Kannengießer et al. (2019b, p. 12). The properties are listed and described in Table 1 and the characteristics in Table 2, Table 3 and Table 4.

Table 1: DLT Properties (adapted from Kannengießer et al. 2019b, p. 12).

DLT Property	Description
Community	A group of individuals who have a common interest in using and/or maintaining a DLT design.
Flexibility	The degree of technical freedom to customize a DLT design and to deploy applications on a DLT design.
Law & Regulation	The ability of authorities to enforce compliance of a DLT design with legal and regulatory requirements.
Transparency	The perception of an individual of being informed about the relevant actions and characteristics of another party who uses the DLT design.
Performance	The accomplishment of a given task on a distrusted ledger measured against targets for accuracy, completeness, cost, and speed.
Security	The preservation of confidentiality, integrity, and availability of data stored on a distributed ledger.
Usability	The extent to which DLT design users can achieve their goals with respect to effectiveness, efficiency, and satisfaction in their use contexts.

Table 2: DLT Characteristics part 1 (adapted from Kannengießer et al. 2019b, p. 13).

DLT Property	DLT Characteristic	Description
Community	Development Activity	The engagement and size of the community involved with the continued development of the DLT design.
	Developer Support	Assistance (e.g., documentation, forums) offered by the community or foundation to answer questions with respect to deployment and operation of applications on the DLT design.
	Incentive Mechanisms	The structures in place to motivate contribution of resources (e.g., computing power) for DLT design operation.
	Network Size	The number of nodes participating in a DLT design.
Flexibility	Interoperability	The ability to communicate between DLT designs and with other external services from a DLT design.
	Maintainability	The degree of effectiveness and efficiency with which a DLT design can be kept operational.
	Modularity	The logical partitioning of a DLT design into smaller components to facilitate implementation, updates, and change management, among others.
	Smart Contract Support	The degree to which the DLT design supports the integration, development, and testing of smart contracts.
	Token Purposes	The possible uses of tokens within a DLT design (e.g., security token, utility token, stable coin).
	Transaction Size Limit	The existence and measure of a fixed maximum storage size of a transaction.
	Compliance	The alignment of DLT design characteristics and operation with regulatory requirements.
	Governance Mechanisms	The existence of control mechanisms (e.g., decision rights and accountabilities) to ensure desirable behavior of DLT design users (e.g., customers, miners).

Table 3: DLT Characteristics part 2 (adapted from Kannengießer et al. 2019b, p. 13-14).

DLT Property	DLT Characteristic	Description
Law & Regulation	Auditability	The degree to which an independent third party (e.g., state institution, certification authority) can assess the technical functionality and stored data of a DLT design.
	Censorship Resistance	The probability that a transaction in a DLT design will be intentionally aborted or processed with malicious modifications.
	Compliance	The alignment of DLT design characteristics and operation with regulatory requirements.
	Governance Mechanisms	The existence of control mechanisms (e.g., decision rights and accountabilities) to ensure desirable behavior of DLT design users (e.g., customers, miners).
	Liability	The existence of a real or juridical person that can be subjected to litigation with respect to the DLT design.
Performance	Block Creation Interval	The time between the creation of consecutive blocks (only in DLT designs using blocks).
	Block Size	The size of data that can be stored in a block (only in DLT designs using blocks).
	Confirmation Latency	The time until sufficient subsequent transactions have been added to a distributed ledger so that the likelihood of future transaction manipulation becomes negligible.
	History Retention	The maximum number of transactions that can be maintained by a DLT design.
	Resource Efficiency	The computational efforts required to operate a DLT design (e.g., transaction validation or block creation).
	Message Propagation Efficiency	The time, bandwidth, and number of connections required to propagate transactions (or blocks) through the network.
	Propagation Delay	The time between the submission of a transaction (or block) and its recipience by all nodes.
	Response Time	The time between sending a transaction and receiving feedback from a DLT design.
	Scalability	The capability of a DLT design to efficiently handle decreasing or increasing amounts of required resources (e.g., of transactions per second).
	Throughput	The maximum number of transactions that can be appended to a DLT design in a given time interval.
	Transaction Validation Latency	The time required for verifying the validity of a transaction.
Transparency	Traceability	The extent to which transactions can be traced chronologically in a DLT design.
	Transaction Content Visibility	The ability to publicly view a user account's holdings and transactions in a DLT design.
	Unidentifiability	The degree of difficulty of mapping an account to real identities in a DLT design.
	Node Verification	The extent to which nodes are verified prior to joining a distributed ledger.
Usability	Cost	Financial resources required for the implementation and operation of a DLT design.
	Ease of Node Setup	The ease of configuring and adding a new or crashed node to the DLT design.
	Ease of Use	The simplicity of accessing and working with a DLT design.
	Support for Constrained Devices	The extent to which devices with limited computing capabilities (e.g., small sensors), can participate in a DLT design.

Table 4: DLT Characteristics part 3 (adapted from Kannengießer et al. 2019b, p. 14).

DLT Property	DLT Characteristic	Description
Security	Atomicity	The assurance that transactions are either completely executed or not executed.
	Authentication	The degree to which the correctness of particular data, which is stored on a distributed ledger, can be verified.
	Availability	The probability that a distributed ledger is operating correctly at any point in time.
	Confidentiality	The degree to which unauthorized access to data is prevented.
	Consistency	The homogeneity of data stored by all nodes participating in a DLT design.
	Durability	The property of a database that data, which was once committed to the ledger, will not be lost.
	Fault Tolerance	The degree to which a DLT design continues to operate correctly even if transactions (or blocks) are dropped (or delayed) or if nodes fail.
	Integrity	The degree to which transactions stored on the distributed ledger are protected against unauthorized (or unintended) modification or deletion.
	Isolation	The property of a database that transactions do not impact each other during their execution.
	Level of Decentralization	The number of independent node controllers participating in transaction validation and consensus finding.
	Node Trust Level	The trustworthiness of nodes participating in a DLT design.
	Non-Repudiation	The difficulty of denying participation in transactions.
	Reliability	The period of time during which a distributed ledger is correctly functioning.
	Stale Block Rate	The number of blocks in a period of time that have been mined but not appended to the distributed ledger (only in DLT designs using blocks).
	Strength of Encryption	The difficulty of breaking cryptographic algorithms employed by the DLT design.

3. Research Method

We conducted a systematic literature review following the Hermeneutic Approach of Boell and Cecez-Kecmanovic (2014). A literature review is not a linear, but rather iterative process of gathering relevant information while developing a broad understanding of it (Boell & Cecez-Kecmanovic, 2014, 260-263). We therefore applied the two hermeneutic circles: the search and acquisition circle and the analysis and interpretation circle, which are closely intertwined (see Figure 4).

3.1. Literature Search

Our search and acquisition process followed the approach by Boell and Cecez-Kecmanovic (2014) and was guided by Lins and Sunyaev (2017). At first, we formulated a general, abstract form of the research problem and question, which is part of the analysis and interpretation circle. We then started a first searching cycle in scientific databases with only the major search terms: (“Distributed Ledger Technology” OR Blockchain) AND (Compliance). To obtain a wide coverage of journal and conference articles and to ensure the high quality of it, we limited our search to peer-reviewed, English articles in representative scientific databases: Association for Computing Machinery Digital Library (ACM DL), Association of Information Systems electronic Library (AISeL), EBSCO HOST, Institute of Electrical and Electronics Engineers Digital Library (IEEE Xplore DL), ProQuest and ScienceDirect.

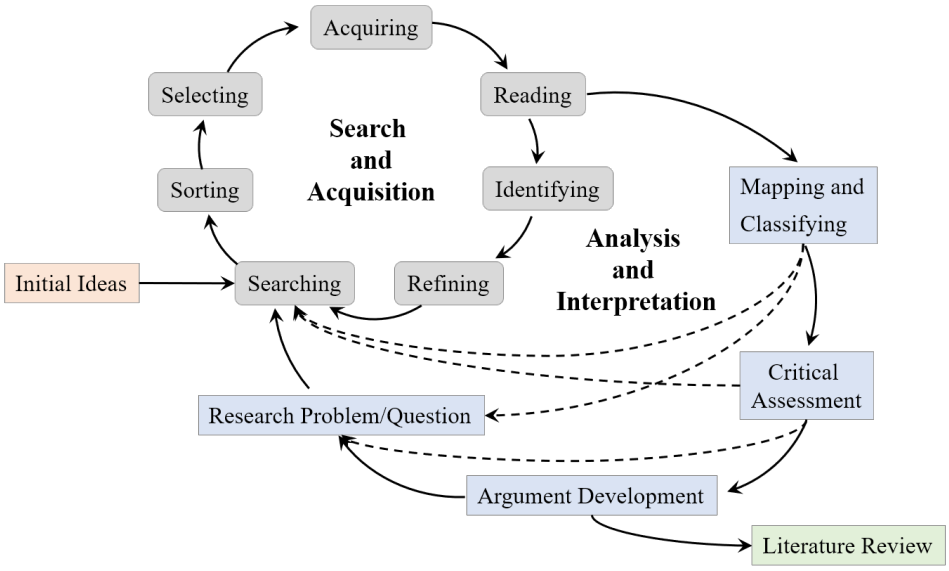

Figure 4: A hermeneutic framework for the literature review process consisting of two major hermeneutic circles (adapted from Boell & Cecez-Kecmanovic, 2014, p. 264).

Through several iterations of searching, reading and identifying further search terms, we refined our search strategy and developed a more precise form of the research problem and question. For the identification of potentially relevant literature for further analysis, we used one final search string, that combined the gathered search terms with logical operators. This way, we received one consistent search documentation. We scanned the title, keywords and abstract of articles with the search string: ("Distributed Ledger Technology" OR DLT OR Blockchain OR "smart contracts" OR Ethereum OR Hyperledger) AND (compliance OR "general data protection regulation" OR GDPR OR KYC OR financial risk OR auditing OR "business process compliance" OR BPC OR regulation OR law). Following the search circle, we sorted out books and grey literature, including dissertations, case reports and magazines. We then read all titles and keywords to sort out duplicates and articles that were completely off topic but occurred for example due to matches with abbreviations of the search terms. In the next step, we read the abstract of the remaining articles, to select those articles that are potentially relevant. The selected articles were acquired and fully read. In the final step, we skimmed the full text of the articles and categorized them into two groups: The relevant articles, that we passed to the analysis circle and the partially relevant articles, that only cover the subject of compliance or DLT as a side topic and that we did not analyze further. The relevant articles are listed with a reference number in the Appendix A.

3.2. Literature Analysis

In the mapping and classifying process of the analysis circle we conducted three concept matrices through an iterative process. It consisted of thorough analytical reading of the relevant articles and defining the structure of the matrices, variables and the appropriate coding scheme.

C1: DLT Concepts and Designs

The first concept matrix, C-1, provides a descriptive overview of the DLT concepts and designs for the use in compliance, that are presented in the literature. The rows of the matrix represent the relevant articles with reference numbers (see Appendix A). The columns represent DLT designs, that we grouped equivalent to their superordinate DLT concept and sorted by their frequency of occurrence in the literature. Table 5 illustrates this schematically. We added a DLT design to the list, if it was studied and recommended by the author regarding the subject of compliance. We then coded every intersection of articles and DLT designs, that met the criteria, with an 'x'. If the author either did not mention the DLT design or studied it in the context of a different subject, we left the intersection blank.

Table 5: Schematic of Concept Matrix C-1: DLT Concepts and DLT Designs.

DLT Concept	e.g. Blockchain			…
DLT Design	e.g. Ethereum	e.g. Hyperledger	…	…
Reference Number				
1	x	…	…	…
2	x	x	…	…
…	…	…	…	…
Frequency of Occurrence	2	1	…	…

C2: DLT Characteristics vs. Challenges and Risks

The second concept matrix, C-2, provides an overview of the relationship between DLT characteristics on the one side and challenges and risks of using DLT on the other side. The rows of the matrix represent the dependent variables: DLT characteristics. The columns represent the independent variables: challenges of compliance as well as risks that can emerge through the use of DLT. We adopted the comprehensive list of DLT characteristics (see chapter 2.2.3) from Kannengießer et al. (2019b, pp. 13–14). In their research, they aggregated similar DLT characteristics to DLT properties as master variables, which we also adopted and used to structure our matrix accordingly Kannengießer et al. (2019b, p. 12).

For the identification and aggregation of the independent variables, we followed the method of Lacity, Khan, Yan, and Willcocks (2010, p. 398). In an iterative process, we first identified the variables and checked them for semantic ambiguities as suggested by Shaw and Gaines (1989) (Lins & Sunyaev, 2017, p. 6). Therefore, we determined one variable name and description, if different terminology was used to describe essentially the same concept (Shaw & Gaines, 1989, p. 343). In the second step, we defined the independent master variables and mapped the variables to them accordingly (Lacity et al., 2010, p. 398). The independent master variables aggregate similar challenges and risks. We adopted and generalized many of the challenges and risks from Meironke et al. (2019) and merged them with our own list of variables.

When we identified a relationship between the dependent and independent variables, we coded the intersection with the according reference number from the list of relevant articles (see Appendix A). In addition, we assigned one of three possible codes to the relationship, using the coding scheme of Jeyaraj, Rottman, and Lacity (2006, pp. 4–7): If the author strongly argued, that a higher value of the DLT characteristic has a positive effect addressing the challenge or reducing the risk, we coded it as '+'. If the author strongly argued that a higher value of the DLT characteristic has a negative effect addressing the challenge or fortify the risk, we coded it as '-' and marked it red. An exception to this rule are the variables: Block Creation Interval, Confirmation Latency, Propagation Delay, Response Time, Transaction Validation Latency, Node Trust Level and Cost. For these variables a lower value is coded '+' for a positive effect addressing the challenge or reducing the risk, respectively '-' for a negative effect or the fortification of the risk. If the relationship was studied by the author but not evaluated, we coded it as '0'. Table 6 illustrates this schematically.

Table 6: Schematic of Concept Matrix C-2: DLT Characteristics vs. Challenges and Risks.

		Challenges in Compliance			**Risks Through Use of DLT**		
Master Variable: Challenge/Risk		e.g. Precise Documentation and Verification		…	…	e.g. Non – Conformity of DLT with laws and regulations	
Variable: Challenge/ Risk		e.g. Authenticity and integrity of evidence and records	…	…	…	e.g. Non – Compliance with GDPR	…
DLT Property	**DLT Characteristic**						
e.g. Flexibility	e.g. Smart Contract Support	e.g. [3, 12, 16, 24] +	…	…	…	[Reference Numbers] -	…
	…	…	…	…	…	…	…
…	**…**	…	…	…	…	…	…

C3: Business use cases

In the third concept matrix, C-3, we identified all business use cases of DLT in compliance, that are presented in the literature. The rows of the matrix represent the business use cases and the columns the relevant articles with reference numbers (see Appendix A). If we identified a new business use case, we added it to the list and coded the intersection with an 'x'. If a business use case was studied by the author and fitted to an existing one from the list, we coded the intersection with an 'x'. Table 7 illustrates this schematically.

Table 7: Schematic of Concept Matrix C-3: Business Use Cases

Business Use Case	e.g. Financial Risk Management	e.g. Auditing of Software Development	…	…
Reference Number				
1	x	…	…	…
2	…	x	…	…
…	…	…	…	…

4. Results of Literature Review

4.1. Descriptive Results of Literature Search

In this chapter we will describe the results of our literature review on a quantitative basis. Our final literature search string yielded a total sum of 965 peer reviewed articles. We excluded 45 non-English articles and another 150 articles belonging to books and grey literature. After we read the title and keywords of the articles, we excluded 7 duplicates and marked 161 articles to be further examined. We then read the abstracts and identified 41 potentially relevant articles that we acquired and read. Finally, we determined 27 articles as relevant and coded our three concept matrices based on them. The whole selection process of our literature search is illustrated in Figure 5.

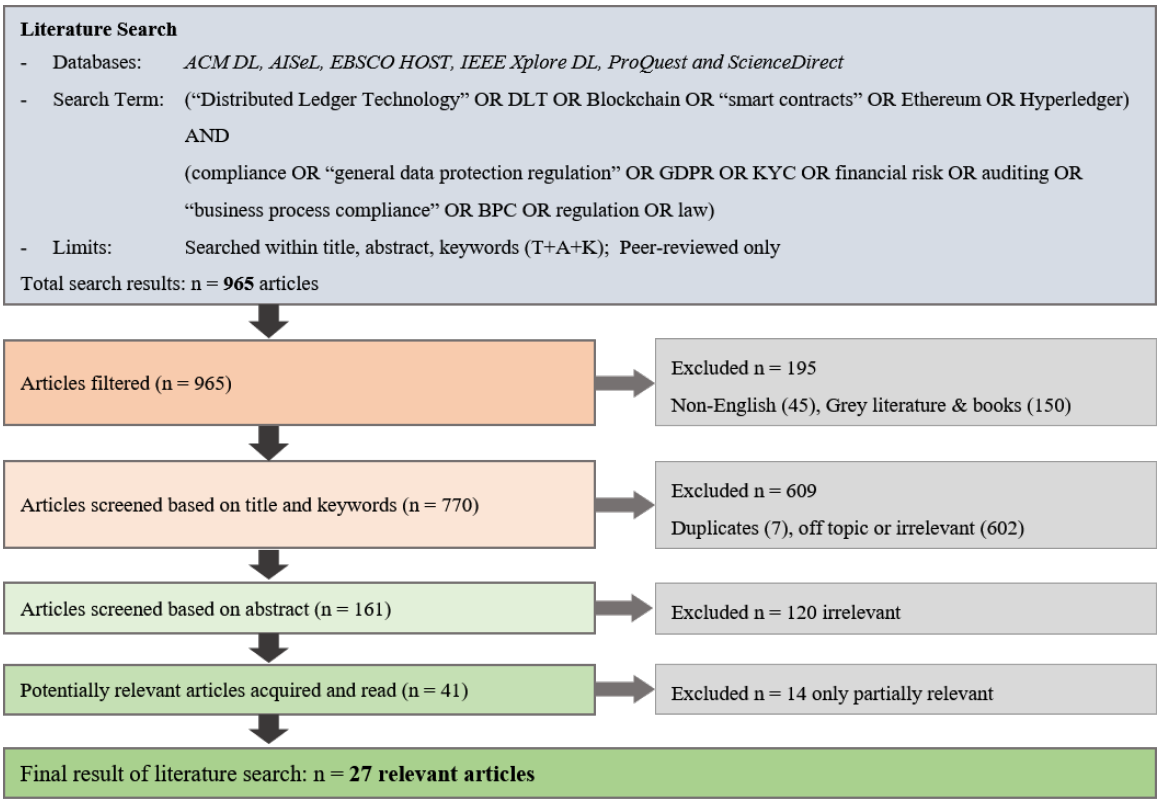

Figure 5: Literature Search and Selection Process Model (adapted from Lins & Sunyaev, 2017, p. 6).

4.2. DLT Concepts and Designs

In our first concept matrix, C-1, we identified and listed 13 different DLT designs that are all classified as a Blockchain. Other DLT concepts, like TDAG, were not studied in the literature. Some of the authors are not explicitly recommending a certain Blockchain design, but rather referring to the main configuration: permissioned or permission less and private, public or consortium blockchain. We listed 11 articles, where the authors recommended a permissioned blockchain configuration and zero articles with explicit recommendation for a permissionless one. We counted seven recommendations for a private blockchain, two for a public one and four recommendations for a consortium blockchain.

Table 8 is a breakdown of C-1 showing the DLT designs with the highest frequency of occurrence. The complete concept matrix is presented in the Appendix B.

Table 8: Breakdown of Concept Matrix C-1: DLT Concepts and DLT Designs.

DLT Concept	Blockchain													
DLT Design	Ethereum	Hyperledger	Hyperledger Fabric	Blockchain (general technology)	Quorum	ProvChain	Multichain 2.0	R3 Corda	[…]	permissioned	permissionless	private	public	consortium
Reference Number														
1														
2		x	x											
3	x				x					x				
4							x					x		
5	x													
6		x	x									x		x
7										x				x
8			x											
9														
10										x		x	x	
11		x								x				x
12	x	x								x				
13						x								
14														
15		x			x					x				
16	x										x		x	
17				x						x				
18	x									x		x		
19	x													
20	x	x						x		x		x		
21		x				x				x				
22														
23	x	x					x					x		x
24				x										
25			x							x		x		
26														
27	x													
Frequency	9	8	4	2	2	2	2	1		11	1	7	2	4

In eight articles the authors recommended in general Hyperledger and in additional four articles they explicitly recommended the Hyperledger framework Fabric. The second most recommended Blockchain design is Ethereum with nine articles referring to it. The authors recommended the Quorum, Multichain and ProvChain Blockchain as well as Blockchain as the general technology each twice in the literature. Quorum is a fork of the Ethereum protocol. Instead of Ethereum's public and permissionless Blockchain design, Quorum is configurable as a private and permissioned Blockchain for enterprise applications (Magrahi, Omrane, Senot, & Jaziri, 2018, p. 2). Equivalent to the Ethereum Blockchain, Quorum supports the Smart Contract language, Solidity. Quorum is a project of JPMorgan Chase.
Multichain 2.0 is an open-source-fork of Bitcoin core protocol but is primarily used in a private or consortium configuration for enterprise applications (Al-Zaben, Hassan Onik, Yang, Lee, & Kim, 2018, p. 81). ProvChain is a concept of a blockchain-based data provenance architecture, to provide provenance tracking and auditing for cloud data storage (Liang et al., 2017, p. 470). The underlying blockchain configuration is not further described in the literature. The other Blockchain designs, namely R3 Corda, Sia, Filecoin, Factom, Verady, Libra, PikcioChain, Truyo and Volta, were each recommended only once and thus we will not discuss them any further. We will narrow our focus on Hyperledger and Ethereum respectively Quorum.

4.3. DLT for Challenges in Compliance

For the first part of our concept matrix C-2, we identified a total of 59 challenges in compliance, which we then aggregated to 19 master challenges (see Table 9). We coded the relationship between every characteristic of DLT and every challenge in compliance. We listed only those challenges in compliance, where at least one author studied a relationship between a DLT characteristic and the challenge. To gain a better overview, we sorted the master challenges according to Meironke et al. (2019) into the five categories: Legal, organizational, technical, economic and human-centered challenges. The complete and detailed results of C-2 are shown in the Appendix C. For a breakdown of C-2 we split the matrix and present in Table 10, Table 11, Table 12 and Table 13 the matrix with only aggregated challenges. Furthermore, we left out the DLT characteristics where no relationship with a challenge or risk occurred.

The authors of the relevant articles that we analyzed focused mostly on the organizational and technical challenges in compliance. Meironke et al. (2019), however, studied in their work a wide range of challenges including also legal, economical and human-centered challenges. We identified only a few arguments of other authors, regarding economic and human-centered challenges and no arguments for legal challenges.

Table 9: Master Variables: Challenges in Compliance

	Challenges in Compliance	Description
Legal	Complexity of compliance requirements	The number and complexity of compliance requirements is high and increasing. Compliance requirements can come in conflict with each other.
	Transformational pace and change of compliance requirements	Continuous and sometimes rapid change of compliance requirements.
	Difficult interpretation of compliance requirements	Due to the complexity and lack of implementation guidelines of compliance requirements, divergent interpretation of terms and concepts can occur.
Organizational	Complexity of business and compliance processes	The complexity of compliance processes is dependent on the size of an organization, the multitude and dynamics of business processes and the degree of global activity.
	Modeling and design-time verification of compliance requirements	Complex risk and vulnerability analysis in business processes. Difficulties in modeling and mapping compliance requirements to business processes. Incomplete documentation of business processes. Various process modeling languages.
	Compliance monitoring and auditability	High manual, time-consuming effort to forward compliance checking. Difficulties to provide compliance monitoring and auditability.
	Financial risk monitoring	Providing a high degree of transparency for risk monitoring and preserving anonymity between financial institutes.
	Precise documentation and verification	Precise, authentic and tamper-proof documentation and verification of assets, events, processes, contractual agreements, customer identity data or (financial) – transactions.
	Transparency and traceability of compliance	Insufficient reporting channels. Protection of anonymity for whistleblowers. Insufficient traceability of compliance requirements and sources.
Technical	Technical support and automation of Compliance	Identification of compliance violations and fraud. Low level and potential of automation of compliance processes.
	Complex and inefficient IT and compliance infrastructure and low system integration	Distributed, heterogeneous and isolated applications and systems. Parallel systems and redundant data. Inconsistent data and decisions of management. Incompatible IT systems.
	Dependency on service providers and centralization of services	Monopoly of service providers. Service provider as single-point-of-failure. Lack of trust regarding the service provider
	Technical aspects of data security and privacy	Confidentiality, availability, authenticity and integrity of data. Transparency of data storing and usage. Data privacy and anonymity.
Economical	Inadequate cost efficiency of provision of compliance	Costs for provision of compliance. Lack of cost efficiency of compliance processes. Consequential charges and legal costs.
	Insufficient efficiency of resources	Low alignment to efficiency. Inefficient allocation of resources.
	Difficulties concerning measurability of compliance	Extensive data processing and evaluation. Lack of key figures and measurement methods to evaluate cost efficiency.
Human-Centered	Lack of awareness and acceptance	Compliance seen as a bureaucratic burden. Ignorance and lack of communication.
	Conscious or unconscious misconduct	Deficits in knowledge and errors. Insufficient compliance focus. Preventing deliberate infringement
	Conflicts of interest and trust issues between stakeholders	Diverse interests and goals. Different roles and relevance. trust issues in distributed working environments. Different opportunities of influence.

We identified arguments in almost every article for positive effects of the DLT properties flexibility, law and regulations, transparency and security on the organizational challenges. We counted 18 articles, where the authors emphasized the positive effect of DLT characteristics to address the challenge of deficiencies in compliance monitoring and auditability. The results for the challenge of precise documentation and verification disclose resemblances. We identified only sporadic arguments for positive effects of DLT characteristics addressing the challenges of complexity of business and compliance processes, modeling and design-time verification of compliance requirements and lack of transparency and traceability of compliance.

In 22 of the articles the authors argue that the flexibility, transparency and security of DLT have a positive effect addressing the technical challenges of compliance. The results suggest that almost every DLT characteristic of the properties law and regulation, transparency and security have a positive effect on technical aspects of data security and privacy. However, there are some conflictive results regarding the effect of the DLT's characteristic integrity and technical aspects of data security and privacy. We will explain and discuss this conflictive result as well as all the above-mentioned relevant relationships in the following discussion chapter.

Table 10: Breakdown of Concept Matrix C-2: Challenges in Compliance

DLT Properties	DLT Characteristics	Master Variable: Challenge in Compliance								
		Complexity of compliance requirements	Transformational pace and change of compliance requirements	Difficult interpretation of compliance requirements	Complexity of business and compliance processes	Modeling and design-time verification of compliance requirements	Compliance monitoring and auditability	Financial risk monitoring	Precise documentation and verification	Transparency and traceability of compliance
Community	Development Activity									
	Developer Support			[16] +						
	Incentive Mechanisms								[13] +	
	Network Size			[16] +						
Flexibility	Interoperability			[16] +		[16] +	[3, 25]+		[3, 6, 8, 12, 20] +	
	Maintainability						[27] +		[20] +	
	Modularity						[2] +		[6] +	
	Smart Contract Support	[16] +	[16] +		[16, 24] +	[16] +	[2, 3, 8, 16, 17, 25, 27] +		[3, 6, 12, 14, 16, 17, 18, 23, 24] +	[16] +
	Token Purposes						[1] +		[20] +	
Law & Regulation	Auditability						[3, 8, 16, 25] +		[1, 3, 12] +	[16] +
	Compliance						[1] +		[20] +	
	Governance Mechanisms				[16] +		[13, 20, 25] +		[3, 20] +	
	Liability								[20] +	
Performance	Block Size								[12] -	
	Computational Resources								[12] 0	
	Message Propagation Efficiency									
	Response Time								[12] +	
	Scalability								[12] 0	
	Throughput									
	Transaction Validation Latency						[2] +			

Table 11: Breakdown of Concept Matrix C-2: Challenges in Compliance

DLT Properties	DLT Characteristics	Master Variable: Challenge in Compliance								
		Complexity of compliance requirements	Transformational pace and change of compliance requirements	Difficult interpretation of compliance requirements	Complexity of business and compliance processes	Modeling and design-time verification of compliance requirements	Compliance monitoring and auditability	Financial risk monitoring	Precise documentation and verification	Transparency and traceability of compliance
Transparency	Traceability				[16] +	[16] +	[8, 9, 13, 16, 20, 24, 27] +	[20] +	[1, 2, 3, 6, 12, 14, 15, 16, 20] +	[16, 20, 24] +
	Transaction Content Visibility				[16] +	[16, 17] +	[8, 13, 16, 24] +		[1, 2, 3, 12, 16, 17] +	[16, 24] +
	Unidentifiability						[13] +	[20] +	[20] +	[16] +
	Node Verification					[17] +	[2] +		[17] +	
Security	Atomicity				[25] +		[1] +		[1] +	
	Authentication						[1, 8, 9, 25] +		[1, 3, 13, 16, 24] +	
	Availability				[25] +		[2, 9, 16] +		[3, 12, 16] +	
	Confidentiality					[17] +	[1, 3, 13, 14, 17] +		[3, 17] +	
	Consistency				[25] +		[1, 2, 8] +		[1, 2, 3, 12] +	
	Durability						[1, 8] +		[3, 12, 13] +	
	Fault Tolerance					[17] +			[3, 13, 17] +	
	Integrity					[17] +	[1, 2, 8, 9, 11, 16, 18, 20, 27] +		[1, 2, 3, 8, 9, 12, 13, 16, 17, 20, 21, 24] +	
	Level of Decentralization				[16] +	[17] +	[2, 25, 27] +		[2, 13, 17, 23] +	[16] +
	Node Trust Level						[2] +			
	Non-Repudiation								[21] +	
	Reliability								[12, 13] +	
	Strength of Encryption			[16] +	[16] +					
Usability	Cost								[12] +	
	Ease of Node Setup									
	Ease of Use				[16] +		[2, 3, 5] +		[5] +	
	Support for Constrained Devices									

Table 12: Breakdown of Concept Matrix C-2: Challenges in Compliance

DLT Properties	DLT Characteristics	Master Variable: Challenge in Compliance									
		Technical support and automation of Compliance	Complex and inefficient IT and compliance infrastructure and low system integration	Centralization of service provider	Technical aspects of data security and privacy	Inadequate cost efficiency of provision of compliance	Insufficient efficiency of resources	Difficulties concerning measurability of compliance	Lack of awareness and acceptance	Conscious or unconscious misconduct	Conflicts of interest and trust issues between stakeholders
Community	Development Activity										
	Developer Support								[16] +		
	Incentive Mechanisms				[16, 27] +	[16] -	[16] +	[16] +			
	Network Size										
Flexibility	Interoperability		[16] +		[11, 18, 19] +						
	Maintainability				[27] +						
	Modularity		[16] +								
	Smart Contract Support	[8, 16, 17, 20, 24] +	[16, 18] +		[4, 6, 10, 11, 14, 17, 21, 27] +	[14, 16, 18, 20] +	[16] +	[16] +	[16] +	[16, 24] +	[24] +
	Token Purposes										
Law & Regulation	Auditability	[8] +			[11, 15, 21, 26] +						
	Compliance				[11, 26] +		[16] +			[16] +	
	Governance Mechanisms			[16, 20] -	[11, 17, 21] +				[16] +		
	Liability				[11] +						
Performance	Block Size										
	Computational Resources				[16, 19, 21] -						
	Message Propagation Efficiency				[21] -						
	Response Time				[27] +						
	Scalability				[19, 27] +						
	Throughput										
	Transaction Validation Latency										

Table 13: Breakdown of Concept Matrix C-2: Challenges in Compliance

DLT Properties	DLT Characteristics	Master Variable: Challenge in Compliance									
		Technical support and automation of Compliance	Complex and inefficient IT and compliance infrastructure and low system integration	Centralization of service provider	Technical aspects of data security and privacy	Inadequate cost efficiency of provision of compliance	Insufficient efficiency of resources	Difficulties concerning measurability of compliance	Lack of awareness and acceptance	Conscious or unconscious misconduct	Conflicts of interest and trust issues between stakeholders
Transparency	Traceability	[8, 13, 16] +	[19, 20] +	[16] +	[4, 10, 11, 14, 16, 17, 18, 27] +	[16] +		[16] +		[16] +	[24] +
	Transaction Content Visibility	[8, 16] +	[16, 19] +	[13, 16] +	[11, 17] + [22] -			[16] +		[16] +	[13, 24] +
	Unidentifiability				[11, 13, 16] +						[20] +
	Node Verification				[22] +						
Security	Atomicity										
	Authentication	[8] +			[9, 16, 21, 26] +						
	Availability			[16] +	[11, 16, 17, 21, 22] +	[16] +	[16] +			[1, 16] +	
	Confidentiality			[16] +	[6, 11, 13, 14, 15, 18, 19, 21, 26] +						
	Consistency	[8] +	[16] +			[16] +	[16] +				
	Durability	[8] +			[19, 22] -						
	Fault Tolerance				[11, 27] +						
	Integrity	[1, 8] +	[19] +	[13, 16] +	[9, 11, 13, 14, 16, 17, 21, 27] + [4, 7, 9, 16, 18, 19, 22] -					[1, 16] +	[24] +
	Level of Decentralization		[19] +	[13, 16] +	[4, 13, 20, 23, 27] + [22] -		[13, 20] +		[16] +		[16, 24] +
	Node Trust Level			[16] -	[21] +						
	Non-Repudiation				[21] +						
	Reliability				[16] +						
	Strength of Encryption										
Usability	Cost					[3, 12, 16] +					
	Ease of Node Setup								[16] +		
	Ease of Use				[4, 5] +				[16] +		
	Support for Constrained Devices										

4.4. Risks Through the Use of DLT

For the second part of the concept matrix C-2 we identified a total of 17 risks, that organizations must consider using DLT for compliance. We aggregated them to nine master risks. A complete list of the master variables with descriptions is presented in Table 14. We coded the relationship between every characteristic of DLT and every risk. The complete and detailed results of the second part of C-2 are shown in the Appendix D. For a breakdown of C-2 we present in Table 15 and Table 16 the matrix with only aggregated risks.

Table 14: Master Variables: Risks through the use of DLT

Risks through the use of DLT	**Description**
Surveillance	Surveillance and profiling through evaluation of metadata.
Identification of perpetrator	Anonymity or pseudonymity of perpetrator.
Difficulties to restructure the IT and compliance system	Lack of expertise for blockchain technology. Required system modulations. Inconsistency problem if not all stakeholders participate and all necessary business processes are implemented via the DLT.
Non - Conformity of DLT with laws and regulations	Immutability of illegal content on the DLT. Non - Compliance with the GDPR.
Security problems	Hard fork-event can compromise the integrity of data. Mathematical or processing power advancements (e.g. quantum computers) can compromise DLT cryptography retroactively. Difficulties translating rules error-free into Smart Contract program code. Behavior of Smart Contract instances cannot be predicted with certainty. Zero-defect-tolerance of Smart Contracts during execution.
Job losses due to automation	Automation may lead to the reduction of intermediaries, process steps and a possible loss of jobs.
IT dependencies	Dominance of the miners: Monopoly position of the miners due to high computing requirements, miners can reject transactions, which increases dependency.
Performance problems	Performance of Peer-to-Peer networks inferior to regular networks.
High consumption of resources	Potentially insufficient storage capacities for the local storage of the DLT copy. High energy wastage.

Half of the authors focused only on the advantageous of DLTs and did not mention any risks, that are caused by DLT. The risks include economic risk, such as the consumption of resources as well as technical risk, such as security problems. Furthermore, we identified legal risks, such as non-conformity with laws and regulations and society risks, such as job losses due to automation. It is noticeable that especially the DLT properties transparency and security are the most beneficial properties to address several challenges. On the other hand, these properties are accountable for several risks. We will examine this in detail in the discussion chapter.

Table 15: Breakdown of Concept Matrix C-2: Risks through the use of DLT

DLT Properties	DLT Characteristics	Master Variable: Risks through the use of DLT									
		Surveillance	Identification of perpetrator	Difficulties to restructure the IT and compliance system	Non - Conformity of DLT with laws and regulations	Security problems	Job losses due to automation	IT dependencies	Performance problems	High consumption of resources
Community	Development Activity			[16] +						
	Developer Support			[16] +						
	Incentive Mechanisms									
	Network Size				[7] -				[16] -	
Flexibility	Interoperability			[16] +		[10] + [16] -				
	Maintainability									
	Modularity			[16] +						
	Smart Contract Support					[10, 16, 20] -	[16] -			
	Token Purposes									
Law & Regulation	Auditability									
	Compliance				[16] +					
	Governance Mechanisms							[16] +		
	Liability				[7] +					
Performance	Block Size									
	Computational Resources									[16, 17, 19] -
	Message Propagation Efficiency									
	Response Time								[16] +	
	Scalability								[16] +	
	Throughput								[16] +	
	Transaction Validation Latency									

Table 16: Breakdown of Concept Matrix C-2: Risks through the use of DLT

DLT Properties	DLT Characteristics	Master Variable: Risks through the use of DLT									
		Surveillance	Identification of perpetrator	Difficulties to restructure the IT and compliance system	Non - Conformity of DLT with laws and regulations	Security problems	Job losses due to automation	IT dependencies	Performance problems	High consumption of resources
Transparency	Traceability	[14, 16] -			[7] -					
	Transaction Content Visibility	[16] -			[7, 9] -					
	Unidentifiability	[16] +	[16] -		[7] +					
	Node Verification									
Security	Atomicity									
	Authentication									
	Availability									
	Confidentiality				[1] +					
	Consistency									
	Durability				[9] -					
	Fault Tolerance									
	Integrity				[4, 7, 9, 16, 18, 22] -	[16] 0 [16] -				
	Level of Decentralization									
	Node Trust Level									
	Non-Repudiation									
	Reliability									
	Strength of Encryption					[19] 0				
Usability	Cost									
	Ease of Node Setup			[16] +						
	Ease of Use			[16] +						
	Support for Constrained Devices				[7] -					[16] +

4.5. Business Use Cases of DLT in Compliance

The third concept matrix C-3 (see Appendix E) lists a total of 24 business use cases, where, according to the authors, DLT could addresses successfully challenges of compliance in organizations. We identified five business use cases in the financial sector, such as *Automated Know Your Customer (KYC) Checks of Financial Transactions* (Dillenberger et al., 2019) or *Financial Risk Management* (Kavassalis, Stieber, Breymann, Saxton, & Gross, 2018). KYC is a compliance requirement for financial institutions and insurances, to prevent money laundering and financing of terrorism. Furthermore, we identified eight business use cases in the area of auditing, such as *Auditing and Monitoring Compliance of Assets in a Circular (Economy) Business Model (CBM)* (Alexandris, Katos, Alexaki, & Hatzivasilis, 2018) and *Audit Logs in Online Transaction Processing (OLTP)* (Ahmad, Saad, Bassiouni, & Mohaisen, 2018).

In the area of Information Governance of Personal Data, the authors proposed in total four business use cases, such as *Blockchain Based Personally Identifiable Information Management System* (Al-Zaben et al., 2018) and *Health Insurance Portability and Accountability Act (HIPAA) Compliant Information Governance in the Healthcare Industry* (P. Zhang et al., 2017). Additional business use cases include *Supply Chain Provenance Tracking* (Dillenberger et al., 2019; Wohlgemuth, Umezawa, Mishina, & Takaragi, 2019), *Advertising Verification to Avoid Advertising Fraud* (Anjum, Sporny, & Sill, 2017), *Business Process Compliance in general* (Meironke et al., 2019), *Distributed Software Development with Open Source Licenses* (Singi et al., 2018) and *Critical Infrastructure Protection (CIP) Compliance* (Mylrea & Gourisetti, 2018).

5. Discussion

Due to the large number of DLT characteristics and compliance challenges and the limitation of this thesis, this discussion focuses on the most prominent relation between DLT characteristics and challenges. Regarding legal, economic and human-centered compliance challenges, the results suggest a rather low potential of improvement through the use of DLT. Thus, we will focus our discussion mainly on how DLT can address organizational and technical compliance challenges and review only a few aspects of economic and human-centered challenges.

DLT Design for Compliance

New DLT designs with different characteristics are constantly being developed and published, thus organizations raise the question which of the many DLT designs is most suitable to their needs. The type of application, the network size and the performance requirements are, among others, all aspects that define, what DLT design should be used for. There is not a one-size-fits-all DLT design for every situation, but rather it is conditioned by many trade-offs between different DLT characteristics. We will

look at some of these trade-offs in the following sections. For a comprehensive overview of the trade-offs of DLT characteristics we refer to Kannengießer et al. (2019b).
The results of our literature review show, that, despite the existence of other DLT concepts like TDAG, the authors mentioned and recommended only the Blockchain concept for the use in compliance. The overall consensus of Hyperledger or Ethereum as their favored Blockchain design has several reasons, although these two designs have different configurations and characteristics. The main reason is the advanced support of Smart Contracts by Hyperledger and Ethereum. As our results show, in most cases the use of Smart Contracts is the foundation of the solution statement to address the compliance challenge. We will discuss this in detail in the following section about Smart Contracts. Since all of the presented approaches in the literature are in a conceptual design phase, it is primarily important to implement a working prototype in the most efficiently manner. Hyperledger and Ethereum are a suitable choice for this matter, because both designs are open source with a strong developer and support community as well as being functional and stable (Ahmad et al., 2018, p. 447).

The Ethereum Blockchain in its original configuration is public and permissionless. This means that any transaction, Smart Contract or data on the distributed ledger is publicly viewable and anybody can be part of the network and the consensus process. While this could be a viable solution for governmental institutions or public organizations to provide full transparency, it is not the case for private organizations. Organizations do not want to have their financial records or customer data on such a permissionless and public network (Parra Moyano & Ross, 2017, p. 420). Hence, five of the nine authors, that recommended Ethereum, suggested a permissioned and private or consortium configuration based on the Ethereum Blockchain. The Quorum Blockchain is such a viable solution and fulfills confidentiality and governance requirements of organizations through its private and permissioned configuration. Furthermore, the Quorum Blockchain requires no decentralized consensus mechanism, like PoW or PoS, because of its private or consortium network. Quorum implements two consensus mechanisms: Raft-based and Istanbul BFT. These consensus mechanisms provide in comparison to PoW or PoS a higher transaction throughput and other beneficial characteristics for the use in organizational environments (JPMorgan Chase, 2018).

Hyperledger Fabric is by design a permissioned and private or consortium Blockchain. It offers high degrees of confidentiality and flexibility through a modular framework architecture (Magrahi et al., 2018, p. 2). Hyperledger Fabric implements the PBFT consensus mechanism, which provides a cost-efficient and high transaction throughput (Bayle, Koscina, Manset, & Perez-Kempner, 2018, p. 788). Organizations can configure and optimize Hyperledger Fabric exactly to their needs by changing different components, such as consensus mechanism, identity management or key management (Ahmad et al., 2018, p. 447).

Hyperledger as well as Quorum or any other private or consortium DLT still has a controlling entity, a so-called trusted third party (TTP), which governs the DLT-based network. By contrast, Ethereum eliminates the TTP through its public nature (Parra Moyano & Ross, 2017, pp. 419–420). In case of a private or consortium network, in which different organizations take part, an external entity can take the role of the TTP. Depending on the required compliance regulations, this entity could for instance be a governmental authority, regulator or third-party auditor. In theory, the TTP might be corrupt or compromised by hacking or by insider fraud. However, in most western countries the possibility of a corrupt TTP is considered to be low (Parra Moyano & Ross, 2017, pp. 419–420). Thus the beneficial characteristics of a private network like Hyperledger outweighs the risk of a corrupt TTP (Parra Moyano & Ross, 2017, pp. 419–420). In case of a corrupt TTP, the distributed validation through the PBFT protocol supports the detection of such abnormalities.

Smart Contracts

In many cases, it is possible to translate compliance requirements from legal terms into structured logical expressions (Dillenberger et al., 2019, p. 9), thus machine-readable code and then implement it into a Smart Contract. The process itself is a difficult challenge and demands very high technological and legal expertise (Al Khalil, Butler, O'Brien, & Ceci, 2017), though, the advantage is that Smart Contracts can monitor business processes or transactions and automatically enforce the compliance requirements in a detective way during runtime (Meironke et al., 2019, p. 1900). Another advantage is that organizations which operate in multiple countries with different laws, regulations and standards, are able to add each local compliance requirement to their international distributed ledger. Thus, Smart Contracts can be applied in the compliance processes of multi-national organizations or distributed working environments to automatically detect and inform conflicts about regulations from different jurisdictions. This prevents, for example, unconscious non-compliant acts of employees who were not aware of foreign compliance requirements. A suitable business use case is, for instance, the Distributed Software Development with Open Source Licenses (Singi et al., 2018).

Smart Contracts are also able to facilitate the auditing process with a third-party auditor (TPA), such as a governmental entity. For this purpose, different Smart Contracts control access rights and ownership registries of data or assets and the auditing policy for the TPA (Alexandris et al., 2018, p. 4). Smart Contracts can not only facilitate TPAs, but also supersede them in some use cases. Smart Contracts can automatically execute auditing tasks, such as verifying the integrity of data in databases, to omit the trust requirement for a TPA (Yu & Yang, 2018, p. 492). It is also possible to deploy compliance requirements with Smart Contracts between different interconnected DLTs, so-called satellite chains (W. Li, Sforzin, Fedorov, & Karame, 2017, p. 11). Another effective and resource efficient use of Smart Contracts is the automated, secured documentation and formatting of evidence, such as financial events and transactions

(Kavassalis et al., 2018, p. 50) or requests and permission logs of financial customer data (Norvill, Steichen, Shbair, & State, 2019, p. 10).

In the field of information governance of personal data, regulations, such as the GDPR, obligate organizations to provide the data owner with full control over their personal data. This includes full control over usage, deletion, transfers and access rights of their personal data (Al-Zaben et al., 2018, p. 77). Smart Contracts are able to hold and execute the terms and conditions for using the personal data of an individual along with their consent (Al-Zaben et al., 2018, p. 79). Hence, the individual, the data owner, keeps full control by dictating the conditions of the Smart Contract (Kaaniche & Laurent, 2017, p. 3). This could be a viable solution for an information governance system in the health care industry (Bayle et al., 2018).

Beside the many beneficial aspects of Smart Contracts, there are, however, some important risks that must be considered before their implementation. At first glance, the acceptance of high-level programming languages makes it relatively easy to specify and encode Smart Contracts (Frantz & Nowostawski, 2016, p. 211). However, it is difficult to fulfill the requirement of error-free code (J. Li, Greenwood, & Kassem, 2019, p. 290). Additionally, hybrid on/off-chain architectures fortify the risks of implementing buggy Smart Contracts due to their higher complexity (Molina-Jimenez et al., 2018, p. 86). A security bug or a deviation between the execution and the defined rule can cause legal problems, loss of sensitive information or financial losses and others. Therefore, Smart Contracts must be thoroughly validated and tested before their use (Molina-Jimenez et al., 2018, p. 86). From a social point of view an increase in automation of compliance tasks through Smart Contracts will likely lead to an elimination of unnecessary process activities and intermediaries, hence eventually to job losses (Meironke et al., 2019, p. 1902).

Transparency and Security

There are compliance processes that require the collaboration of multiple parties. In such a collaboration between organizations and customer, between multiple organizations or between organizations and trusted third parties like a TPA, trust issues occur. This is often based on asymmetric information (Akerlof, 1970). To reduce this asymmetry, a high level of transparency is desirable, while keeping identities as well as personal and business sensitive data protected. DLTs like Hyperledger or Ethereum provide a full chronological record of every transaction on the distributed ledger at any time (Dillenberger et al., 2019, p. 8). The traceability and the ability to view the content of the distributed ledger is the key factor for every auditing process, compliance monitoring, provenance tracking and verification of evidence and records. Timestamped and traceable records make corrective measures such as the investigation to the source of a compliance breach feasible. Liang et al. (2017), for instance, present a Blockchain-based data provenance tracking architecture for cloud storage applications. Their concept provides transparency and auditability for TPAs, while at the same time ensuring privacy for the content owner. Kaaniche

and Laurent (2017) developed a Hyperledger-based concept, with which organizations can provide auditing of data usage for their customer. Hence, the organization can fulfill the requirement to give data owners full transparency on how they collect, store, access and process their (personal) data. In the use case of distributed KYC identity data processing (Parra Moyano & Ross, 2017), one financial institution collects and stores the KYC identity data of a customer and shares it with the customers permission with other financial institutions, which are part of the same network. However, the financial institutions do not trust one another and compete for the customer's assets and accounts. The DLT allows them to collaborate anonymously, but ensures through Smart Contracts that all parties involved comply with regulations at all times (Parra Moyano & Ross, 2017, p. 422). DLT overcomes the trust issues between the collaborating parties by making all relevant information equally available to the involved parties, thus averting asymmetric information.

While transparency is necessary for many compliance tasks, the security, in particular the integrity and authenticity of data, is essential and the key benefit of DLT. To ensure these features, every node in the network validates and stores the entire data and executes every Smart Contract that is on the distributed ledger. This is a simplification of the validation and consensus process, since different DLT designs have different gradations of the functional range of the nodes. However, by raising the number of participating nodes, hence the level of decentralization, the integrity and the availability of the data improves. Considering again the previous use case, the KYC record of a customer is stored tamper-proof and consistently distributed in the ledger, which serves all financial institutions as well as TPAs as a single point of truth (Parra Moyano & Ross, 2017, p. 422). The DLT ensures that nobody, not even with access to the data, such as the data owning organization, a competitor, a government entity nor any third party is able to modify or erase any data on the distributed ledger. This prevents the conscious misconduct of hiding, altering or faking records and is essential, when verifying documentation, conducting audits or investigating into compliance breaches.
In addition to the authenticity and integrity of data on the distributed ledger, organizations gain full control over access rights of data through private and public key management (Liang et al., 2017, p. 472). The benefit of confidentiality is especially relevant for preserving data privacy and anonymity, but also for business sensitive or safety-critical data. The use case of a multi-disciplinary optimization (MDO) process between distributed engineering teams in the aircraft building industry illustrates the benefit of DLT (Reniers et al., 2019). Engineering teams from multiple organizations collaborate in the research and development process and thus need to share safety-critical information. Due to the safety critical nature of the data, the non-repudiation of data access operations and its auditability must be ensured (Reniers et al., 2019, p. 346). The proposed DLT fulfills the requirement of sharing the data confidentially among the specific parties while preserving accessibility only to the designated parties (Reniers et al., 2019, p. 348). Every data access and modification is recorded on the distributed ledger to provide non-repudiation and auditability (Reniers et al., 2019, p. 347).

Even though the DLT provides confidentiality and anonymity and data is usually additionally encrypted, there remains the potential risk of surveillance or profiling through the analysis of metadata of transactions (Ma et al., 2018, p. 74). The metadata, such as transaction times, is publicly available due to the traceability and transaction content visibility. Another controversial aspect is the unidentifiability characteristic. In case of an investigation into an infringement of compliance, it is difficult to identify the perpetrator, if the DLT provides anonymity or pseudonymity through a high degree of unidentifiability (Meironke et al., 2019).

The increase in digitalization of compliance processes make organization more dependent on a stable, functional and continuous IT system. A high level of decentralization averts the dependency in one entity as a single point of failure (Liang et al., 2017, p. 474). The DLT's degree of availability, durability, fault tolerance and reliability are dependent on the DLT design, configuration, consensus mechanism and on the size and complexity of the network. In case of single nodes failing, the distributed character helps the system to be less vulnerable. This supports the use in critical infrastructure systems, such as the use for cybersecurity of energy grids. Mylrea and Gourisetti (2018) elaborate the advantages of a Blockchain-based system for the North American Electric Reliability (NERC) Critical Infrastructure Protection (CIP) compliance process. They propose a system that automatically detects compliance violations in a preventative way already at design time as well as during runtime (Mylrea & Gourisetti, 2018, pp. 71–72).

Interoperability and Performance

Many of the above-mentioned possible applications of Smart Contracts require the interoperability with other systems to address the compliance challenge. This includes the interoperability of Smart Contracts or the whole DLT with other trusted structures or interfaces, such as non-DLT-based IT-systems or other DLTs. The external (off-chain) sources, from which the Smart Contract retrieves data, are called oracles. As an example. in distributed KYC identity data processing the bank's local non-DLT-based client application communicates with a Smart Contract of a customer in order to obtain the customer's KYC verification status (Parra Moyano & Ross, 2017, p. 419).

In this use cases, the required storage capacity of a DLT for a small data set per individual is sufficient. In other use cases, extensive documentation and large files must be stored for compliance. Since the current DLT designs are not capable of storing large data files and being scalable as well as providing high performance at the same time, the solution is a hybrid on/off-chain storage system (Reniers et al., 2019, pp. 350–351). The term on/off-chain stems originally from the Blockchain but is used here universal for any DLT. The actual data is stored off-chain in a trusted database and the distributed ledger only stores hash values of the data and, or metadata, such as its location. This way, a modification of the actual data changes the hash value. It is therefore possible to recognize any modification of the data in

the database by comparing the original hash value on the distributed ledger with the current hash value of the data (Al-Zaben et al., 2018, p. 80). This provides verification of data integrity and availability of the data at the same time (Reniers et al., 2019, p. 351). Furthermore, an off-chain solution reduces significantly the computational resources and cost for storing data on-chain (P. Zhang et al., 2017, p. 2).

Another reasons to store data off-chain is the risk that DLT is not compliant with regulations regarding the controlling and processing of personal data. For instance, article 17 of the GDPR requires "the right to be forgotten" meaning that the data owner has the right to obtain erasure or complete anonymization of his personal data at any time without undue delay (General Data Protection Regulation, 2016). This requirement contradicts the before mentioned benefit of the integrity of data in DLT. All of the presented DLT designs do not allow the erasure or modification of any transaction respectively data on the distributed ledger (Schmelz et al., 2018, p. 227). Even if the distributed ledger contains only encrypted personal data, the GDPR qualifies it only as pseudonymized not anonymized personal data, which does not fall under the scope of the GDPR. In article 32, the GDPR defines pseudonymization only as a suggested security measure, since encryption can be broken by trial and error (so-called brute force attacks) or by future quantum computing (Bayle et al., 2018, p. 790). Furthermore, in the case that illegal content enters the distributed ledger, the integrity of data makes the whole distributed ledger illegal (Ateniese, Magri, Venturi, & Andrade, 2017, p. 112). An off-chain storage solution bypasses this risk.

The Blockchain-based data storage solutions InterPlanetary File System (IPFS), Storj and Blockstack all solve the problem of storing large data files decentralized and safe (Magrahi et al., 2018, p. 2). However, they are also unable to fulfill the compliance requirements of the GDPR (Magrahi et al., 2018, p. 2). In order to develop GDPR-compliant DLT solutions, personal data must be stored off-chain and erasable. This diminishes the benefits of transparency and security, in particular the confidentiality of the data at the transition of the DLT-based system to the off-chain oracle. Therefore, the use of off-chain storage solutions should be limited to the necessary minimum, since a purer DLT setup provides a higher leverage of the DLT-based solution (Parra Moyano & Ross, 2017, p. 414).
In conclusion, storing the data on the distributed ledger is, for now, not an effective solution. Hyperledger and R3 Corda are developing more advanced DLTs, where larger data could be stored on the distributed ledger (Parra Moyano & Ross, 2017, p. 421). However, the risk of being non-compliant with data protection regulations will persist. Nevertheless, one advantage of a hybrid on/off-chain solution is that organizations can implement the DLT more easily in an existing system, if the main data remains in the current data base.

Apart from legal risks, current DLTs face performance problems, due to technical restrictions. This limits the scalability of the network. However, the relevance of the scalability depends on the use case, as the following examples illustrate. In the afore mentioned case, confidential data sharing in federated

MDO the number of collaborating parties is relatively low and constant. In such a business use case, the scalability regarding the number of participating nodes of a private or consortium distributed ledger network will be sufficient. Ahmad et al. (2018) examine the performance of their Hyperledger-based auditing architecture. In their experiment, they evaluate the correlation between the number of nodes in their network and the transaction validation latency with regard to different payload sizes of the transaction. The payload ranges from 2 Megabyte to 20 Megabyte. Their results show that independently of the payload size, the network latency margins remain insignificant as long as the network consists of less than 30 nodes (Ahmad et al., 2018, p. 447). If the number of nodes exceeds 30, the latency factor increases significantly with every additional node (Ahmad et al., 2018, p. 447).

In other use cases, such as the information governance in the healthcare industry, the DLT must be very scalable to provide services for millions of patients (P. Zhang et al., 2017, p. 3). The required scalability cannot be achieved by any DLT currently available. To increase the performance, especially the scalability in private or consortium networks, multiple parallel distributed ledgers are interconnected. This method is called sharding and requires a high interoperability between those distributed ledgers (W. Li et al., 2017). The developers of Ethereum are currently working on Ethereum 2.0 with the objective to increase the scalability through sharding, a shift from the PoW consensus mechanism to PoS and off-chain solutions. An additional aspect is the high energy consumption of the PoW consensus mechanism (Mylrea & Gourisetti, 2018, p. 76). Considering the challenges of climate change, organizations should avoid such consensus mechanisms, if there are not powered by renewable energy. Consensus mechanisms in private or consortium distributed ledgers, such as Hyperledger's PBFT consensus, are much more energy efficient.

Economic aspects and Usability

Beside organizational and technical challenges of compliance, organizations face high and increasing costs for the provision of compliance. Thus, one key factor for the decision whether an organization uses DLT for compliance, is the final cost-value ratio of implementing and operating a DLT.

One advantage of DLT is that the automation of compliance tasks through Smart Contracts can reduce the resource effort and therefore the costs for organizations for the provision of compliance (Kavassalis et al., 2018, p. 45). Furthermore, in a consortium of organizations DLT can replace centralized compliance management systems that operate in parallel. In such a distributed system with multiple collaborating organizations, the costs for the system can be divided proportionally. In the use case of distributed KYC identity data processing, the customer needs to carry out the KYC process only once with a financial institution (Shbair et al., 2018, p. 4). Once the customer intends to work with other financial institutions, they can share their KYC results through the distributed ledger with those financial institutions (Shbair et al., 2018, p. 4). This eliminates duplicated tasks for both parties and the financial institutions share the cost for the KYC process proportionally among them (Parra Moyano & Ross, 2017, p. 417).

Smart Contracts control and automatically execute the money transfer in cryptocurrency, while maintaining full anonymity for the financial institutions (Parra Moyano & Ross, 2017, p. 417).

Many aspects of this discussion on DLT's potential for compliance are inhibited by the lack of practical implementations in a realistic environment. All of the proposed solutions in the literature are either still at a conceptual stage or were evaluated only as a prototype in a test environment. Therefore, it is difficult to calculate and foresee the operating cost and required resources for a DLT implementation for compliance tasks at the moment. Organizations need to deliberate for their specific use case, whether the advantage of DLT outweigh the operating costs and investments of converting all necessary applications to a DLT-based system. If an organization uses a conventional system parallel to the DLT for the same compliance tasks, they cannot assure consistency of their data. This risk of inconsistency can also occur if not all required stakeholders, such as collaborating organizations, governmental entities or TPAs, participate with the new DLT-based system. To reduce this risk, further simplification of setting up a distributed ledger system and an improvement in the ease of use is necessary.

6. Conclusion

The third generation of DLT allows advanced and various applications with Smart Contracts in an environment of interconnected organizations, external entities and real-world processes. Organizations operate in such an environment and are engaged with compliance requirements. Organizations face a multitude of challenges to fulfill these compliance requirements, but they lack a general understanding for this emerging technology regarding the use in compliance. Thus, we raised the following research question: What are the potentials and risks for the use of DLT for organizational compliance? We conducted a literature review of the current state of research of DLT in compliance. Based on this review, we identified compliance challenges in organizations and provided an overview, what challenges DLT can address due to its distinctive and beneficial characteristics. The results suggest that DLT has a high potential to address organizational and technical challenges, though, economic, human-centered and legal challenges are only partially addressed.

The implementation of Smart Contracts is the key concept of DLT for compliance challenges. Compliance requirements can be translated and implemented into Smart Contracts to monitor business processes and automatically enforce compliance. Furthermore, Smart Contracts are able to execute automatic auditing tasks and control access rights and auditing policies for TPAs. Smart Contracts can be used for automatic documentation and verification of evidence in a secure and consistent manner. In the field of information governance of personal data, Smart Contracts control the access rights and usage of personal data, to protect the data owner's privacy.

The underlying distributed ledger provides the secure and transparent storage of all evidence that is required for compliance while preserving confidentiality for the content owner. In particular, the integrity of the DLT ensures that nobody is able to modify or erase any data on the distributed ledger, which

prevents conscious fraud. Time-stamped, authentic and traceable records on the distributed ledger are essential for verifying documentations, conducting audits and the investigation into compliance breaches. DLT can reduce the cost for the provision of compliance by automating compliance tasks with Smart Contracts or by sharing the cost for a distributed compliance management Systems with collaborating organizations. However, due to the conceptual stage of the DLT solutions the overall costs-benefit ratio in comparison to conventional systems is difficult to calculate and depends on the use case.

Beside the potentials of DLT for compliance, we identified several risks that organizations must consider using DLT for this matter. Smart Contracts are difficult to implement error-free and a deviation between the execution and the defined rule can cause severe risks. Thus, a thorough validation is inevitable before deployment. For many compliance tasks Smart Contracts need to interoperate with external non-DLT-based IT systems or other DLTs. In addition, due to the limited storage capacity of current DLTs or the GDPR requirement of the right to erasure of personal data, storing large or personal data off-chain is inevitable. However, this diminishes the benefits of DLT. A controversial aspect and risk is that on the one hand the DLT provides the required confidentiality and anonymity for collaborating organizations but on the other hand this characteristic impedes the identification of a perpetrator in case of an infringement of compliance. Considering the challenges of climate change, the high energy consumption of the PoW consensus mechanism in public DLTs needs to be avoided. While developers are working on different solutions and improvements, current DLTs face also performance problems, if the required network needs to be scaled to a large number of participants.

Due to the overall consensus of the authors to use a Hyperledger or Ethereum based Blockchain, we compared both designs to distinguish their advantages and suitable use cases of compliance. The most prominent characteristic of both DLT designs is the advanced support of Smart Contracts, which is essential for compliance tasks. The modular Hyperledger framework Fabric is most suitable for smaller trusted environments in private or consortium enterprise networks, where it provides a cost-efficient and high transaction throughput. Additionally, the consensus mechanism of Hyperledger Fabric is much more energy efficient. Ethereum is most suitable for compliance applications in large untrusted public networks, where a high degree of decentralization is required, such as the information governance in the health care industry. Further concrete business use cases, where DLT is able to address compliance challenges, are foremost in the financial sector or related to auditing. The secure and reliable character of DLT makes it also suitable for compliance in critical infrastructure IT systems.

6.1. Limitations of this Work

Since compliance, as the area of application for DLT, is a rather new field of research, there is constantly new scientific literature published or under review. We therefore limited our analysis to already published scientific literature until 22 August 2019. Additionally, the published literature represents only a

part of the global research regarding this field, due to the fact that many DLT projects are published in white papers or are private commercial research projects by organizations. All of the analyzed literature studied only the DLT concept Blockchain. Therefore, our derived results are limited to the generalizability of DLT characteristics to other concepts. The concept matrix C2 only consists of those relationships that were studied by the author. Due to the large number of DLT characteristics and the limitation of scientific articles, not every author studied every characteristic in relationship to their topic, which limits the quantitative results of our concept matrix C2. Due to the limitation of this work, we are not able to consider every tradeoff between different DLT characteristics and different DLT designs. For a more detailed overview we refer to Kannengießer et al. (2019b).

6.2. Future Research

The proposed DLT-based solutions are still in a conceptual stage. Thus, the next step is to convert the concept into a working prototype and implement it in an appropriate business environment. Analyzing the functionality and performance of the operating DLT, especially in the interaction with oracles, will provide further information on the impact of the network structure. The analysis should be extended, if applicable, to different DLT designs in order to have a comprehensive comparison which DLT design is most suitable for a given compliance challenge and business use case. As most of the proposed concepts focus on addressing one particular compliance challenge, further research must be conducted regarding the combination of different concepts to one DLT system, that addresses multiple compliance requirements. As an example, many concepts are successfully addressing an organizational challenge, but are not compliant with the GDPR.

Despite the exigency of climate change and illegal destruction of biotopes, we identified no business use cases with regard to environmental compliance. Thus, we suggest further research into the use of DLT for environmental compliance requirements, such as the supply chain provenance tracking of natural resources.

Appendix

A. List of Relevant Literature with Reference Number

Author	Title	Reference Number
Abreu et al. (2018)	Blockchain technology in the auditing environment	**1**
Ahmad et al. (2018)	Towards Blockchain-Driven, Secure and Transparent Audit Logs	**2**
Alexandris et al. (2018)	Blockchains as Enablers for Auditing Cooperative Circular Economy Networks	**3**
Al-Zaben et al. (2018)	General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management	**4**
Anjum et al. (2017)	Blockchain Standards for Compliance and Trust	**5**
Bayle et al. (2018)	When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry	**6**
Buocz et al. (2019)	Bitcoin and the GDPR: Allocating responsibility in distributed networks	**7**
Dillenberger et al. (2019)	Blockchain Analytics and Artificial Intelligence	**8**
Hofman et al. (2019)	"The margin between the edge of the world and infinite possibility"	**9**
J. Li et al. (2019)	Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases	**10**
Kaaniche and Laurent (2017)	A blockchain-based data usage auditing architecture with enhanced privacy and availability	**11**
Kavassalis et al. (2018)	An innovative RegTech approach to financial risk monitoring and supervisory reporting	**12**
Liang et al. (2017)	ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability	**13**
Ma et al. (2018)	Nudging Data Privacy Management of Open Banking Based on Blockchain	**14**
Magrahi et al. (2018)	NFB: A Protocol for Notarizing Files over the Blockchain	**15**
Meironke et al. (2019)	Business Process Compliance and Blockchain: How Does the Ethereum Blockchain Address Challenges	**16**
Mylrea and Gourisetti (2018)	Blockchain for Supply Chain Cybersecurity, Optimization and Compliance	**17**
Norvill et al. (2019)	Demo: Blockchain for the Simplification and Automation of KYC Result Sharing	**18**
P. Zhang et al. (2017)	Metrics for assessing blockchain-based healthcare decentralized apps	**19**
Parra Moyano and Ross (2017)	KYC Optimization Using Distributed Ledger Technology	**20**
Reniers et al. (2019)	Analysis of architectural variants for auditable blockchain-based private data sharing	**21**
Schmelz et al. (2018)	Towards Using Public Blockchain in Information-Centric Networks: Challenges Imposed by the European Union's General Data Protection Regulation	**22**
Shbair et al. (2018)	Blockchain orchestration and experimentation framework: A case study of KYC	**23**
Singi et al. (2018)	Compliance adherence in distributed software delivery	**24**
W. Li et al. (2017)	Towards Scalable and Private Industrial Blockchains	**25**
Wohlgemuth et al. (2019)	Competitive Compliance with Blockchain	**26**
Yu and Yang (2018)	Decentralized and Smart Public Auditing for Cloud Storage	**27**

B. Concept Matrix C-1: DLT Concepts and Designs

DLT Concept	Blockchain																			
DLT Design	Ethereum	Hyperledger	Hyperledger Fabric	Blockchain (g. t.)	Quorum	ProvChain	Multichain 2.0	R3 Corda	Sia (filesharing)	Filecoin (filesharing)	Factom	Verady	PikcioChain	Truyo	Volta	permissioned	permissionless	private	public	consortium
Ref. No.																				
1											x	x								
2		x	x																	
3	x				x											x				
4							x											x		
5	x																			
6		x	x															x		x
7																x				x
8			x																	
9													x	x	x					
10																x		x	x	
11		x														x				x
12	x	x														x				
13						x														
14																				
15		x			x											x				
16	x																x		x	
17				x												x				
18	x															x		x		
19	x																			
20	x	x						x								x		x		
21		x				x			x	x						x				
22																				
23	x	x					x											x		x
24				x																
25			x													x		x		
26																				
27	x																			
FREQ.	9	8	4	2	2	2	2	1	1	1	1	1	1	1	1	11	1	7	2	4

C. Concept Matrix C-2: Challenges in Compliance

DLT Properties	Challenge in Compliance	Complexity of compliance requirements		Transformational pace and change of compliance requirements		Difficult interpretation of compliance requirements	
	DLT Characteristics	High number and complex compliance requirements	Conflicting compliance requirements	Continuous change of compliance requirements	Rapid change of compliance requirements	Divergent interpretation of terms and concepts	Insufficient implementation guidelines
Community	Development Activity						
	Developer Support						[16] +
	Incentive Mechanisms						
	Network Size					[16] +	
Flexibility	Interoperability					[16] +	
	Maintainability						
	Modularity						
	Smart Contract Support	[16] +	[16] +	[16] +	[16] +		
	Token Purposes						
	Transaction Size Limit						
Law & Regulation	Auditability						
	Censorship Resistance						
	Compliance						
	Governance Mechanisms						
	Liability						
Performance	Block Creation Interval						
	Block Size						
	Confirmation Latency						
	History Retention						
	Computational Resources						
	Message Propagation Efficiency						
	Propagation Delay						
	Response Time						
	Scalability						
	Throughput						
	Transaction Validation Latency						

DLT Properties	Challenge in Compliance	Complexity of compliance requirements		Transformational pace and change of compliance requirements		Difficult interpretation of compliance requirements	
	DLT Characteristics	High number and complex compliance requirements	Conflicting compliance requirements	Continuous change of compliance requirements	Rapid change of compliance requirements	Divergent interpretation of terms and concepts	Insufficient implementation guidelines
Transparency	Traceability						
	Transaction Content Visibility						
	Unidentifiability						
	Node Verification						
Security	Atomicity						
	Authentication						
	Availability						
	Confidentiality						
	Consistency						
	Durability						
	Fault Tolerance						
	Integrity						
	Isolation						
	Level of Decentralization						
	Node Trust Level						
	Non-Repudiation						
	Reliability						
	Stale Block Rate						
	Strength of Encryption					[16] +	[16] +
Usability	Cost						
	Ease of Node Setup						
	Ease of Use						
	Support for Constrained Devices						

DLT Properties	Challenge in Compliance	Complexity of business and compliance processes			Modeling and design-time verification of compliance requirements			
	DLT Characteristics	Organization size, multitude of business and compliance processes	Complex global business and compliance processes	Rapid business process model change	Complex risk and vulnerability analysis in business processes	Modeling and mapping compliance requirements to business processes	Incomplete documentation of business processes	Various process modeling languages
Community	Development Activity							
	Developer Support							
	Incentive Mechanisms							
	Network Size							
Flexibility	Interoperability				[16] +	[16] +	[16] +	[16] +
	Maintainability							
	Modularity							
	Smart Contract Support	[16] +	[16, 24] +	[16] +	[16] +	[16] +	[16] +	[16] +
	Token Purposes							
	Transaction Size Limit							
Law & Regulation	Auditability							
	Censorship Resistance							
	Compliance							
	Governance Mechanisms		[16] +					
	Liability							
Performance	Block Creation Interval							
	Block Size							
	Confirmation Latency							
	History Retention							
	Computational Resources							
	Message Propagation Efficiency							
	Propagation Delay							
	Response Time							
	Scalability							
	Throughput							
	Transaction Validation Latency							

DLT Properties	Challenge in Compliance	Complexity of business and compliance processes			Modeling and design-time verification of compliance requirements			
	DLT Characteristics	Organization size, multitude of business and compliance processes	Complex global business and compliance processes	Rapid business process model change	Complex risk and vulnerability analysis in business processes	Modeling and mapping compliance requirements to business processes	Incomplete documentation of business processes	Various process modeling languages
Transparency	Traceability	[16] +	[16] +		[16] +		[16] +	
	Transaction Content Visibility	[16] +	[16] +		[16, 17] +		[16] +	
	Unidentifiability							
	Node Verification				[17] +			
Security	Atomicity	[25] +						
	Authentication							
	Availability	[25] +						
	Confidentiality				[17] +			
	Consistency	[25] +						
	Durability							
	Fault Tolerance				[17] +			
	Integrity				[17] +			
	Isolation							
	Level of Decentralization	[16] +	[16] +		[17] +			
	Node Trust Level							
	Non-Repudiation							
	Reliability							
	Stale Block Rate							
	Strength of Encryption	[16] +						
Usability	Cost							
	Ease of Node Setup							
	Ease of Use	[16] +	[16] +					
	Support for Constrained Devices							

DLT Properties	Challenge in Compliance	Compliance monitoring and auditability			Financial risk monitoring		Transparency and traceability of compliance		
	DLT Characteristics	High manual, time-consuming effort to forward compliance checking	Compliance monitoring	Auditability	Transparency of risks	Anonymity between financial institutes	Reporting channels	Anonymity for whistleblowers	Traceability of compliance requirements and sources
Community	Development Activity								
	Developer Support								
	Incentive Mechanisms								
	Network Size								
Flexibility	Interoperability		[3] +	[3, 25]+					
	Maintainability			[27] +					
	Modularity			[2] +					
	Smart Contract Support	[16] +	[3, 16, 17] +	[2, 3, 8, 16, 17, 25, 27] +					[16] +
	Token Purposes			[1] +					
	Transaction Size Limit								
Law & Regulation	Auditability			[3, 8, 16, 25] +			[16] +		[16] +
	Censorship Resistance								
	Compliance			[1] +					
	Governance Mechanisms			[13, 20, 25] +					
	Liability								
Performance	Block Creation Interval								
	Block Size								
	Confirmation Latency								
	History Retention								
	Computational Resources								
	Message Propagation Efficiency								
	Propagation Delay								
	Response Time								
	Scalability								
	Throughput								
	Transaction Validation Latency			[2] +					

DLT Properties	Challenge in Compliance	Compliance monitoring and auditability			Financial risk monitoring		Transparency and traceability of compliance		
	DLT Characteristics	High manual, time-consuming effort to forward compliance checking	Compliance monitoring	Auditability	Transparency of risks	Anonymity between financial institutes	Reporting channels	Anonymity for whistleblowers	Traceability of compliance requirements and sources
Transparency	Traceability		[16, 24] +	[8, 9, 13, 16, 20, 24, 27] +	[20] +				[16, 20, 24] +
	Transaction Content Visibility		[16, 24] +	[8, 13, 16, 24] +					[16, 24] +
	Unidentifiability			[13] +		[20] +		[16] +	
	Node Verification			[2] +					
Security	Atomicity			[1] +					
	Authentication			[1, 8, 9, 25] +					
	Availability		[16] +	[2, 9, 16] +					
	Confidentiality			[1, 3, 13, 14, 17] +					
	Consistency			[1, 2, 8] +					
	Durability			[1, 8] +					
	Fault Tolerance								
	Integrity			[1, 2, 8, 9, 11, 16, 18, 20, 27] +					
	Isolation								
	Level of Decentralization			[2, 25, 27] +					[16] +
	Node Trust Level			[2] +					
	Non-Repudiation								
	Reliability								
	Stale Block Rate								
	Strength of Encryption								
Usability	Cost								
	Ease of Node Setup								
	Ease of Use			[2, 3, 5] +					
	Support for Constrained Devices								

DLT Properties	Challenge in Compliance	Precise documentation and verification					Technical support and automation of Compliance	
	DLT Characteristics	Non-repudiation of action regarding data (e.g. access to data)	Authenticity and integrity of evidence and records	Provenance tracking	Effort and resources needed regarding archiving and processing of evidence and records	Know Your Customer (KYC): diligence process	Identification of compliance violations and fraud	Low level and potential of automation of compliance processes
Community	Development Activity							
	Developer Support							
	Incentive Mechanisms			[13] +				
	Network Size							
Flexibility	Interoperability		[3, 12] +	[6, 8] +	[12] +	[20] +		
	Maintainability					[20] +		
	Modularity			[6] +				
	Smart Contract Support		[3, 12, 16, 24] +	[6] +	[3, 12, 17, 18] +	[14, 18, 23] +	[8, 16, 17] +	[16, 24, 20, 17] +
	Token Purposes					[20] +		
	Transaction Size Limit							
Law & Regulation	Auditability		[1, 3, 12] +				[8] +	
	Censorship Resistance							
	Compliance					[20] +		
	Governance Mechanisms		[3] +			[20] +		
	Liability					[20] +		
Performance	Block Creation Interval							
	Block Size				[12] -			
	Confirmation Latency							
	History Retention							
	Computational Resources				[12] 0			
	Message Propagation Efficiency							
	Propagation Delay							
	Response Time		[12] +					
	Scalability				[12] 0			
	Throughput							
	Transaction Validation Latency							

DLT Properties	Challenge in Compliance	Precise documentation and verification					Technical support and automation of Compliance	
	DLT Characteristics	Non-repudiation of action regarding data (e.g. access to data)	Authenticity and integrity of evidence and records	Provenance tracking	Effort and resources needed regarding archiving and processing of evidence and records	Know Your Customer (KYC): diligence process	Identification of compliance violations and fraud	Low level and potential of automation of compliance processes
Transparency	Traceability		[1, 12, 14, 16]+	[2, 3, 6, 15, 16, 20] +			[8, 13, 16] +	[16] +
	Transaction Content Visibility		[1, 3, 12, 16, 17] +	[2] +			[8, 16] +	[16] +
	Unidentifiability					[20] +		
	Node Verification		[17] +					
Security	Atomicity		[1] +					
	Authentication		[1, 3, 16, 24] +	[13] +			[8] +	
	Availability		[3, 12, 16] +					
	Confidentiality		[3, 17] +					
	Consistency		[1, 2, 3, 12] +				[8] +	
	Durability		[3, 12] +	[3, 13] +			[8] +	
	Fault Tolerance		[3,17] +	[13] +				
	Integrity	[2, 21] +	[1, 2, 3, 9, 12, 13, 16, 17, 24] +	[3, 8, 13, 17, 20] +			[1, 8] +	
	Isolation							
	Level of Decentralization		[2, 17] +	[13, 23] +		[23] +		
	Node Trust Level							
	Non-Repudiation	[21] +						
	Reliability		[12] +	[13] +				
	Stale Block Rate							
	Strength of Encryption							
Usability	Cost				[12] +			
	Ease of Node Setup							
	Ease of Use			[5] +				
	Support for Constrained Devices							

DLT Properties	Challenge in Compliance	Complex and inefficient IT and compliance infrastructure and low system integration				Centralization of service provider		
	DLT Characteristics	Distributed, heterogeneous and isolated applications and systems	Parallel systems and redundant data	Inconsistent data and decisions of management	Incompatible IT systems	Monopoly of service providers	Service provider as single-point-of-failure	Lack of trust regarding the service provider
Community	Development Activity							
	Developer Support							
	Incentive Mechanisms							
	Network Size							
Flexibility	Interoperability	[16] +	[16] +	[16] +	[16] +			
	Maintainability							
	Modularity	[16] +			[16] +			
	Smart Contract Support	[16] +	[16, 18] +	[16] +	[16] +			
	Token Purposes							
	Transaction Size Limit							
Law & Regulation	Auditability							
	Censorship Resistance							
	Compliance							
	Governance Mechanisms					[16] -	[20] -	[16, 20] -
	Liability							
Performance	Block Creation Interval							
	Block Size							
	Confirmation Latency							
	History Retention							
	Computational Resources							
	Message Propagation Efficiency							
	Propagation Delay							
	Response Time							
	Scalability							
	Throughput							
	Transaction Validation Latency							

DLT Properties	Challenge in Compliance	Complex and inefficient IT and compliance infrastructure and low system integration				Centralization of service provider		
	DLT Characteristics	Distributed, heterogeneous and isolated applications and systems	Parallel systems and redundant data	Inconsistent data and decisions of management	Incompatible IT systems	Monopoly of service providers	Service provider as single-point-of-failure	Lack of trust regarding the service provider
Transparency	Traceability		[20] +		[19] +			[16] +
	Transaction Content Visibility	[16] +	[16] +	[16] +	[19] +			[13, 16] +
	Unidentifiability							
	Node Verification							
Security	Atomicity							
	Authentication							
	Availability						[16] +	
	Confidentiality						[16] +	
	Consistency	[16] +	[16] +	[16] +				
	Durability							
	Fault Tolerance							
	Integrity				[19] +		[16] +	[13] +
	Isolation							
	Level of Decentralization				[19] +	[16] +	[13, 16] +	[16] +
	Node Trust Level							[16] -
	Non-Repudiation							
	Reliability							
	Stale Block Rate							
	Strength of Encryption							
Usability	Cost							
	Ease of Node Setup							
	Ease of Use							
	Support for Constrained Devices							

DLT Properties	Challenge in Compliance	Technical aspects of data security and privacy							
	DLT Characteristics	Confidentiality of data	Availability of data	Authenticity of data	Integrity of data	Transparency of data storing and usage	Data privacy (e.g. GDPR) and anonymity	Patching critical IT and operational technology systems	Auditing of private data usage
Community	Development Activity								
	Developer Support								
	Incentive Mechanisms		[16] +						[27] +
	Network Size								
Flexibility	Interoperability					[18] +	[19] +		[11, 18] +
	Maintainability								[27] +
	Modularity								
	Smart Contract Support		[10] +		[10, 27] +		[4, 6, 14] +	[17] +	[11, 21, 27] +
	Token Purposes								
	Transaction Size Limit								
Law & Regulation	Auditability					[15] +			[11, 21, 26] +
	Censorship Resistance								
	Compliance						[11, 26] +		[11] +
	Governance Mechanisms							[17] +	[11, 21] +
	Liability								[11] +
Performance	Block Creation Interval								
	Block Size								
	Confirmation Latency								
	History Retention								
	Computational Resources				[16] -		[19] -		[21] -
	Message Propagation Efficiency								[21] -
	Propagation Delay								
	Response Time								[27] +
	Scalability						[19] +		[27] +
	Throughput								
	Transaction Validation Latency								

DLT Properties	Challenge in Compliance	Technical aspects of data security and privacy							
	DLT Characteristics	Confidentiality of data	Availability of data	Authenticity of data	Integrity of data	Transparency of data storing and usage	Data privacy (e.g. GDPR) and anonymity	Patching critical IT and operational technology systems	Auditing of private data usage
Transparency	Traceability				[4, 10] +	[4, 14, 16, 18] +		[17] +	[11, 18, 27] +
	Transaction Content Visibility					[11] +	[22] -	[17] +	[11] +
	Unidentifiability						[13, 16] +		[11] +
	Node Verification						[22] +		
Security	Atomicity								
	Authentication			[9, 16, 26] +					[21] +
	Availability		[11, 16, 17] +				[22] +		[21] +
	Confidentiality	[6, 11, 13, 15, 18, 21, 26] +				[18] +	[13, 14, 19] +		[11, 21] +
	Consistency								
	Durability						[19, 22] -		
	Fault Tolerance		[27] +						[11, 27] +
	Integrity				[9, 11, 13, 14, 16] +		[4, 7, 9, 16, 18, 19, 22] -	[17] +	[11, 21, 27] +
	Isolation								
	Level of Decentralization		[13, 27] +		[4, 13, 20, 23] +	[20, 23] +	[22] -		[27] +
	Node Trust Level								[21] +
	Non-Repudiation								[21] +
	Reliability	[16] +	[16] +		[16] +	[16] +	[16] +		
	Stale Block Rate								
	Strength of Encryption								
Usability	Cost								
	Ease of Node Setup								
	Ease of Use					[4] +			[5] +
	Support for Constrained Devices								

DLT Properties	Challenge in Compliance	Inadequate cost efficiency of provision of compliance			Insufficient efficiency of resources		Difficulties concerning measurability of compliance	
	DLT Characteristics	Costs for provision of compliance	Lack of cost efficiency of compliance processes	Consequential charges and legal costs	Low alignment to efficiency	Inefficient allocation of resources	Extensive data processing and evaluation	Lack of key figures and measurement methods to evaluate cost efficiency
Community	Development Activity							
	Developer Support							
	Incentive Mechanisms	[16] -				[16] +		[16] +
	Network Size							
Flexibility	Interoperability							
	Maintainability							
	Modularity							
	Smart Contract Support	[14, 16, 18, 20] +	[20] +		[16] +	[16] +	[16] +	[16] +
	Token Purposes							
	Transaction Size Limit							
Law & Regulation	Auditability							
	Censorship Resistance							
	Compliance					[16] +		
	Governance Mechanisms							
	Liability							
Performance	Block Creation Interval							
	Block Size							
	Confirmation Latency							
	History Retention							
	Computational Resources							
	Message Propagation Efficiency							
	Propagation Delay							
	Response Time							
	Scalability							
	Throughput							
	Transaction Validation Latency							

DLT Properties	Challenge in Compliance	Inadequate cost efficiency of provision of compliance			Insufficient efficiency of resources		Difficulties concerning measurability of compliance	
	DLT Characteristics	Costs for provision of compliance	Lack of cost efficiency of compliance processes	Consequential charges and legal costs	Low alignment to efficiency	Inefficient allocation of resources	Extensive data processing and evaluation	Lack of key figures and measurement methods to evaluate cost efficiency
Transparency	Traceability			[16] +			[16] +	[16] +
	Transaction Content Visibility						[16] +	[16] +
	Unidentifiability							
	Node Verification							
Security	Atomicity							
	Authentication							
	Availability		[16] +			[16] +		
	Confidentiality							
	Consistency		[16] +			[16] +		
	Durability							
	Fault Tolerance							
	Integrity							
	Isolation							
	Level of Decentralization					[13, 20] +		
	Node Trust Level							
	Non-Repudiation							
	Reliability							
	Stale Block Rate							
	Strength of Encryption							
Usability	Cost	[3, 12, 16] +						
	Ease of Node Setup							
	Ease of Use							
	Support for Constrained Devices							

DLT Properties	Challenge in Compliance	Lack of awareness and acceptance		Conscious or unconscious misconduct			Conflicts of interest and trust issues between stakeholders			
	DLT Characteristics	Compliance seen as a bureaucratic burden	Ignorance and lack of communication	Deficits in knowledge and errors	Insufficient compliance focus	Preventing deliberate infringement	Diverse interests and goals	Different roles and relevance	Trust issues in distributed working environments	Different opportunities of influence
Community	Development Activity									
	Developer Support	[16] +	[16] +							
	Incentive Mechanisms									
	Network Size									
Flexibility	Interoperability									
	Maintainability									
	Modularity									
	Smart Contract Support	[16] +	[16] +	[16, 24] +	[16] +	[16] +			[24] +	
	Token Purposes									
	Transaction Size Limit									
Law & Regulation	Auditability									
	Censorship Resistance									
	Compliance			[16] +	[16] +					
	Governance Mechanisms	[16] +	[16] +							
	Liability									
Performance	Block Creation Interval									
	Block Size									
	Confirmation Latency									
	History Retention									
	Computational Resources									
	Message Propagation Efficiency									
	Propagation Delay									
	Response Time									
	Scalability									
	Throughput									
	Transaction Validation Latency									

DLT Properties	Challenge in Compliance	Lack of awareness and acceptance		Conscious or unconscious misconduct			Conflicts of interest and trust issues between stakeholders			
	DLT Characteristics	Compliance seen as a bureaucratic burden	Ignorance and lack of communication	Deficits in knowledge and errors	Insufficient compliance focus	Preventing deliberate infringement	Diverse interests and goals	Different roles and relevance	Trust issues in distributed working environments	Different opportunities of influence
Transparency	Traceability			[16] +	[16] +	[16] +			[24] +	
	Transaction Content Visibility			[16] +	[16] +	[16] +	[13] +		[24] +	
	Unidentifiability						[20] +			
	Node Verification									
Security	Atomicity									
	Authentication									
	Availability			[16] +	[16] +	[1, 16] +				
	Confidentiality									
	Consistency									
	Durability									
	Fault Tolerance									
	Integrity					[1, 16] +			[24] +	
	Isolation									
	Level of Decentralization	[16] +	[16] +				[16] +	[16] +	[24] +	[16] +
	Node Trust Level									
	Non-Repudiation									
	Reliability									
	Stale Block Rate									
	Strength of Encryption									
Usability	Cost									
	Ease of Node Setup	[16] +	[16] +							
	Ease of Use	[16] +	[16] +							
	Support for Constrained Devices									

D. Concept Matrix C-2: Risks Through the Use of DLT

DLT Properties	Risks through the use of DLT	Surveillance	Identification of perpetrator	Difficulties to restructure the IT and compliance system			Non - Conformity of DLT with laws and regulations	
	DLT Characteristics	Surveillance and profiling through evaluation of metadata	Anonymity or pseudonymity of perpetrator	Lack of expertise for blockchain technology	Required system modulations	Inconsistency problem, if not all stakeholders participate and all necessary business processes are implemented via the DLT	Immutability of illegal content on the DLT	Non - Compliance with GDPR
Community	Development Activity			[16] +				
	Developer Support			[16] +				
	Incentive Mechanisms							
	Network Size							[7] -
Flexibility	Interoperability				[16] +			
	Maintainability							
	Modularity				[16] +			
	Smart Contract Support							
	Token Purposes							
	Transaction Size Limit							
Law & Regulation	Auditability							
	Censorship Resistance							
	Compliance							[16] +
	Governance Mechanisms							
	Liability							[7] +
Performance	Block Creation Interval							
	Block Size							
	Confirmation Latency							
	History Retention							
	Computational Resources							
	Message Propagation Efficiency							
	Propagation Delay							
	Response Time							
	Scalability							
	Throughput							
	Transaction Validation Latency							

DLT Properties	Risks through the use of DLT	Surveillance	Identification of perpetrator	Difficulties to restructure the IT and compliance system			Non - Conformity of DLT with laws and regulations	
	DLT Characteristics	Surveillance and profiling through evaluation of metadata	Anonymity or pseudonymity of perpetrator	Lack of expertise for blockchain technology	Required system modulations	Inconsistency problem, if not all stakeholders participate and all necessary business processes are implemented via the DLT	Immutability of illegal content on the DLT	Non - Compliance with GDPR
Transparency	Traceability	[14, 16] -						[7] -
	Transaction Content Visibility	[16] -						[7, 9] -
	Unidentifiability	[16] +	[16] -					[7] +
	Node Verification							
Security	Atomicity							
	Authentication							
	Availability							
	Confidentiality							[1] +
	Consistency							
	Durability							[9] -
	Fault Tolerance							
	Integrity						[16] -	[4, 7, 9, 16, 18, 22] -
	Isolation							
	Level of Decentralization							
	Node Trust Level							
	Non-Repudiation							
	Reliability							
	Stale Block Rate							
	Strength of Encryption							
Usability	Cost							
	Ease of Node Setup					[16] +		
	Ease of Use					[16] +		
	Support for Constrained Devices							[7] -

DLT Properties	Risks through the use of DLT	Security problems				
	DLT Characteristics	Hard fork event can compromise the integrity of data	Mathematical or processing power advancements can compromise DLT cryptography retroactively	Difficulties translating rules error-free into Smart Contract program code	Behavior of Smart Contract instances cannot be predicted with certainty	Zero-defect-tolerance of Smart Contracts during execution
Community	Development Activity					
	Developer Support					
	Incentive Mechanisms					
	Network Size					
Flexibility	Interoperability			[10] +	[16] -	
	Maintainability					
	Modularity					
	Smart Contract Support			[10, 16, 20] -	[16] -	[16] -
	Token Purposes					
	Transaction Size Limit					
Law & Regulation	Auditability					
	Censorship Resistance					
	Compliance					
	Governance Mechanisms					
	Liability					
Performance	Block Creation Interval					
	Block Size					
	Confirmation Latency					
	History Retention					
	Computational Resources					
	Message Propagation Efficiency					
	Propagation Delay					
	Response Time					
	Scalability					
	Throughput					
	Transaction Validation Latency					

DLT Properties	Risks through the use of DLT	Security problems				
	DLT Characteristics	Hard fork event can compromise the integrity of data	Mathematical or processing power advancements can compromise DLT cryptography retroactively	Difficulties translating rules error-free into Smart Contract program code	Behavior of Smart Contract instances cannot be predicted with certainty	Zero-defect-tolerance of Smart Contracts during execution
Transparency	Traceability					
	Transaction Content Visibility					
	Unidentifiability					
	Node Verification					
Security	Atomicity					
	Authentication					
	Availability					
	Confidentiality					
	Consistency					
	Durability					
	Fault Tolerance					
	Integrity	[16] -	[16] 0			
	Isolation					
	Level of Decentralization					
	Node Trust Level					
	Non-Repudiation					
	Reliability					
	Stale Block Rate					
	Strength of Encryption		[19] 0			
Usability	Cost					
	Ease of Node Setup					
	Ease of Use					
	Support for Constrained Devices					

DLT Properties	Risks through the use of DLT	Job losses due to automation	IT dependencies	Performance problems	High consumption of resources	
	DLT Characteristics	Automation may lead to the reduction of intermediaries, process steps and a possible loss of jobs	Dominance of the miners	Performance of Peer-to-Peer networks inferior to regular networks	Potentially insufficient storage capacities for the local storage of the DLT copy	High energy wastage
Community	Development Activity					
	Developer Support					
	Incentive Mechanisms					
	Network Size			[16] -		
Flexibility	Interoperability					
	Maintainability					
	Modularity					
	Smart Contract Support	[16] -				
	Token Purposes					
	Transaction Size Limit					
Law & Regulation	Auditability					
	Censorship Resistance					
	Compliance					
	Governance Mechanisms		[16] +			
	Liability					
Performance	Block Creation Interval					
	Block Size					
	Confirmation Latency					
	History Retention					
	Computational Resources				[19] -	[16, 17, 19] -
	Message Propagation Efficiency					
	Propagation Delay					
	Response Time			[16] +		
	Scalability			[16] +		
	Throughput			[16] +		
	Transaction Validation Latency					

DLT Properties	Risks through the use of DLT	Job losses due to automation	IT dependencies	Performance problems	High consumption of resources	
	DLT Characteristics	Automation may lead to the reduction of intermediaries, process steps and a possible loss of jobs	Dominance of the miners	Performance of Peer-to-Peer networks inferior to regular networks	Potentially insufficient storage capacities for the local storage of the DLT copy	High energy wastage
Transparency	Traceability					
	Transaction Content Visibility					
	Unidentifiability					
	Node Verification					
Security	Atomicity					
	Authentication					
	Availability					
	Confidentiality					
	Consistency					
	Durability					
	Fault Tolerance					
	Integrity					
	Isolation					
	Level of Decentralization					
	Node Trust Level					
	Non-Repudiation					
	Reliability					
	Stale Block Rate					
	Strength of Encryption					
Usability	Cost					
	Ease of Node Setup					
	Ease of Use					
	Support for Constrained Devices				[16] +	

E. Concept Matrix C-3: Business Use Cases

	Financial sector					Auditing							
Business Use Case	Automated KYC Checks of Financial Transactions	Distributed KYC Identity Data Processing	Customer Data Privacy Management in Open Banking	Anti-Money Laundering Prevention	Financial Risk Management	Privat Data Sharing and Auditing in Federated Multi-Disciplinary Optimization (MDO)	Auditing and Provenance Tracking of Artificial Intelligence - (Model Training)	Computer-assisted Audit Tools Techniques (CAATTs)	Auditing and Monitoring Compliance of Assets in a CBM	Auditing and Provenance Tracking of Cloud Data	Audit Logs in Online Transaction Processing	Auditing of Software Development	Auditing of (Private) Data Usage
Reference Number													
1								x					
2											x		
3									x				
4													
5													
6													
7													
8	x			x			x						x
9													
10													
11													x
12					x								
13										x			
14		x	x										
15													
16													
17												x	
18		x											
19													
20		x											
21						x							
22													
23	x	x											
24													
25													
26													x
27										x			

	Information Governance of Personal Data										
Business Use Case	GDPR Compliant Information Governance	Blockchain Based Personally Identifiable Information Management System	HIPAA Compliant Information Governance in the Healthcare Industry	GDPR Compliant Information governance in the Healthcare Industry (MyHeathMyData)	Supply Chain Provenance Tracking	Advertising Verification to Avoid Advertising Fraud	Business Process Compliance	Distributed Software Development with Open Source Licenses	Notarizing Files Over the Blockchain Protocol	Critical Infrastructure Protection (CIP) Compliance	Compliance in the Construction and Building Industry
Reference Number											
1											
2											
3											
4		x									
5						x					
6				x							
7											
8					x						
9	x										
10											x
11											
12											
13											
14											
15									x		
16							x				
17										x	
18											
19			x								
20											
21											
22											
23											
24								x			
25											
26					x						
27											

References

Abreu, P. W., Aparicio, M., & Costa, C. J. (2018). Blockchain technology in the auditing environment. In *13th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1–6). Caceres, Spain. https://doi.org/10.23919/CISTI.2018.8399460

Ahmad, A., Saad, M., Bassiouni, M., & Mohaisen, A. (2018). Towards Blockchain-Driven, Secure and Transparent Audit Logs. In H. Schulzrinne (Ed.), *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems Computing, Networking and Services* (pp. 443–448). New York NY. https://doi.org/10.1145/3286978.3286985

Akerlof, G. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500. https://doi.org/10.2307/1879431

Al Khalil, F., Butler, T., O'Brien, L., & Ceci, M. (2017). Trust in Smart Contracts is a Process, As Well. In M. Brenner (Ed.), *Lecture Notes in Computer Science: Vol. 10323. Financial cryptography and data security* (pp. 510–519). Sliema, Malta. https://doi.org/10.1007/978-3-319-70278-0_32

Alexandris, G., Katos, V., Alexaki, S., & Hatzivasilis, G. (2018). Blockchains as Enablers for Auditing Cooperative Circular Economy Networks. In *2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1–7). Piscataway, NJ. https://doi.org/10.1109/CAMAD.2018.8514985

Al-Zaben, N., Hassan Onik, M. M., Yang, J., Lee, N. Y., & Kim, C. S. (2018). General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management. In M. H. Miraz (Ed.), *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* (pp. 77–82). Piscataway, NJ. https://doi.org/10.1109/iCCECOME.2018.8658586

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. de, . . . Yellick, J. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference* (pp. 1–15). New York, NY. https://doi.org/10.1145/3190508.3190538

Anjum, A., Sporny, M., & Sill, A. (2017). Blockchain Standards for Compliance and Trust. *IEEE Cloud Computing*, *4*(4), 84–90. https://doi.org/10.1109/MCC.2017.3791019

Ateniese, G., Magri, B., Venturi, D., & Andrade, E. (2017). Redactable Blockchain – or – Rewriting History in Bitcoin and Friends. In *2nd IEEE European Symposium on Security and Privacy* (pp. 111–126). Paris, France. https://doi.org/10.1109/EuroSP.2017.37

Axon, L., Goldsmith, M., & Creese, S. (2018). Privacy Requirements in Cybersecurity Applications of Blockchain. In P. Raj & G. C. Deka (Eds.), *Advances in Computers: Blockchain Technology: Platforms, Tools and Use Cases* (Vol. 111, pp. 229–278). https://doi.org/10.1016/bs.adcom.2018.03.004

Bayle, A., Koscina, M., Manset, D., & Perez-Kempner, O. (2018). When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry. In *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)* (pp. 788–792). Santiago, Chile. https://doi.org/10.1109/WI.2018.00133

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A Hermeneutic Approach for Conducting Literature Reviews and Literature Searches. *Communications of the Association for Information Systems*, *34*(12), 257–286. https://doi.org/10.17705/1CAIS.03412

Buocz, T., Ehrke-Rabel, T., Hödl, E., & Eisenberger, I. (2019). Bitcoin and the GDPR: Allocating responsibility in distributed networks. *Computer Law & Security Review*, *35*(2), 182–198. https://doi.org/10.1016/j.clsr.2018.12.003

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Dillenberger, D., Novotny, P., Zhang, Q., Jayachandran, P., Gupta, H., Mehta, S., . . . Verma, D. (2019). Blockchain Analytics and Artificial Intelligence. *IBM Journal of Research and Development*, 1–13. https://doi.org/10.1147/JRD.2019.2900638

Drescher, D. (2017). *Blockchain Basics*. Berkeley, CA. https://doi.org/10.1007/978-1-4842-2604-9

English, S., & Hammond, S. (2018). Cost of Compliance 2018. Retrieved from https://legal.thomsonreuters.com/en/insights/reports/cost-of-compliance-2018

Fdhila, W., Rinderle-Ma, S., Knuplesch, D., & Reichert, M. (2015). Change and Compliance in Collaborative Processes. In P. P. Maglio (Ed.), *2015 IEEE International Conference on Services Computing (SCC)* (pp. 162–169). New York, NY. https://doi.org/10.1109/SCC.2015.31

Frantz, C. K., & Nowostawski, M. (2016). From Institutions to Code: Towards Automated Generation of Smart Contracts. In S. Elnikety, P. R. Lewis, & C. Müller-Schloer (Eds.), *Ieee 1st international workshops on Foundations and Applications of Self-* Systems* (pp. 210–215). Piscataway, NJ. https://doi.org/10.1109/FAS-W.2016.53

General Data Protection Regulation. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. In *Official Journal of the European Union* (pp. 1–88). Retrieved from http://data.europa.eu/eli/reg/2016/679/oj

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* (pp. 1543–1552). Manoa, Hawaii. https://doi.org/10.24251/HICSS.2017.186

Hofman, D., Lemieux, V. L., Joo, A., & Batista, D. A. (2019). “The margin between the edge of the world and infinite possibility”. *Records Management Journal*, *29*(1), 240–257. https://doi.org/10.1108/RMJ-12-2018-0045

Jeyaraj, A., Rottman, J. W., & Lacity, M. C. (2006). A Review of the Predictors, Linkages, and Biases in IT Innovation Adoption Research. *Journal of Information Technology*, *21*(1), 1–23. https://doi.org/10.1057/palgrave.jit.2000056

JPMorgan Chase (2018). Quorum Whitepaper v0.2. Retrieved from https://github.com/jpmorganchase/quorum/blob/master/docs/Quorum%20Whitepaper%20v0.2.pdf

Kaaniche, N., & Laurent, M. (2017). A blockchain-based data usage auditing architecture with enhanced privacy and availability. In A. Gkoulalas-Divanis, M. Correira, & D. R. Avresky (Eds.), *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)* (pp. 1–5). Cambridge, MA. https://doi.org/10.1109/NCA.2017.8171384

Kannengießer, N., Lins, S., Dehling, T., & Sunyaev, A. (2019a). What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs. In T. Bui (Ed.), *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 7069–7078). Manoa, Hawaii. https://doi.org/10.24251/HICSS.2019.848

Kannengießer, N., Lins, S., Dehling, T., & Sunyaev, A. (2019b, June 3). *Mind the Gap: Trade-Offs between Distributed Ledger Technology Characteristics*. Retrieved from http://arxiv.org/pdf/1906.00861v1

Kavassalis, P., Stieber, H., Breymann, W., Saxton, K., & Gross, F. J. (2018). An innovative RegTech approach to financial risk monitoring and supervisory reporting. *The Journal of Risk Finance*, *19*(1), 39–55. https://doi.org/10.1108/JRF-07-2017-0111

Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., & Thompson, C. (2017). A Distributed-Ledger Consortium Model for Collaborative Innovation. *Computer*, *50*(9), 29–37. https://doi.org/10.1109/MC.2017.3571057

Knuplesch, D., Reichert, M., Fdhila, W., & Rinderle-Ma, S. (2013). On Enabling Compliance of Cross-Organizational Business Processes. In F. Daniel, J. Wang, & B. Weber (Eds.), *Lecture Notes in Computer Science / Information Systems and Applications: Vol. 8094. Business Process Management* (pp. 146–154). Berlin/Heidelberg, Germany. https://doi.org/10.1007/978-3-642-40176-3_12

Kühnel, S. (2017). Toward Cost-Effective Business Process Compliance. In M. Eibl & M. Gaedke (Eds.), *Informatik 2017: Chemnitz, Deutschland* (pp. 2379–2384). https://doi.org/10.18420/in2017_242

Lacity, M. C., Khan, S., Yan, A., & Willcocks, L. P. (2010). A review of the IT outsourcing empirical literature and future research directions. *Journal of Information Technology*, *25*(4), 395–433. https://doi.org/10.1057/jit.2010.21

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 382–401. https://doi.org/10.1145/357172.357176

Li, J., Greenwood, D., & Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. *Automation in Construction*, *102*, 288–307. https://doi.org/10.1016/j.autcon.2019.02.005

Li, W., Sforzin, A., Fedorov, S., & Karame, G. O. (2017). Towards Scalable and Private Industrial Blockchains. In S. Lokam (Ed.), *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts* (pp. 9–14). New York, NY. https://doi.org/10.1145/3055518.3055531

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Provchain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing* (pp. 468–477). Madrid, Spain. https://doi.org/10.1109/CCGRID.2017.8

Lins, S., & Sunyaev, A. (2017). Unblackboxing IT certifications: A theoretical model explaining IT certification effectiveness. In *International Conference on Information Systems (ICIS)* (pp. 1–13). Retrieved from https://aisel.aisnet.org/icis2017/Security/Presentations/26/

The Linux Foundation (2018). Hyperledger Architecture, Volume II: Smart Contracts. Retrieved from https://www.hyperledger.org/resources/publications

Ma, S., Guo, C., Wang, H. [Hao], Xiao, H., Xu, B., Dai, H. N. [Hong-Ning], . . . Wang, T. (2018). Nudging Data Privacy Management of Open Banking Based on Blockchain. In *2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN)* (pp. 72–79). Yichang, China. https://doi.org/10.1109/I-SPAN.2018.00021

Magrahi, H., Omrane, N., Senot, O., & Jaziri, R. (2018). Nfb: A Protocol for Notarizing Files over the Blockchain. In *2018 9th IFIP International Conference on New Technologies, Mobility & Security* (pp. 1–4). Paris, France. https://doi.org/10.1109/NTMS.2018.8328740

Meironke, A., Seyffarth, T., & Damarowsky, J. (2019). Business Process Compliance and Blockchain: How Does the Ethereum Blockchain Address Challenges of Business Process Compliance? In T. Ludwig (Ed.), *14. Internationale Tagung Wirtschaftsinformatik: Human Practice. Digital Ecologies. Our Future.* (pp. 1894–1905). Siegen, Germany. Retrieved from https://www.researchgate.net/publication/331398949_Business_Process_Compliance_and_Blockchain_How_Does_the_Ethereum_Blockchain_Address_Challenges_of_Business_Process_Compliance

Merkle, R. C. (1990). A Certified Digital Signature. In G. Brassard (Ed.), *Lecture Notes in Computer Science: Vol. 435. Advances in cryptology - CRYPTO '89: Proceedings* (pp. 218–238). New York NY. https://doi.org/10.1007/0-387-34805-0_21

Molina-Jimenez, C., Sfyrakis, I., Solaiman, E., Ng, I., Weng Wong, M., Chun, A., & Crowcroft, J. (2018). Implementation of Smart Contracts Using Hybrid Architectures with On and Off–Blockchain Components. In *8th IEEE International Symposium on Cloud and Service Computing* (pp. 83–90). Paris, France. https://doi.org/10.1109/SC2.2018.00018

Mylrea, M., & Gourisetti, S. N. G. (2018). Blockchain for Supply Chain Cybersecurity, Optimization and Compliance. In *2018 Resilience Week (RWS)* (pp. 70–76). Denver, CO. https://doi.org/10.1109/RWEEK.2018.8473517

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Norvill, R., Steichen, M., Shbair, W. M., & State, R. (2019). Demo: Blockchain for the Simplification and Automation of KYC Result Sharing. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 9–10). Seoul, South Korea. https://doi.org/10.1109/BLOC.2019.8751480

Parra Moyano, J., & Ross, O. (2017). KYC Optimization Using Distributed Ledger Technology. *Business & Information Systems Engineering*, *59*(6), 411–423. https://doi.org/10.1007/s12599-017-0504-2

Pass, R., & Shi, E. (2017). The Sleepy Model of Consensus. In T. Takagi & T. Peyrin (Eds.), *Lecture Notes in Computer Science: Vol. 10625. Advances in cryptology - ASIACRYPT 2017* (pp. 380–409). Cham. https://doi.org/10.1007/978-3-319-70697-9_14

Pilkington, M. (2016). Blockchain technology: Principles and applications. In F.-J. Olleros & M. Zhegu (Eds.), *Research handbooks in business and management series. Research handbook on digital transformations* (pp. 225–253). Cheltenham, UK, Northampton, MA. https://doi.org/10.4337/9781784717766.00019

Reniers, V., van Landuyt, D., Viviani, P., Lagaisse, B., Lombardi, R., & Joosen, W. (2019). Analysis of architectural variants for auditable blockchain-based private data sharing. In C.-C. Hung & G. A. Papadopoulos (Eds.), *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing - SAC '19* (pp. 346–354). Limassol, Cyprus. https://doi.org/10.1145/3297280.3297316

Sadiq, S. (2011). A Roadmap for Research in Business Process Compliance. In W. Abramowicz, L. Maciaszek, & K. W cel (Eds.), *Lecture Notes in Business Information Processing: Vol. 97. Business Information Systems Workshops* (pp. 1–4). Berlin/Heidelberg, Germany. https://doi.org/10.1007/978-3-642-25370-6_1

Sadiq, S., & Governatori, G. (2015). Managing Regulatory Compliance in Business Processes. In J. vom Brocke & M. Rosemann (Eds.), *International Handbooks on Information Systems. Handbook on Business Process Management 2* (2nd ed., pp. 265–288). Berlin/Heidelberg, Germany. https://doi.org/10.1007/978-3-642-45103-4_11

Sadiq, S., Governatori, G., & Namiri, K. (2007). Modeling Control Objectives for Business Process Compliance. In G. Alonso, P. Dadam, & M. Rosemann (Eds.), *Lecture Notes in Computer Science: Vol. 4714. Business process management* (pp. 149–164). Berlin, Germany. https://doi.org/10.1007/978-3-540-75183-0_12

Saito, K., & Yamada, H. (2016). What's So Different about Blockchain? — Blockchain is a Probabilistic State Machine. In *2016 IEEE 36th International Conference on Distributed Computing Systems workshops - ICDCSW 2016* (pp. 168–175). Nara, Japan. https://doi.org/10.1109/ICDCSW.2016.28

Schäfer, T., Fettke, P., & Loos, P. (2012). Towards an Integration of GRC and BPM – Requirements Changes for Compliance Management Caused by Externally Induced Complexity Drivers. In F. Daniel, K. Barkaoui, & S. Dustdar (Eds.), *Lecture Notes in Business Information Processing: Vol. 100. Business Process Management Workshops* (pp. 344–355). Berlin/Heidelberg, Germany. https://doi.org/10.1007/978-3-642-28115-0_33

Schmelz, D., Fischer, G., Niemeier, P., Zhu, L., & Grechenig, T. (2018). Towards Using Public Blockchain in Information-Centric Networks: Challenges Imposed by the European Union's General Data Protection Regulation. In L. Kai (Ed.), *Proceedings of 2018 1st IEEE International Conference on Hot Information-Centric Networking* (pp. 223–228). Shenzhen, China. https://doi.org/10.1109/HOTICN.2018.8606000

Shaw, M. L.G., & Gaines, B. R. (1989). Comparing conceptual structures: consensus, conflict, correspondence and contrast. *Knowledge Acquisition*, *1*(4), 341–363. https://doi.org/10.1016/S1042-8143(89)80010-X

Shbair, W. M., Steichen, M., Francois, J., & State, R. (2018). Blockchain orchestration and experimentation framework: A case study of KYC. In *Cognitive management in a cyber world* (pp. 1–6). Taipei, Taiwan. https://doi.org/10.1109/NOMS.2018.8406327

Singi, K., S, P. D., Kaulgud, V., & Podder, S. (2018). Compliance adherence in distributed software delivery. In M. Paasivaara, D. Šmite, & R. Evaristo (Eds.), *Proceedings of the 13th Conference on Global Software Engineering - ICGSE '18* (pp. 131–132). Gothenburg, Sweden. https://doi.org/10.1145/3196369.3196383

Suciu, G., Nadrag, C., Istrate, C., Vulpe, A., Ditu, M. C., & Subea, O. (2018). Comparative Analysis of Distributed Ledger Technologies. In *The 6th Global Wireless Summit (GWS-2018)* (pp. 370–373). Chiang Rai, Thailand. https://doi.org/10.1109/GWS.2018.8686563

Turetken, O., Elgammal, A., van den Heuvel, W. J., & Papazoglou, M. (2011). Enforcing compliance on business processes through the use of patterns. In *European Conference on Information Systems (ECIS) 2011 Proceedings 5.* (pp. 1–14). Retrieved from https://aisel.aisnet.org/ecis2011/5/

Wohlgemuth, S., Umezawa, K., Mishina, Y., & Takaragi, K. (2019). Competitive Compliance with Blockchain. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops* (pp. 967–972). Kyoto, Japan. https://doi.org/10.1109/PERCOMW.2019.8730684

Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J.P.C., & Ko, K. (2018). Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. *IEEE Access*. (6), 1513–1524. https://doi.org/10.1109/ACCESS.2017.2779263

Yu, H., & Yang, Z. (2018). Decentralized and Smart Public Auditing for Cloud Storage. In *Proceedings, 2018 IEEE 9th International Conference on Software Engineering and Service Science* (pp. 491–494). Beijing, China. https://doi.org/10.1109/ICSESS.2018.8663780

Zhang, K., & Jacobsen, H. A. (2018). Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains. In *2018 IEEE 38th International Conference on Distributed Computing Systems* (pp. 1337–1346). Vienna, Austria. https://doi.org/10.1109/ICDCS.2018.00134

Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2017). Metrics for assessing blockchain-based healthcare decentralized apps. In *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)* (pp. 1–4). Dalian, China. https://doi.org/10.1109/HealthCom.2017.8210842

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, *2*(1), 1–7. https://doi.org/10.1186/s40854-016-0049-2

Zheng, Z., Xie, S., Dai, H. [Hongning], Chen, X., & Wang, H. [Huaimin]. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In G. Karypis & J. Zhang (Eds.), *2017 IEEE International Congress on Big Data - BigData Congress 2017* (pp. 557–564). Honolulu, HI. https://doi.org/10.1109/BigDataCongress.2017.85

Declaration about the Thesis

Ich versichere wahrheitsgemäß, die Arbeit selbstständig verfasst, alle benutzten Hilfsmittel vollständig und genau angegeben und alles kenntlich gemacht zu haben, was aus Arbeiten anderer unverändert oder mit Abänderungen entnommen wurde sowie die Satzung des KIT zur Sicherung guter wissenschaftlicher Praxis in der jeweils gültigen Fassung beachtet zu haben.

_____

Karlsruhe, den 30. Oktober 2019 VORNAME NACHNAME