Business Process Compliance and Blockchain: How Does the Ethereum Blockchain Address Challenges of Business Process Compliance?

Anja Meironke[1], Tobias Seyffarth[1], and Johannes Damarowsky[1]

[1]Martin Luther University Halle-Wittenberg, Chair of Information Management, Halle (Saale), Germany
{anjameironke}@gmail.com
{tobias.seyffarth, johannes.damarowsky}@wiwi.uni-halle.de

Abstract. Second generation blockchain technologies such as Ethereum can be used not only for financial transactions but also for cross-organizational processes, for applications in the pharmaceutical industry and even in the field of Business Process Compliance (BPC). However, there are many challenges in the field of BPC. Thus, we raised the following research question: How does the Ethereum blockchain address challenges of BPC? To answer this question, we conducted a structured literature review to identify challenges in BPC as well as features of the Ethereum blockchain that may solve the selected BPC challenges. As a result, we identified 21 BPC challenges and categorized these into legal, organizational, human-centered, technical and economic challenges. We found that the technical and organizational BPC challenges were those that Ethereum could best solve, while human-centered challenges could be less well addressed. Furthermore, the implementation of the Ethereum blockchain leads to additional challenges, such as the immutability of illegal content within the Ethereum blockchain or the error-proneness and zero-defect tolerance of smart contracts.

Keywords: Blockchain, Ethereum, Business Process Compliance, Challenges

1 Introduction

In the time of digital innovation, advanced technologies are emerging and changing the way business is done, especially business between organizations. One of the recent technologies which is said to be disruptive in nature is blockchain [1–3]. Currently, the most prominent blockchain technology is Bitcoin, due to its correlated and identically named cryptocurrency [2, 4]. However, modern blockchain deployments such as Ethereum provide even more elaborate functionalities and, therefore, have also gained attention. Ethereum reaches beyond digital currencies, enabling applications in cross-organizational business processes, logistics and pharma [5–7]. Another potential area of application is in Business Process Compliance (BPC), which denotes the execution of business processes in adherence to compliance requirements such as laws or contracts [8]. However, there are various challenges within BPC such as the complexity

14th International Conference on Wirtschaftsinformatik,
February 24-27, 2019, Siegen, Germany

of business and compliance processes, the high administrative efforts required to ensure compliance in business processes and the lack of automation and standardization to adequately support BPC [9, 10]. Whereas research and earlier blockchain applications mainly concentrated on financial applications and use cases in the field of cross-organizational business process execution [6, 7, 11], further applications are of interest as well. Therefore, our goal is to answer the following research question: *How does the Ethereum blockchain address challenges of BPC?*

The remainder of this paper is organized as follows. In Section 2, we describe the applied methodology to answer our research question. In Section 3, we briefly highlight the technological underpinnings of the blockchain deployment Ethereum and its main features. Section 4 provides an overview of the major challenges within the field of BPC. In Section 5, we map the features of Ethereum to the different BPC challenges and discuss the potential of the findings derived. Finally, Section 6 concludes the paper.

2 Methodology

We performed a three-step approach to answer our research question. First, we worked out the features of the Ethereum blockchain. Second, we identified challenges in the field of BPC, which were then mapped to the Ethereum features in the third step.
We conducted a literature review according to vom Brocke et al. [12] to identify relevant literature for each step. Table 1 shows the applied search terms within each database, the initial hits and the numbers of selected and relevant papers.

Table 1. Literature search

Step	Search term	Database	Hits	Selected	Relevant
1	ethereum AND (functionality OR "mode of operation" OR "way of functioning")	Google Scholar	211	6	5
2	("business process compliance" OR BPC) AND (challenge OR lifecycle)	Google Scholar	Aborted after 610	80	17
	"Business Process Compliance" challenge	KVK	104	12	12
3	("business process compliance" OR BPC") AND (blockchain OR ethereum)	Google Scholar	38	9	1
	“business process compliance” ethereum	KVK	36	28	17
Backward search					19
Sum					71

The literature search was performed using Google Scholar and Karlsruher Virtueller Katalog (KVK), which includes the following databases: GBV, SWB, BVB, HBZ, HEBIS, KOBV, DNB, StaBi Berlin and Worldcat. In Google Scholar we searched within the general search field, while we used the keyword search within KVK, which only allowed restricted search strings and no connectors. The initial hits were selected

based on their titles and abstracts. In the next step, the papers' abstracts and several papers in full were read to identify relevant publications. We also conducted a backward search, which led to 71 relevant papers that were considered to help answer the research question.

3 Fundamentals of Blockchain and Ethereum

Blockchain is the technology that supports Ethereum [4]. The Ethereum blockchain is a public and distributed ledger, which stores all of the transactions occurring within the Ethereum network. Transactions are processed between different accounts. Every party of the blockchain network can create any number of accounts without restrictions and third party authentications. The creation of accounts and the authorization of transactions are based on asymmetric cryptographic mechanisms. When creating an account, a public and a private key are generated whereby the account address is derived from the public key, which guarantees a certain degree of anonymity. The sender authorizes the transaction using the account's private key. Processed transactions are visible to every party of the network. Due to the implemented consensus mechanism, the blockchain technology is tamper-proof, without any need for a trusted third party (e.g. a bank or a notary) to avoid double spending.

One consensus mechanism is proof-of-work (PoW), whereby so-called miners have to solve a puzzle using cryptographic methods. Next, new transactions are published in the blockchain network and are approved by the miners. Miners summarize a number of transactions to blocks, validate their signature and the transaction nonce and check that the sender's account balance covers the amount, including the fees to execute the transaction. Then a hash is computed over the current and previous block of transactions and their metadata. A valid hash must correspond to a certain pattern (for example, in the case of Ethereum, the hash must be below a certain threshold). In order to achieve this, a nonce is added as a further input of the hash function. It is not possible to simply compute this nonce. Nonces have to be tested randomly. After finding a matching nonce, the blocks are chained together to form a blockchain. Finally, the miner who first finds a valid nonce is awarded with an amount of new crypto-coins and all transactions fees of the respective block. Based on chaining blocks by means of their computed hash values, a manipulation can be easily detected by recalculating the hashes of two linked blocks and their nonce.

Additionally, there are further design parameters for blockchain solutions. Blockchains can be differentiated between public and private and between permission-less and permissioned blockchains. In a public blockchain, everyone can be part of the blockchain network, whereas private blockchain access is only granted to dedicated participants. Within a permission-less network, everyone can approve new blocks, while in a permissioned network only certain parties are allowed to [13]. By default, Ethereum represents a public, permission-less blockchain [5].

Finally, two generations of blockchains are discussed in the literature. The first generation of blockchain is able to transfer tokens (e.g. Bitcoins) between nodes. The second generation, to which Ethereum belongs, allows more elaborate bytecode to run

on top of the blockchain, which is denoted as so-called smart contracts. A smart contract is a user-defined program executed within the blockchain network [14]. In Ethereum, smart contracts are written in Solidity and executed within its execution environment, the Ethereum Virtual Machine. They can be executed automatically and allow a flexible adaption of the blockchain technology to other fields of application [5]. Based on the five technical underpinnings explained above, we derived fourteen main features of Ethereum in Figure 1.

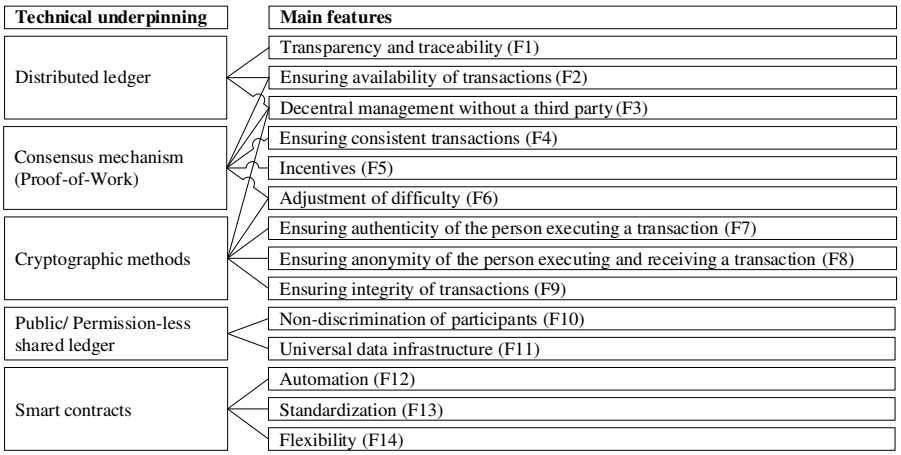

Figure 1. Technical underpinnings and main features of the Ethereum blockchain

4 Challenges in Business Process Compliance

The successful management of BPC is associated with various challenges. We classified these challenges into groups, including legal, organizational, human-centered, technical and economic challenges. Table 2 shows an excerpt of the concept matrix. The entire concept matrix can be found at: `https://bit.ly/2A3O35O`.

Table 2. Concept matrix of BPC challenges (H: Human-centered | T: Technical)

		[15]	[16]	[17]	…
H	Lack of awareness and acceptance (C_H 1)	x	x		
	Conscious or unconscious misconduct (C_H 2)		x		
	…				
T	Technical support and automation of BPC (C_T 1)		x		
	Complex IT architecture and low system integration (C_T 2)		x		
	Proprietary service providers and centralized services (C_T 3)		x		
	Data security and data privacy (C_T 4)			x	
…	…				

Legal challenges include the complexity of the compliance requirements that must be taken into account [8, 10]. A compliance requirement is an assertion resulting from the interpretation of compliance sources, such as laws, norms, standards or internal

policies [18]. Compliance requirements change rapidly, which requires a continuous adaptation of related business processes [9, 19]. Moreover, the vagueness of compliance requirements and differing interpretations by the stakeholders make it difficult to interpret compliance requirements unambiguously [15, 20].

Further, organizations are often confronted with **organizational challenges**. In addition to different organizational structures, the complexity and multitude of business and compliance processes can turn BPC management into a difficult task [9, 10]. Organizations cooperate and interact on an increasingly global level [21]. Therefore, not only must internal business processes be checked for compliance, but entire cross-organizational business processes of the involved partner organizations must also be checked [21, 22]. In these cases, BPC management is difficult and time-consuming, especially because different legislation may be applicable for each country and the stakeholders involved may pursue different objectives. Often there is a problem of trust concerning the exchange of information between different organizations [13, 22–24]. Further organizational BPC challenges comprise the modelling and verification of compliance rules and their integration into the corresponding business processes [25]. Additional organizational challenges include the monitoring of compliance requirements and their operationalization in business processes, for example through compliance processes [19], the associated documentation of compliance process execution and verification, as well as adequate transparency and traceability. Business processes and their instances must be checked for compliance during and after runtime by either external auditors or internal evaluations by means of reports or log files [17, 25, 26]. For this purpose, documented evidence must be tamper-proof, available and easily accessible to the parties involved [13, 16]. In addition, the traceability of compliance requirements back to their relevant business process models and vice versa is often inadequately designed, meaning changes of compliance requirements and business processes cannot be implemented adequately, due to a lack of referential clarity [16].

Closely linked to organizational challenges are **human-centered challenges**. The lack of stakeholder acceptance and awareness, combined with insufficient communication and awareness measures on the part of management, impede the successful implementation of necessary BPC measures. Moreover, a successful BPC is limited by either conscious or unconscious misconduct due to deficiencies in knowledge or by the deliberate violation of compliance requirements resulting from malicious intent, a lack of motivation or fear [16].

Technical challenges generally reside in the low level of automation. There are often manually performed BPC tasks, such as the modeling of compliant business processes and the verification and monitoring of business processes according to their compliance requirements, which are not only time-consuming but also error-prone [9, 10, 13, 16, 27]. Moreover, not all tasks within the BPC management lifecycle [28] can be automated; for example the generation of compliance requirements deduced from different compliance sources requires a broad understanding and complex, strategic thinking [16]. Additionally, the management of information technology (IT) architectures is also challenging because these are usually heterogeneous, distributed, isolated and mutually incompatible [15]. Therefore, the integration of common tools to

support BPC across several organizations and the reduction of parallel IT systems, as well as redundant and inconsistent data fragments, is a challenging task [29]. Above all, the implementation of tools to support BPC often leads to dependence on the corresponding service provider in terms of financial aspects, data security and data privacy [16]. Moreover, sensitive data of an organization is to be treated confidentially and therefore must be protected against unauthorized access and manipulation [13, 17, 24]. Additionally, a service provider may become a single-point-of-failure, if used as the sole provider for data processing [27]. At the same time, successful BPC management must be able to provide information at all times and therefore requires consistent information that is available and documented in a comprehensible manner [30]. Consequently, the simultaneous protection of privacy and availability of BPC-relevant information are often conflicting objectives [16, 17].

Economic challenges include, among other things, a lack of cost and resource efficiency. Companies and organizations have to face increased compliance, IT and staff-related expenses for the management, evaluation and adjustment of complex compliance requirements and business processes or as a result of legal claims for damages due to uncovered compliance violations [8, 21, 31]. Additionally, due to redundant processes, inconsistent data and a low degree of automation, BPC tasks are often inefficient and time consuming [10, 13]. The lack of adequate methods and indicators to analyze the efficiency and effectiveness of BPC so as to assess their cost-benefit ratio constitutes another difficulty [16, 31]. Finally, poor standardization as well as the ad hoc-oriented tasks of the BPC lifecycle make it difficult to optimize business and compliance processes or to react appropriately to compliance deviations [16].

5 How Does Ethereum Address BPC Challenges?

In the previous sections, we focused on the technical underpinnings and main features of Ethereum and on the identified BPC challenges. In the upcoming section, we answer the research question by explaining how Ethereum can potentially address these BPC challenges. For this purpose, the main features of Ethereum were mapped to the identified BPC challenges. The classification of the results is based on our own assessment and the findings of the literature analysis. Table 3 shows an excerpt of our classification. The complete classification including a short explanation and literature references can be found at: `https://bit.ly/2ygavHk`.

Table 3. Classification of Ethereum features referred to BPC challenges (excerpt)

	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14
C_H 1			x									x	x	x
C_H 2	x	x						x	x			x	x	
…														
C_T 1	x											x		x
C_T 2	x		x	x						x	x			x
C_T 3		x	x						x		x			
C_T 4	x	x	x		x		x	x	x					
…														

In terms of **legal BPC challenges**, there is low potential for improvement by the features of Ethereum. According to [32], it is conceivable to store compliance requirements, such as laws and standards, as independent objects of a smart contract within the Ethereum blockchain to make them tamper-proof and publicly accessible. Thus, compliance and business process managers can be informed automatically if changes in the status of a referred requirement occur.

Ethereum offers promising opportunities to address **organizational BPC challenges**, such as the modeling of business processes according to their compliance requirements and the monitoring of compliance requirements and verifying their documentation, transparency and traceability. The decentralized and distributed structure of the Ethereum blockchain supports the streamlining of business and compliance processes, especially with regard to cross-organizational business processes. Accordingly, certain organizational units or trusted third parties that are in charge of monitoring BPC can be omitted (e.g. the central banks for foreign transfers), since transactions may be carried out directly between the transaction partners [7, 33]. Using the Ethereum blockchain as a universal data infrastructure for accessing and coordinating shared data and processes between different stakeholders also reduces data traffic and complex procedures necessary for reconciling, managing and controlling data and processes [34, 35]. In addition, Ethereum contributes to the modelling and verification of compliance rules and their integration into business processes. Logics and rules associated with business and compliance processes can be expressed and automatically checked with the help of smart contracts. However, business and compliance processes as well as their associated rules cannot always be translated seamlessly from natural language into program code [36]. Additionally, due to the overly domain-specific expertise of programmers or legal experts, smart contracts may be programmed inaccurately and might not reflect the underlying rules and process models as intended [36, 37].

Besides supporting BPC-modelling, Ethereum also offers various options for monitoring, verification and transparent documentation within the context of BPC. With the help of smart contracts, a large part of BPC tasks like monitoring and verification can be automated and outsourced to Ethereum, thus reducing manual effort and various process activities [1, 11, 13]. Applying an if-then pattern, smart contracts also automatically enforce compliance with defined rules, with the result that violations cannot occur in the first place, making a permanent monitoring unnecessary. An illustrative example would be a locked leased car that can only be opened by means of a digital key after payment was made [33].

Additionally, the connection to or general accessibility of the blockchain as a public and shared ledger enables extended transparency towards internal and external compliance units and supervisory authorities [7]. Transactions that are documented in the Ethereum blockchain in a verifiable and tamper-proof manner can be verified by internal and external auditors and legislators [2, 13, 17, 38]. In addition, specific verifiable documents and records (e.g. certificates, contracts) or material assets (for example motor vehicles, land) can be stored as digital assets. If their status changes, for example in the case of value transfers and changes of ownership, changes can be documented in a tamper-proof way [7, 11, 13, 39].

However, relevant process participants, such as supervisory authorities or employees, have to be an integral part of the Ethereum network to provide access to information on

transactions [33, 37]. Moreover, illegal contents (e.g. child pornography or unauthorized personal data) are also problematic, since they cannot be simply removed from the blockchain and therefore risk making the entire blockchain illegal [3].

In contrast to the organizational aspects mentioned above, Ethereum has a moderate potential for solving **human-centered BPC challenges**. Ethereum shows potential in terms of reducing conscious (e.g. fraud and deliberate disregard of rules) or unconscious (e.g. lack of knowledge) misconduct. On the one hand, knowledge deficits, errors or deviations can be diminished by mapping compliance requirements, compliance processes or entire business processes as smart contracts for (partial) automation so that they are prevented from circumvention [33, 37, 38]. On the other hand, the manipulation of transaction data causes high costs due to the enormous computing effort necessary to find a valid nonce. Furthermore, fraud and erroneous practices are immediately recognizable due to real-time transaction processing and transparent documentation in the public ledger, so that problems like payment defaults or insurance fraud can be avoided [1, 7, 37].

Ethereum also contributes significantly to addressing **technical BPC challenges**. This particularly concerns aspects of automation, IT architecture, data security and data privacy. As already mentioned, entire business and compliance processes can be (partially) automated with the help of smart contracts [3, 33, 37, 39]. When defined events act as triggers or when pre-defined conditions are met, the smart contract code is validated and executed by the miner according to if-then patterns and, finally, documented in the Ethereum blockchain [32, 36, 38, 40]. However, with regard to deviations from defined rules or algorithms during execution, [33] considers the zero-defect tolerance of smart contracts to be problematic. What happens, for example, in terms of a package delivery, if the order is delivered later than stipulated in the smart contract, but has nevertheless been delivered?

In addition, the Ethereum blockchain can be used as a universal infrastructure to connect and coordinate different stakeholders and organizations, which is often a serious challenge, especially with regard to the modeling, verification and monitoring of compliant business processes within BPC [11, 13, 33]. Redundant and non-compliant business processes and data management may be reduced, as the same business processes and data basis can be used equally by the parties involved [10, 13, 33]. The question that arises at this point is to what extent a public blockchain is suitable for making (partly) sensitive data from cross-organizational business processes generally accessible and public [33].

Nevertheless, with regard to aspects of data security, Ethereum has a particularly high potential due to its inherent properties. In contrast to client-server architectures, the decentralized structure of the Ethereum blockchain and its redundant data distribution ensure a high degree of reliability [7, 33]. If a party of the blockchain network fails due to technical faults or manipulation, all other parties have a local copy, ensuring that the data remains available [2]. Moreover, Ethereum offers an additional security mechanism by charging transaction fees for code execution, which ensures that transactions are reversed when their limit is exceeded. Thus, failures due to maliciously built-in loops causing a program code to run infinitely are prevented [40].

The most important feature of the Ethereum blockchain is the guarantee of integrity by means of cryptographic hashing and linking of the data blocks, as described in

Section 3. Due to high energy costs incurred for recalculation, attacks would be unprofitable for attackers [1, 2]. In addition, manipulated data and attempted fraud would be detectable not only in the context of consensus checks, but also after publishing the data in the Ethereum blockchain [24, 33, 39]. Furthermore, the authenticity and anonymity of the transaction participants can be guaranteed by the use of digital signatures and anonymous account addresses (see Section 3). [1, 10, 13, 39].

According to [41], however, there are vulnerabilities regarding long-term data security. Due to improved computing power and mathematical advances, it is doubtful whether current cryptographic hash methods will maintain their current security level in the foreseeable future. Then the data within Ethereum could be compromised retroactively [23]. Besides, users do not know where their data is stored or to what extent it is processed [42].

Finally, Ethereum offers potential approaches for the solution of **economic BPC challenges,** such as suboptimal cost and resource efficiency, measurability and standardization. Thus, the automation of compliance processes and business processes and their streamlining, by eliminating unnecessary process activities and intermediaries, enables a better cost and resource efficiency, especially on a cross-organizational level [6, 7, 11]. Cost and resource efficiency benefits can also be realized using the Ethereum blockchain as a universal data infrastructure for managing shared data, since multiple data checking by the individual transaction units might become obsolete. This can reduce inconsistent, redundant information as well as the associated work effort, since the Ethereum blockchain is turned into a single-point-of-truth [2, 32, 33].

Interesting approaches also arise in terms of the measurability of BPC efficiency and effectiveness. Due to the public and shared nature, it is possible to implement comprehensive methods for a better monitoring of transaction data. Thus, BPC-relevant process and transaction data can be collected and evaluated in real time [10, 13, 24]. Since transaction fees have to be paid and compliance processes can be partially automated by smart contracts, BPC costs can be determined on process activity level [43].

However, the high energy consumption for performing the PoW and the local memory requirements for redundant blockchain replications are considered to be critical [44]. All in all, Ethereum offers comprehensive possibilities to address different BPC challenges. Nevertheless, resulting risks must be considered as well.

6 Conclusion

The second generation of Blockchain technologies, such as Ethereum, allows not only for the processing of financial transactions [11], but also for elaborated applications in various fields, such as BPC. Since there are a lot of BPC challenges (e.g. [9, 10]), we raised the following research question: How does the Ethereum blockchain address challenges of BPC? By conducting a literature review, we identified 14 main features of Ethereum. Furthermore, we identified 21 BPC challenges and categorized them according to legal, organizational, human-centered, technical and economic challenges.

A large portion of the challenges is of organizational and technical nature. It has been shown that the main contribution of the Ethereum blockchain is to solve technical and organizational challenges, whereas human-centered challenges are less solvable. The following main features are of utmost importance to meeting BPC challenges: automation with the help of smart contracts; the transparent design and traceability of the public ledger; and the possibility of using Ethereum as a universal data infrastructure. However, the use of the blockchain also results in new risks, such as the immutability of illegal content or the error-proneness of smart contracts due to a lack of knowledge or their zero-defect tolerance during execution [3, 33, 36, 37].

A well-known shortcoming of any literature review is the fact that it is not possible to consider all relevant work. However, by documenting the literature research according to vom Brocke et al. [12], comprehensibility in the development of arguments is provided in a scientific manner. The assignment of BPC challenges and Ethereum properties is not always documented in the literature and therefore results from an argumentative assignment. Additionally, each property of the Ethereum Blockchain in our reference table has an equally weighted potential to meet the respective BPC challenges. Our future research aims to investigate these potentials explicitly, according to their specific impact on solving BPC challenges.

References

1. Aste, T., Tasca, P., Di Matteo, T.: Blockchain Technologies. The Foreseeable Impact on Society and Industry. Computer, 50(9), 18–28 (2017)
2. Asharaf, S., Adarsh, S.: Decentralized computing using blockchain technologies and smart contracts: Emerging research and opportunities. Introduction to Blockchain Technology. IGI Global, Hershey, PA, USA (2017)
3. Ateniese, G., Magri, B., Venturi, D., Andrade, E.: Redactable Blockchain - or - Rewriting History in Bitcoin and Friends. In: IEEE EuroS&P 2017, pp. 111–126
4. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf (Accessed: 12.05.2018)
5. Buterin, V.: Ethereum White Paper. A next generation smart contract & decentralized application platform, https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (Accessed: 18.06.2017)
6. Bocek, T., Rodrigues, B.B., Strasser, T., Stiller, B.: Blockchains everywhere - a use-case of blockchains in the pharma supply-chain. In: IFIP/IEEE IM 2017, Lisbon, Portugal, pp. 772–777
7. Deubel, M., Moormann, J., Holotiuk, F.: Nutzung der Blockchain-Technologie in Geschäftsprozessen. In: INFORMATIK 2017, Chemnitz, Germany, pp. 829–842
8. Schäfer, T., Fettke, P., Loos, P.: Towards an Integration of GRC and BPM - Requirements Changes for Compliance Management Caused by Externally Induced Complexity Drivers. In: BPM 2011, Clermont-Ferrand, France, pp. 344–355
9. Becker, J., Delfmann, P., Eggert, M., Schwittay, S.: Generalizability and Applicability of Model-Based Business Process Compliance-Checking Approaches — A State-of-the-Art Analysis and Research Roadmap. Business Research, 5(2), 221–247 (2012)

10. Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., Thompson, C.: A Distributed-Ledger Consortium Model for Collaborative Innovation. Computer, 50(9), 29–37 (2017)
11. Modsching, M., Apfelbacher, A., Horch, J., Kummer, N.: Using a blockchain-based approach to exchange (financial) assets. Journal of digital banking, 2(2), 110–122 (2017)
12. Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A.: Reconstructing the giant. On the importance of rigour in documenting the literature search process. In: ECIS 2009, Verona, Italy, pp. 2206–2217
13. Fridgen, G., Radszuwill, S., Urbach, N., Utz, L.: Cross-Organizational Workflow Management Using Blockchain Technology - Towards Applicability, Auditability, and Automation. In: HICSS-51 2018, Hilton Waikoloa Village, Hawaii, pp. 3507–3516
14. Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., Mendling, J.: Untrusted Business Process Monitoring and Execution Using Blockchain. In: BPM 2016, Rio de Janeiro, Brazil, pp. 329–347
15. Sadiq, S., Governatori, G.: Managing Regulatory Compliance in Business Processes. In: Brocke, J., Rosemann, M. (eds.) Handbook on Business Process Management 2. Strategic Alignment, Governance, People and Culture, pp. 159–175. Springer, Berlin, Heidelberg (2010)
16. Elgammal, A.F.S.A.: Towards a comprehensive framework for business process compliance. Diss. Tilburg University, Netherlands (2012)
17. Kaaniche, N., Laurent, M.: A blockchain-based data usage auditing architecture with enhanced privacy and availability. In: IEEE NCA 2017, Cambridge, MA, USA, pp. 1–5
18. Turetken, O., Elgammal, A., van den Heuvel, W.-J., Papazoglou, M.: Enforcing compliance on business processes through the use of patterns. In: ECIS 2011, Helsinki, Finland. 5.
19. Seyffarth, T., Kühnel, S., Sackmann, S.: A Taxonomy of Compliance Processes for Business Process Compliance. In: BPM 2017, Barcelona, Spain, pp. 71–87
20. Fellmann, M., Zasada, A.: State-of-the-Art of Business Process Compliance Approaches: A Survey. In: ECIS 2014, Tel Aviv, Israel, pp. 1–17
21. Sadiq, S.: A Roadmap for Research in Business Process Compliance. In: BIS 2011, Poznań, Poland, pp. 1–4
22. Knuplesch, D., Reichert, M., Fdhila, W., Rinderle-Ma, S.: On Enabling Compliance of Cross-Organizational Business Processes. In: BPM 2013, Beijing, China, pp. 146–154
23. Zhang, P., Walker, M.A., White, J., Schmidt, D.C., Lenz, G.: Metrics for assessing blockchain-based healthcare decentralized apps. In: IEEE Healthcom 2017, Dalian, China, pp. 1–4
24. Imeri, A., Khadraoui, D.: The Security and Traceability of Shared Information in the Process of Transportation of Dangerous Goods. In: IFIP NTMS 2018, pp. 1–5
25. Rinderle-Ma, S., Thao Ly, L. and Dadam, P.: Aktuelles Schlagwort: Business Process Compliance, https://www.uni-ulm.de/fileadmin/website_uni_ulm/iui.emisa/Downloads/EMISA_aktschlagwort_compliance.pdf (Accessed: 25.02.2018)
26. Reichert, M., Weber, B.: Enabling Flexibility in Process-Aware Information Systems. Challenges, Methods, Technologies. Springer, Heidelberg, Berlin (2012)
27. Matsumoto, S., Reischuk, R.M.: IKP: Turning a PKI Around with Decentralized Automated Incentives. In: IEEE SP 2017, San Jose, CA, USA, pp. 410–426
28. Sackmann, S., Kühnel, S., Seyffarth, T.: Using Business Process Compliance Approaches for Compliance Management with regard to Digitization: Evidence from a Systematic Literature Review. In: BPM 2018, Sydney, Australia, pp. 409–425
29. Brammertz, W., Mendelowitz, A.I.: From digital currencies to digital finance. The case for a smart financial contract standard. The Journal of Risk Finance, 19(1), 76–92 (2018)

30. Kavassalis, P., Stieber, H., Breymann, W., Saxton, K., Gross, F.J.: An innovative RegTech approach to financial risk monitoring and supervisory reporting. The Journal of Risk Finance, 19(1), 39–55 (2018)
31. Kühnel, S.: Toward Cost-Effective Business Process Compliance. A Research Agenda. In: INFORMATIK 2017, Chemnitz, Germany, pp. 2379–2384
32. Yoo, S.: Blockchain based financial case analysis and its implications. APJIE, 11(3), 312–321 (2017)
33. Morabito, V.: Business Innovation Through Blockchain. The B³ Perspective. Springer International Publishing, Cham (2017)
34. Cen, Y., Wang, H., Li, X.: Improving Business Process Interoperability by Shared Ledgers. In: IEEA 2017, Jeju, Republic of Korea, pp. 89–93
35. Kharitonov, A.: A Framework for Strategic Intra- and Inter-Organizational Adoption of the Blockchain Technology. SSRN Electronic Journal, 1–6
36. Frantz, C.K., Nowostawski, M.: From Institutions to Code. Towards Automated Generation of Smart Contracts. In: IEEE FAS*W 2016, Augsburg, Germany, pp. 210–215
37. Clack, C.D., Bakshi, V.A. and Braine, L.: Smart Contract Templates: foundations, design landscape and research directions, https://arxiv.org/pdf/1608.00771v2.pdf (Accessed: 11.05.2018)
38. Reijers, W., O'Brolcháin, F. and Haynes, P.: Governance in Blockchain Technologies & Social Contract Theories, https://ledger.pitt.edu/ojs/index.php/ledger/article/view/62/51 (Accessed: 11.05.2018)
39. Lemieux, V.L.: A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In: IEEE Big Data 2017, pp. 2271–2278
40. Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E.: Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. In: FC 2016, Christ Church, Barbados, pp. 79–94
41. Conte de Leon, D., Stalick, A., Jillepalli, A., Haney, M.: Blockchain: Properties and misconceptions. APJIE, 11(3), 286–300 (2017)
42. Fabiano, N.: Internet of Things and Blockchain. Legal Issues and Privacy. The Challenge for a Privacy Standard. In: IEEE iThings and IEEE GreenCom and IEEE CPSCom and IEEE SmartData, Exeter, UK, pp. 727–734
43. García-Bañuelos, L., Ponomarev, A., Dumas, M., Weber, I.: Optimized Execution of Business Processes on Blockchain. In: BPM 2017, Barcelona, Spain, pp. 130–146
44. Marsal-Llacuna, M.-L., Oliver-Riera, M.: The standards revolution. Who will first put this new kid on the blockchain? In: ITU K 2017, pp. 1–7