arXiv:1704.03610v2 [cs.SE] 2 Jul 2017

Blockchains for Business Process Management - Challenges and Opportunities

Jan Mendling[a,*], Ingo Weber[b,c,*], Wil van der Aalst[d], Jan vom Brocke[e], Cristina Cabanillas[a], Florian Daniel[f], Søren Debois[g], Claudio Di Ciccio[a], Marlon Dumas[h], Schahram Dustdar[i], Avigdor Gal[j], Luciano García-Bañuelos[h], Guido Governatori[b], Richard Hull[k], Marcello La Rosa[m], Henrik Leopold[l], Frank Leymann[n], Jan Recker[m], Manfred Reichert[o], Hajo A. Reijers[l], Stefanie Rinderle-Ma[p], Andreas Rogge-Solti[a], Michael Rosemann[m], Stefan Schulte[i], Munindar P. Singh[q], Tijs Slaats[r], Mark Staples[b,c], Barbara Weber[s], Matthias Weidlich[t], Mathias Weske[u], Xiwei Xu[b,c], Liming Zhu[b,c]

[a] *Wirtschaftsuniversität Wien, Vienna, Austria*
[b] *Data61, CSIRO, Australia*
[c] *University of New South Wales, Sydney, Australia*
[d] *Eindhoven University of Technology, Eindhoven, The Netherlands*
[e] *University of Liechtenstein, Liechtenstein*
[f] *Politecnico di Milano, Italy*
[g] *IT University of Copenhagen, Denmark*
[h] *University of Tartu, Estonia*
[i] *TU Wien, Vienna, Austria*
[j] *Technion - Israel Institute of Technology, Haifa, Israel*
[k] *IBM Research, Yorktown Heights, NY, USA*
[l] *Vrije Universiteit Amsterdam, Amsterdam, The Netherlands*
[m] *Queensland University of Technology, Brisbane, Australia*
[n] *IAAS, Universität Stuttgart, Germany*
[o] *Ulm University, Ulm, Germany*
[p] *University of Vienna, Vienna, Austria*
[q] *North Carolina State University, Raleigh, NC, USA*
[r] *University of Copenhagen, Copenhagen, Denmark*
[s] *Technical University of Denmark, Lyngby, and University of Innsbruck, Innsbruck, Austria, Denmark*
[t] *Humboldt-Universität zu Berlin, Germany*

[*] Corresponding author

Email addresses: jan.mendling@wu.ac.at (Jan Mendling), ingo.weber@data61.csiro.au (Ingo Weber), w.m.p.v.d.aalst@tue.nl (Wil van der Aalst), jan.vom.brocke@uni.li (Jan vom Brocke), cristina.cabanillas@wu.ac.at (Cristina Cabanillas), florian.daniel@polimi.it (Florian Daniel), debois@itu.dk (Søren Debois), claudio.di.ciccio@wu.ac.at (Claudio Di Ciccio), marlon.dumas@ut.ee (Marlon Dumas), dustdar@tuwien.ac.at (Schahram Dustdar), avigal@technion.ac.il (Avigdor Gal), luciano.garcia@ut.ee (Luciano García-Bañuelos), guido.governatori@data61.csiro.au (Guido Governatori), hull@us.ibm.com (Richard Hull), m.larosa@qut.edu.au (Marcello La Rosa), h.leopold@vu.nl (Henrik Leopold), frank.leymann@iaas.uni-stuttgart.de (Frank Leymann), j.recker@qut.edu.au (Jan Recker), manfred.reichert@uni-ulm.de (Manfred Reichert), h.a.reijers@vu.nl (Hajo A. Reijers), stefanie.rinderle-ma@univie.ac.at (Stefanie Rinderle-Ma), andreas.rogge-solti@wu.ac.at (Andreas Rogge-Solti), m.rosemann@qut.edu.au (Michael Rosemann), stefan.schulte@tuwien.ac.at (Stefan Schulte), mpsingh@ncsu.edu (Munindar P. Singh), slaats@di.ku.dk (Tijs Slaats), mark.staples@data61.csiro.au (Mark Staples), bweb@dtu.dk (Barbara Weber), matthias.weidlich@hu-berlin.de (Matthias Weidlich), mathias.weske@hpi.de (Mathias Weske), xiwei.xu@data61.csiro.au (Xiwei Xu), liming.zhu@data61.csiro.au (Liming Zhu)

Preprint submitted to ACM Transactions on Management Information Systems July 4, 2017

[u]Hasso-Plattner-Institute, Universität Potsdam, Germany

Abstract

Blockchain technology offers a sizable promise to rethink the way inter-organizational business processes are managed because of its potential to realize execution without a central party serving as a single point of trust (and failure). To stimulate research on this promise and the limits thereof, in this paper we outline the challenges and opportunities of blockchain for Business Process Management (BPM). We structure our commentary alongside two established frameworks, namely the six BPM core capabilities and the BPM lifecycle, and detail seven research directions for investigating the application of blockchain technology to BPM.

Keywords: Blockchain, Business Process Management, Research Challenges

1. Introduction

Business process management (BPM) is concerned with the design, execution, monitoring, and improvement of business processes. Systems that support the enactment and execution of processes have extensively been used by companies to streamline and automate *intra*-organizational processes. Yet, for *inter*-organizational processes, challenges for the joint design and a lack of mutual trust have hampered a broader uptake.

Emerging *blockchain* technology has the potential to drastically change the environment in which inter-organizational processes are able to operate. Blockchains offer a way to execute processes in a trustworthy manner even in a network without any mutual trust between nodes. Key aspects are specific algorithms that lead to consensus among the nodes and market mechanisms that motivate the nodes to progress the network. Through these capabilities, this technology has the potential to shift the discourse in BPM research about how systems might enable the enactment, execution, monitoring or improvement of business process within or across business networks.

In this paper, we describe what we believe are the main new challenges and opportunities of blockchain technology for BPM. This leads to directions for research activities to investigate both challenges and opportunities. Section 2 provides a background on fundamental concepts of blockchain technology and an illustrative example of how this technology applies to business processes. In Sections 3 and 4 we then discuss blockchains' impact on BPM. We use the *six core BPM elements* [Rosemann & vom Brocke, 2015] and the *BPM lifecycle phases* [Dumas et al., 2013] to structure this discussion. Section 5 summarizes this discussion by emphasizing seven future research directions.

2. Background

This section summarizes the essential aspects of blockchain technology and discusses initial research efforts at the intersection of BPM and blockchains.

2.1. Blockchain Technology

Blockchain is the technology underlying Bitcoin and other cryptocurrencies [Nakamoto, 2008]. It is a distributed database technology that builds on a tamper-proof list of timestamped transaction records. Its innovative power stems from allowing parties to transact with others they do not trust over a network in which nobody is trusted. This is enabled by a combination of peer-to-peer networks, consensus-making, cryptography, and market mechanisms. Blockchains ensure data integrity and transparency, such that the blockchain network stays operational even under byzantine faults. A copy of the entire blockchain is held on every node on the network and consensus is achieved either by proof-of-work or proof-of-stake algorithms [Mougayar, 2016].

Blockchain technology is more broadly applicable than to cryptocurrencies alone: in essence, it offers access to the history of all previous states. Furthermore, several of the available implementations of blockchain networks offer the possibility of executing user-defined scripts, so-called *smart contracts* [Szabo, 1997]. For instance, the *Ethereum* blockchain supports Turing-complete programming languages for smart contracts[1]. The code in this language is deterministic and relies on a closed-world assumption: only knowledge from blockchain transactions is available in the runtime environment. Smart contract code is deployed with a specific type of transaction. As with any other blockchain transaction, the deployment of smart contract code to the blockchain is immutable. Once deployed, smart contracts offer a way to execute code directly on the blockchain network, for instance to transfer money if a certain condition is fulfilled. This way, untrusted parties can establish trust in the truthful execution of the code. Smart contracts can be used to implement business collaborations in general, and inter-organizational business processes in particular. The potential of blockchain-based distributed ledgers to enable collaboration in open environments has been successfully tested in diverse fields ranging from diamonds trading to securities settlement [Walport, 2016].

Blockchain technology itself still faces numerous general technological challenges, which Swan [2015] organized into the categories we discuss in the following. A mapping study by Yli-Huumo et al. [2016] found that a majority of these challenges have not been addressed by the research community, albeit we note that blockchain developer communities actively discuss some of these challenges and suggest a myriad of potential solutions[2].

[1] https://www.ethereum.org/

[2] http://www.the-blockchain.com/2017/01/24/adi-ben-ari-outstanding-challenges-blockchain-technology-2017/

Throughput in the Bitcoin blockchain is limited to 7 transaction inclusions per second (tps) currently, and is likely to double in the near future. In comparison, transaction volumes for the VISA payment network are 2,000 tps on average, with a tested capacity of up to 50,000 tps. Ethereum achieves on the order of 15 tps. However, this limitation becomes less relevant if private or consortium blockchains [Mougayar, 2016] were used in cross-organizational networks.

Latency is a weak spot of Bitcoin in particular, where transaction inclusion in the absence of network congestion would take on average 15 minutes (1.5x interblock time of 10 minutes, since the transaction on average gets submitted half-way into a block creation, and mining the next block which includes this transaction takes 1 interblock time). In addition, 5 confirmation blocks are typically recommended to ensure the transaction does not get removed due to accidental or deliberate (malicious) forking – resulting in an average 65 minutes to be certain a transaction remains part of the ledger permanently. Network congestion increases this number further. Other public blockchains like Ethereum decrease this time to about 3 to 10 minutes, depending on the required level of probabilistic guarantees. Private or consortium blockchains can use other mechanisms, like coordinated mining, which can reduce the transaction confirmation time. Efforts like the *Lightning Network* or *Raiden* propose to create lightweight, very fast transaction networks on top of public blockchains like Bitcoin and Ethereum. They achieve this by binding liquidity and smart contracts. While highly promising, these concepts are still in their infancy. Similarly, *side chains* are blockchains that are spun off a main chain, with ties back to the main chain. By including cryptographic hashes of the side chain periodically into the main chain, the history of the side chain could not be rewritten without overpowering the main chain. Thus, side chains can afford to operate on much less computational power. Nevertheless, blockchains are unlikely to achieve latencies as low as centrally-controlled systems, due to their distributed nature. Their use will remain a trade-off.

Size and bandwidth limitations are variations of the throughput issue: if the transaction volume of VISA were to be processed by Bitcoin, the full replication of the entire blockchain data structure would pose massive problems – Yli-Huumo et al. [2016] quote 214 PB per year, thus posing a challenge in data storage and bandwidth. Private and consortium chains and concepts like the lightning network or side chains all aim to address these challenges.

Usability is limited, in terms of both developer support (lack of adequate tooling) and end-user support (hard to use and understand). Recent advances on developer support include efforts by some of the authors towards model-driven development [Weber et al., 2016; García-Bañuelos et al., 2017; Tran et al., 2017].

Security will always pose a challenge on an open network like a public blockchain. Security is often discussed in terms of the CIA properties [Dhillon & Backhouse, 2000]. First, *confidentiality* is per se low in a distributed system that replicates all data over its network, but can be addressed by targeted encryption [Kosba et al., 2016]. Second, *integrity* is a strong suit of blockchains, albeit challenges do exist [Eyal & Sirer, 2014; Gervais et al., 2016]. Third, *availability* can be considered high in terms of reads from blockchain due to the wide replication, but less clear in terms of write availability, since large-scale experiments on this matter have not been published to date. The often-quoted 51% attack of nodes taking over the blockchain [Bradbury, 2013] is a fairly theoretical question for large-scale blockchains like Bitcoin. Bitcoin miners are hypothesized to collectively use as much power as Paraguay, the entire country, mostly with specialized hardware. To amass more computational power than that is unlikely for any given player, be it a nation state or a corporation. It does, however, remain a credible threat for consortium blockchains – albeit these can be controlled with organizational governance structures.

Wasted resources, particularly electricity, are due to the *proof-of-work* mechanism, where miners constantly compete in a race to mine the next block for a high reward. Alternatives, like *proof-of-stake* [Bentov et al., 2016], have been discussed for a while and would be much more efficient. At the time of writing, they remain an unproven but highly interesting alternative.

Hard forks are changes to the protocol of a blockchain which enable transactions or blocks which were previously considered invalid [Decker & Wattenhofer, 2013]. They essentially change the rules of the game and therefore require a consensus by a vast majority of the miners to be effective [Bonneau et al., 2015]. While hard forks can be controversial in public blockchains, as demonstrated by the split of the Ethereum blockchain into a hard forked main chain and Ethereum Classic, this is less of an issue for private and consortium blockchains where such a consensus is more easily found.

Many of these general technological challenges of blockchains are currently the focus of the emergent body of research. As noted, several solution attempts to the problems above have been proposed and tested. Notwithstanding current and future issues and developments, our main interest is in the *potential* of blockchain technology to enable a consensus shift in BPM research. Our belief is vested both in the novel technological properties discussed above and in the already available attempts of using blockchain technology in the definition and implementation of fundamentally novel business processes. We review these attempts in the following.

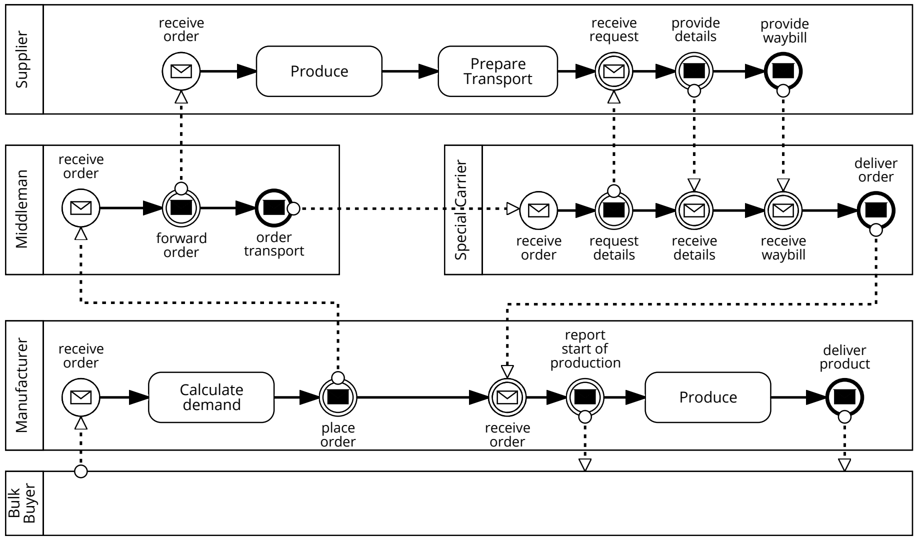

Figure 1: Supply Chain Scenario from Weber et al. [2016]

2.2. Business Processes and Blockchain Technology

We are not the first to identify the application potential of blockchain technology to business processes. In fact, several blockchains are currently adopted in various domains to facilitate the operation of new business processes. For example, Nofer et al. [2017] list applications in the financial sector including crypto-currency transactions, securities trading and settlement, and insurances as well as non-financial applications such as notary services, music distribution, and various services for proof of existence, authenticity and storage. Other works describe application scenarios involving blockchain technology in logistics and supply chain processes, for instance in the agricultural sector [Staples et al., 2017].

A proposal to support inter-organizational processes through blockchain technology is described by Weber et al. [2016]: specific aspects of inter-organizational business processes can be compiled into smart contracts that ensure the joint process is correctly executed. So-called *trigger* components allow connecting these inter-organizational process implementations to Web services and internal process implementations. These triggers serve as a bridge between the blockchain and enterprise applications. The cryptocurrency concept enables the optional implementation of conditional payment and built-in escrow management at defined points within the process, where this is desired and feasible.

To illustrate these capabilities, Figure 1 shows a simplified supply chain scenario, where a bulk buyer orders goods from a manufacturer. The manufacturer, in turn, orders supplies through a middleman, which are sent from the supplier to the manufacturer via a special carrier. Without global monitoring each participant has a restricted visibility of the overall progress. This may very well be a basis for misunderstandings and shifting blame in cases of conflict.

If executed using smart contracts on a blockchain, typical barriers complicating the deployment of inter-organization processes can be removed. (i) The blockchain can serve as an immutable public ledger, so that participants can review a trustworthy history of messages to pinpoint the source of an error. This means that all state-changing messages have to be recorded in the blockchain. (ii) Smart contracts can offer independent process monitoring from a global viewpoint, such that only expected messages are accepted, and only if they are sent from the player registered for the respective role in the process instance. (iii) Encryption can ensure that only the data that must be visible is public, while the remaining data is only readable for the process participants that require it.

These capabilities demonstrate how blockchains can help organizations to implement and execute business processes across organizational boundaries even if they cannot agree on a trusted third party. This is a fundamental advance, because the core aspects of this technology now enable support of enterprise collaborations going far beyond asset management, including the management of entire supply chains, tracking food from source to consumption to increase safety, or sharing personal health records in privacy-ensuring ways amongst medical service providers.

The technical realization of this advance is still nascent at this stage, although some early efforts can be found in the literature. For example, smart contracts that enforce a process execution in a trustworthy way can be generated from BPMN process models [Weber et al., 2016] and from domain-specific languages [Frantz & Nowostawski, 2016]. Further cost optimizations are proposed by García-Bañuelos et al. [2017]. Likewise, the affinity of artifact-centric process specification [Cohn & Hull, 2009; Marin et al., 2012] to blockchain execution has already been emphasized by Hull et al. [2016].

Even at this stage, research on the benefits and potentials of blockchain technology is mixed with studies that highlight or examine issues and challenges. For example, Norta [2015, 2016] discusses ways to ensure secure negotiation and creation of smart contracts for Decentralized Autonomous Organizations (DAOs), among others in order to avoid attacks like the DAO hack during which approx. US$ 60M were stolen. This in turn was partly reversed by a hard fork of the Ethereum blockchain, which was controversial among the respective mining node operators and resulted in a part of the public Ethereum network splintering off into the *Ethereum classic* (ETC) network. This split, in turn, caused major issues for the network in the medium term, allowing among others *replay attacks* where transactions from Etherium can be replayed on ETC. A formal analysis of smart contract participants using game theory and formal methods is conducted by Bigi et al. [2015]. As pointed out by Norta [2016], the assumption of perfect rationality underlying the game-theoretic analysis is unlikely to hold for human participants.

These examples go to show that blockchain technology and its application to BPM are at an important crossroads: technical realization issues blend with promising application scenarios; early implementations mix with unanticipated challenges. It is timely, therefore, to discuss in broad and encompassing ways where open questions lie that the scholarly community should be interested in addressing. We do so in the two sections that follow.

3. Blockchain Technology and BPM Capabilities

We now discuss challenges and opportunities for BPM that arise from blockchain technology in relation to six BPM core capability areas [Rosemann & vom Brocke, 2015], namely strategic alignment, governance, methods, information technology, people, and culture.

3.1. Strategic Alignment

Strategic alignment refers to the active management of connections between organizational priorities and enterprise processes [Rosemann & vom Brocke, 2015], which aims at facilitating effective actions to improve business performance. Currently, various approaches to BPM assume that the corporate strategy is defined first and business processes are aligned with the respective strategic imperatives [Dumas et al., 2013]. Blockchain technology challenges these approaches to strategic alignment in the following way.

First, companies need to define a strategic position with respect to blockchain technology, such that processes can be aligned with this position. This calls for research on how the impact of blockchains on specific processes can be systematically analyzed. Such analysis includes, for instance, the assessment of which processes can be improved with blockchains, which new strategic priorities emerge from using blockchain technology in business processes, or which strategic risks comparable to lock-in effects [Tassey, 2000] might emerge.

Second, blockchain as a disruptive technology challenges the traditional process-follows-strategy paradigm, which could be flipped upside down with new blockchain-based processes challenging entire industries. For many companies, a potential disintermediation enabled by the use of blockchain-based systems might pose more of a threat than an opportunity, as discussed for instance for the banking industry [Guo & Liang, 2016].

3.2. Governance

BPM governance refers to appropriate and transparent accountability in terms of roles, responsibilities, and decision processes for different BPM-related programs, projects, and operations [Rosemann & vom Brocke, 2015]. Currently, BPM as a management approach builds on the explicit definition of BPM-related roles and responsibilities with a focus on the internal operations of a company. Blockchain technology changes governance towards a more externally oriented coopetition as a new management mode for processes. This has the following implications.

First, dedicated roles have to be defined that liaise not only with internal, but also with external partners for setting up blockchain support for processes. These new roles require both technical and jurisprudential knowledge.

Second, there is a need for policies that define where and when blockchain technology can be used or must not be used for supporting processes. For instance, cryptocurrencies have highly volatile exchange rates to traditional currencies – gains and losses of 10-50% within a single day are not uncommon. It is expected that this volatility will decrease with broader uptake [Mougayar, 2016]; but as of today, it is a roadblock for many applications. Exchange rate volatility is less of a concern for private and consortium-based blockchains which will not see a sudden influx of new capital without prior authorization and are less likely to attach monetary value to blocks, but rather use blockchain as a common ledger for shared processes and data.

Third, new attack scenarios on blockchain networks are difficult to foresee [Hurlburt, 2016]. Therefore, guidelines for using private, public, or consortium-based blockchains are required [Mougayar, 2016]. It also has to be decided what types of smart contract and which cryptocurrency are allowed to be used.

Finally, smart contracts promise to facilitate self-governance of not only processes, but of entire organizations. Research on corporate governance investigates agency problems and effective mechanisms to incentivize intended behavior [Shleifer & Vishny, 1997]. Smart contracts can be used to establish new governance models as exemplified by the Decentralized Autonomous Organization (DAO) [3]. It is an important question in how far this idea of the DAO can be extended towards reducing the agency problem of management discretion or eventually eliminate the need for management altogether. Furthermore, the revolutionary change suggested by the DAO for organization shows just how disruptive this technology can be, and whether similarly radical changes could apply to BPM.

3.3. Methods

BPM methods refer to tools and techniques that support management activities along the process lifecycle and throughout an enterprise-wide BPM program [Dumas et al., 2013]. Currently, these methods often focus on issues and weaknesses of how a process currently operates and they require labor-intensive and time-consuming data collection and analysis.

Blockchains may affect methods in the following three ways. First, specific novel analysis methods are required to assess costs, benefits, and potential risks associated with using blockchain for processes. Second, specific engineering methods are needed to address the specific features of blockchain technology and its usage in supporting inter-organizational processes. In particular, there is a need for formal reasoning capabilities about the correctness and privacy preservation of processes that are designed based on smart contracts. Finally, the emergence of blockchain technology emphasizes the need to complement exploitative analysis methods that start from the weaknesses of existing processes with methods that explore both new ways of implementing existing processes

[3] https://daohub.org

and innovating completely new processes. In this way, blockchain might arguably redirect attention from analyzing process weaknesses back to searching unexplored new opportunities in the spirit of the process re-engineering concepts of the early 1990s. Back then, Hammer & Champy [1993] formulated their credo of "Do not automate, obliterate:" companies should re-engineer their processes from scratch by the help of then new client-server technology instead of automating old-fashioned and ineffective ways of operation. Now, it is blockchain that provides the potential to re-engineer processes from scratch.

3.4. Information Technology

BPM-related information technology subsumes all systems that support process execution. Currently, business process technology is shaped by process-aware information systems [Dumas et al., 2005] and business process management systems [Weske, 2012], which both typically assume central control over the process.

Blockchain technology enables novel ways of process execution, but several challenges have to be considered. First, implementing processes with blockchains requires new software components and integrated development environments. Second, such blockchain-based process execution gives rise to new challenges in terms of security and privacy, such as how to prevent confidential business data leakage. While the visibility of encrypted data on a blockchain is restricted, it is up to the participants in the process to ensure that these mechanisms are used according to their confidentiality requirements. Some of these requirements are currently investigated in the financial industry[4]. Further challenges can be expected with the enactment of the General Data Protection Regulation[5].

Finally, inherent limitations of blockchains have to be considered including computational power, data storage, throughput, and processing costs. Rather than using an existing blockchain, an alternative could be to adopt only the corresponding design principles, like replicated transaction history, or using private blockchains to reduce costs.

3.5. People

People in this context refers to all individuals, possibly in different roles, who engage with BPM [Rosemann & vom Brocke, 2015]. Currently, these are people who work as process analyst, process manager, process owner or in other process-related roles. The roles of these individuals are shaped by skills in the area of management, business analysis and requirements engineering. In this capability area, the use of blockchain technology requires extensions of their skill sets. New required skills relate to partner and contract management, software enginering, and cryptography. Blockchains and the design of smart contracts will also require new ways of thinking about people, since actors in inter-organizational

[4] https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

processes have more freedom to act than intra-organizational process participants. This is not only a challenge, but also an opportunity since the openness of blockchains makes it easy to offer incentives for third parties to contribute to ongoing processes. Finally, people have to be willing to design blockchain-based collaborations within the frame of existing regulations to enable adoption. This implies that research into blockchain-specific technology acceptance is needed, extending the established technology acceptance model [Venkatesh, 2014].

3.6. Culture

Organizational culture is defined by the collective values of a group of people in an organization [Rosemann & vom Brocke, 2015]. Currently, BPM is discussed in relation to organizational culture [vom Brocke & Sinnl, 2011] from a perspective that emphasizes an affinity with clan and hierarchy culture [Štemberger et al., 2017]. These culture types are often found in the many companies that use BPM as an approach for documentation. Blockchains are likely to influence organizational culture towards a stronger emphasis on flexibility and an outward-looking perspective. In the competing values framework by Cameron & Quinn [2005], these aspects are associated with an adhocracy organizational culture. Furthermore, not only consequences of blockchain adoption have to be studied, but also antecedants. These include organizational factors that facilitate early and successful adoption.

4. Blockchain Technology and the BPM Lifecycle

In this section, we discuss blockchain in relation to the traditional BPM lifecycle [Dumas et al., 2013] including the following phases: identification, discovery, analysis, redesign, implementation, execution, monitoring, and adaptation. These phases mainly refer to the general *information technology* and *methods* capability areas. We discuss specific challenges for each phase here.

4.1. Identification

Process identification is concerned with the high-level description and evaluation of a company from a process-oriented perspective, thus connecting strategic alignment with process improvement. Currently, identification is mostly approached from an inward-looking perspective [Dumas et al., 2013]. Blockchain technology adds another relevant perspective for evaluating high-level processes in terms of the implied strengths, weaknesses, opportunities, and threats. Research is needed into how these perspectives can be systematically integrated into the identification phase. Because blockchains have affinity with the support of inter-organizational processes, process identification may need to encompass not only the needs of one organization, but broader known and even unknown partners.

4.2. Discovery

Process discovery refers to the collection of information about the current way a process operates and its representation as an *as-is* process model. Currently, classical methods of process discovery and elicitation are complemented by various recent process mining techniques for structured and non-encrypted data [van der Aalst, 2016]. Blockchain technology defines new challenges for process discovery techniques: the information may be fragmented and encrypted; accounts and keys can change frequently; and payload data may be stored partly on-chain and partly off-chain. This fragmentation might require a repeated alignment of information from all relevant parties operating on the blockchain. Work on matching could represent a promising starting point to solve this problem [Euzenat & Shvaiko, 2013; Gal, 2011; Cayoglu et al., 2014]. There is both the risk and opportunity of conducting process mining on the blockchain. An opportunity could involve establishing trust in how a process or a prospective business partner operates, while a risk is that other parties may gain access to internal information and know-how. There are also opportunities for reverse engineering business processes, among others, from smart contracts.

4.3. Analysis

Process analysis refers to obtaining insights into issues relating to the way a business process currently operates. Currently, the analysis of processes mostly builds on data that is available inside of organizations or from perceptions shared by internal and external process stakeholders [Dumas et al., 2013]. Records of processes executed on the blockchain yield valuable information that can help to assess the case load, durations, frequencies of paths, parties involved, and correlations between unencrypted data items. These pieces of information can be used to discover processes, detect deviations, and conduct root cause analysis [van der Aalst, 2016], ranging over small groups of companies or over an industry at large.

4.4. Redesign

Process redesign deals with the systematic improvement of a process. Currently, process redesign is mostly supported by so-called redesign heuristics, which formulate proven solutions for specific issues a process might face [Vanwersch et al., 2016]. Blockchain technology offers novel ways of improving specific business processes or resolving specific problems, e.g. because blockchain offers new ways of interaction in cross-organizational settings. The question is where blockchains can be applied for optimizing existing interactions and where new interaction patterns without a trusted central party can be established, potentially drawing on insights from related research on Web service interaction [Barros et al., 2005]. A promising direction for developing blockchain-appropriate abstractions and heuristics may come from data-aware workflows [Marin et al., 2012] and BPMN choreography diagrams [Decker & Weske, 2011]. Both techniques combine two primary ingredients of blockchain, namely data and process, in a holistic manner that is well-suited for top-down design of cross-organizational processes. It might also be beneficial to formulate blockchain-specific redesign heuristics that could mimic how Incoterms [Ramberg, 2011] define standardized interactions in international trade. Specific challenges for redesign include the joint engineering of blockchain processes between all parties involved, an ongoing problem for choreography design. Balancing the trade-off between blockchain benefits, transaction cost, risk, delay, and other factors is a major open question.

4.5. Implementation

Process implementation refers to the procedure of transforming a *to-be* model into software components executing the business process. Currently, business processes are often implemented using process-aware information systems or business process management systems inside single organizations. Some of the challenges of model transformation to blockchain artifacts are discussed by Weber et al. [2016]. Several ideas from earlier work on choreography can be reused in this new setting [van der Aalst & Weske, 2001; Mendling & Hafner, 2008; Weber et al., 2008; Decker & Weske, 2011; Chopra et al., 2014; Telang & Singh, 2012]. It has to be noted that choreographies have not been adopted by industry to a large extent yet. Despite this, they are especially helpful in inter-organizational settings, where it is not possible to control and monitor a complete process in a centralized fashion because of organizational borders [Breu et al., 2013]. To verify that contracts between choreography stakeholders have been fulfilled, a trust basis, which is not under control of a particular party, needs to be established. Blockchains may serve to establish this kind of trust between stakeholders.

An important challenge on the implementation level is the identification and definition of abstractions for the design of blockchain-based business process execution. Libraries and operations for engines are required, accompanied by modeling primitives and language extensions of BPMN. Software patterns and anti-patterns will be of good help to engineers designing blockchain-based processes. There is also a need for new approaches for quality assurance, correctness, and verification, as well as for new quality assurance and correctness criteria. These can build on existing notions of compliance [van der Aalst et al., 2008], reliability Subramanian et al. [2008], quality of services [Zeng et al., 2004] or data-aware workflow verification [Calvanese et al., 2013], but will have to go further in terms of consistency and consideration of potential payments. Furthermore, dynamic partner binding and rebinding is a challenge that requires attention. Process participants will have to find partners, either manually or automatically on dedicated marketplaces using dedicated look-up services. For instance, the property of inhabiting a certain role in a process might itself be a tradable asset, e.g., a supplier may auction off the role of shipper to the highest bidder as part of the process. Also, directories for smart contract templates will emerge. All these characteristics emphasize the need for specific testing and verification approaches. Finally, as more and more companies use blockchain there will be a proliferation of smart contract templates available for use. Tools for finding templates appropriate for a given style of collaboration will be essential.

4.6. Execution

Execution refers to the instantiation of individual cases and their information-technological processing. Currently, such execution is facilitated by process-aware information systems or business process management systems [Dumas et al., 2013]. For the actual execution of a process deployed on a blockchain following the method of Weber et al. [2016], several differences with the traditional ways exist. During the execution of an instance, messages between participants need to be passed as blockchain transactions to the smart contract; resulting messages need to be observed from the blocks in the blockchain. Both of these can be achieved by integrating blockchain technology directly with existing enterprise systems, or through the use of dedicated integration components, such as the triggers suggested by Weber et al. [2016]. The main challenge here involves ensuring correctness and security, especially when monetary assets are transferred using this technology.

4.7. Monitoring

Process monitoring refers to collecting events of process executions, displaying them in an understandable way, and triggering alerts and escalation in cases where undesired behavior is observed. Currently, such process execution data is recorded by systems that support process execution [Dumas et al., 2013]. First, we face issues in terms of data fragmentation and encryption as in the analysis phase; e.g., the need to integrate local off-chain data with decrypted local copies of on-chain data. With such tracing in place, the global view of the process can be monitored independently by each involved party. This provides a suitable basis for continuous conformance and compliance checking and monitoring of service-level agreements. Second, based on monitoring data exchanged via the blockchain, it is possible to verify if a process instance meets the original process model and the contractual obligations of all involved process stakeholders. For this, blockchain technology can be exploited to store the process execution data and handovers between process participants. Notably, this is even possible without the usage of smart contracts, i.e., in a first-generation blockchain like the one operated by Bitcoin [Prybila et al., 2017].

4.8. Adaptation

Runtime adaptation refers to the concept of changing the process during execution. Currently, this can for instance be achieved by allowing participants in a process to change the model during its execution [Reichert & Weber, 2012]. In the setting discussed by Weber et al. [2016], blockchain is used to enforce conformance with the model, so that participants can rely on the joint model being followed. In such a setting, adaptation is by default something to be *avoided:* if a participant can change the model, this could be used to gain an unfair advantage over the other participants. For instance, the rules of retrieving cryptocurrency from an escrow account could be changed, or the terms of payment. Therefore, process adaptation must strictly adhere to defined paths for it, e.g., any change to a deployed smart contract may require a transaction signed by all participants. More abstractly speaking, in order to preserve trustworthiness it must be clear who can change what, until when and under which circumstances. There are also problems arising in relation to evolution. New smart contracts will be needed to reflect changes to a new version of the process model. Porting running instances from an old version to a new one would require effective coordination mechanisms involving all participants.

5. Seven Future Research Directions

Blockchains will fundamentally shift how we deal with transactions in general, and therefore how organizations manage their business processes within their network. Our discussion of challenges in relation to the BPM capability areas and the BPM lifecycle points to seven major future research directions:

1. Understanding the impact of blockchain on strategy and governance, in particular regarding new business and governance models enabled by revolutionary innovation based on blockchain.
2. Devising new methods for analysis and engineering business processes based on blockchain technology.
3. Investigating the culture shift towards openness in the management and execution of business processes, and on hiring as well as upskilling people as needed.
4. Developing techniques for identifying, discovering, and analyzing relevant processes for their adoption of blockchain technology.
5. Redesigning processes to leverage the opportunities granted by blockchain. Just like the move from paper files to digital files allowed streamlining processes, blockchain may allow re-imagining how processes can be done in collaboration with external stakeholders. The whole area of choreographies may be re-vitalized by this technology.
6. Developing a diverse set of execution and monitoring frameworks on blockchain.
7. Defining appropriate methods for evolution and adaptation.

The BPM community has a unique opportunity to help shape this fundamental shift towards a distributed, trustworthy infrastructure to promote inter-organizational processes. With this paper we aim to provide clarity, focus, and impetus for the research challenges that are upon us.

References

References

van der Aalst, W. M. P. (2016). *Process Mining - Data Science in Action, Second Edition*. Springer.

van der Aalst, W. M. P., Dumas, M., Ouyang, C., Rozinat, A., & Verbeek, E. (2008). Conformance checking of service behavior. *ACM Trans. Internet Techn.*, *8*.

van der Aalst, W. M. P., & Weske, M. (2001). The P2P approach to interorganizational workflows. In *Proc. CAiSE* (pp. 140–156).

Barros, A., Dumas, M., & ter Hofstede, A. H. (2005). Service interaction patterns. In *International Conference on Business Process Management* (pp. 302–318). Springer.

Bentov, I., Gabizon, A., & Mizrahi, A. (2016). Cryptocurrencies without proof of work. In J. Clark, S. Meiklejohn, P. Y. Ryan, D. Wallach, M. Brenner, & K. Rohloff (Eds.), *Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers* (pp. 142–157). Berlin, Heidelberg: Springer Berlin Heidelberg. URL: `http://dx.doi.org/10.1007/978-3-662-53357-4_10`. doi:`10.1007/978-3-662-53357-4_10`.

Bigi, G., Bracciali, A., Meacci, G., & Tuosto, E. (2015). Validation of decentralised smart contracts through game theory and formal methods. In C. Bodei, G. Ferrari, & C. Priami (Eds.), *Programming Languages with Applications to Biology and Security: Essays Dedicated to Pierpaolo Degano on the Occasion of His 65th Birthday* (pp. 142–161). Springer International Publishing.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy* (pp. 104–121). doi:`10.1109/SP.2015.14`.

Bradbury, D. (2013). The problem with bitcoin. *Computer Fraud & Security*, *2013*, 5–8.

Breu, R., Dustdar, S., Eder, J., Huemer, C., Kappel, G., Köpke, J., Langer, P., Mangler, J., Mendling, J., Neumann, G., Rinderle-Ma, S., Schulte, S., Sobernig, S., & Weber, B. (2013). Towards Living Inter-Organizational Processes. In *15th IEEE Conference on Business Informatics* (pp. 363–366). IEEE. doi:`dx.doi.org/10.1109/CBI.2013.59`.

vom Brocke, J., & Sinnl, T. (2011). Culture in business process management: a literature review. *Business Process Management Journal*, *17*, 357–378.

Calvanese, D., De Giacomo, G., & Montali, M. (2013). Foundations of data-aware process analysis: a database theory perspective. In R. Hull, & W. Fan (Eds.), *Proceedings of the 32nd ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, PODS 2013, New York, NY, USA - June 22 - 27, 2013* (pp. 1–12). ACM.

Cameron, K. S., & Quinn, R. E. (2005). *Diagnosing and changing organizational culture: Based on the competing values framework*. John Wiley & Sons.

Cayoglu, U., Dijkman, R. M., Dumas, M., Fettke, P., García-Bañuelos, L., Hake, P., Klinkmüller, C., Leopold, H., Ludwig, A., Loos, P., Mendling, J., Oberweis, A., Schoknecht, A., Sheetrit, E., Thaler, T., Ullrich, M., Weber, I., & Weidlich, M. (2014). Report: The process model matching contest 2013. In N. Lohmann, M. Song, & P. Wohed (Eds.), *Business Process Management Workshops - BPM 2013 International Workshops, Beijing, China, August 26, 2013, Revised Papers* (pp. 442–463). Springer volume 171 of *Lecture Notes in Business Information Processing*.

Chopra, A. K., Dalpiaz, F., Aydemir, F. B., Giorgini, P., Mylopoulos, J., & Singh, M. P. (2014). Protos: Foundations for engineering innovative sociotechnical systems. In *Proceedings of the 18th IEEE International Requirements Engineering Conference (RE)* (pp. 53–62). Karlskrona, Sweden: IEEE Computer Society.

Cohn, D., & Hull, R. (2009). Business artifacts: A data-centric approach to modeling business operations and processes. *IEEE Data Eng. Bull.*, *32*, 3–9. URL: `http://sites.computer.org/debull/A09sept/david.pdf`.

Decker, C., & Wattenhofer, R. (2013). Information propagation in the bitcoin network. In *P2P* (pp. 1–10). IEEE.

Decker, G., & Weske, M. (2011). Interaction-centric modeling of process choreographies. *Inf. Syst.*, *36*, 292–312.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*, 125–128.

Dumas, M., van der Aalst, W. M. P., & ter Hofstede, A. H. M. (2005). *Process-Aware Information Systems: Bridging People and Software Through Process Technology*. Wiley. URL: `http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0471663069.html`.

Dumas, M., Rosa, M. L., Mendling, J., & Reijers, H. A. (2013). *Fundamentals of Business Process Management*. Springer.

Euzenat, J., & Shvaiko, P. (2013). *Ontology Matching, Second Edition*. Springer.

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In N. Christin, & R. Safavi-Naini (Eds.), *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers* (pp. 436–454). Berlin, Heidelberg: Springer Berlin Heidelberg. URL: `http://dx.doi.org/10.1007/978-3-662-45472-5_28`. doi:10.1007/978-3-662-45472-5_28.

Frantz, C. K., & Nowostawski, M. (2016). From institutions to code: Towards automated generation of smart contracts. In *Workshop on Engineering Collective Adaptive Systems (eCAS), co-located with SASO, Augsburg*.

Gal, A. (2011). *Uncertain schema matching*. Synthesis Lectures on Data Management. Morgan & Claypool Publishers.

García-Bañuelos, L., Ponomarev, A., Dumas, M., & Weber, I. (2017). Optimized execution of business processes on blockchain. In *BPM'17: International Conference on Business Process Management*. Barcelona, Spain.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* CCS '16 (pp. 3–16). New York, NY, USA: ACM. URL: http://doi.acm.org/10.1145/2976749.2978341. doi:10.1145/2976749.2978341.

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, *2*, 24.

Hammer, M., & Champy, J. (1993). *Reengineering the Corporation: A Manifesto for Business Revolution*.

Hull, R., Batra, V. S., Chen, Y., Deutsch, A., III, F. F. T. H., & Vianu, V. (2016). Towards a shared ledger business collaboration language based on data-aware processes. In Q. Z. Sheng, E. Stroulia, S. Tata, & S. Bhiri (Eds.), *Service-Oriented Computing - 14th International Conference, ICSOC 2016, Banff, AB, Canada, October 10-13, 2016, Proceedings* (pp. 18–36). Springer volume 9936 of *Lecture Notes in Computer Science*.

Hurlburt, G. (2016). Might the blockchain outlive bitcoin? *IT Professional*, *18*, 12–16.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 839–858). doi:10.1109/SP.2016.55.

Marin, M., Hull, R., & Vaculín, R. (2012). Data centric BPM and the emerging case management standard: A short survey. In *Business Process Management Workshops, Tallinn, Estonia, September 3, 2012. Revised Papers* (pp. 24–30). Springer.

Mendling, J., & Hafner, M. (2008). From WS-CDL choreography to BPEL process orchestration. *J. Enterprise Information Management*, *21*, 525–542.

Mougayar, W. (2016). The business blockchain: Promise, practice, and application of the next internet technology.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*, 183–187. URL: https://doi.org/10.1007/s12599-017-0467-3. doi:10.1007/s12599-017-0467-3.

Norta, A. (2015). Creation of smart-contracting collaborations for decentralized autonomous organizations. In *BIR'15: International Conference on Perspectives in Business Informatics Research* (pp. 3–17).

Norta, A. (2016). Designing a smart-contract application layer for transacting decentralized autonomous organizations. In *ICACDS'16: International Conference on Advances in Computing and Data Sciences*.

Prybila, C., Schulte, S., Hochreiner, C., & Weber, I. (2017). *Runtime Verification for Business Processes Utilizing the Bitcoin Blockchain*. arXiv report 1706.04404 arXiv. URL: https://arxiv.org/abs/1706.04404.

Ramberg, J. (2011). ICC Guide to Incoterms 2010. ICC.

Reichert, M., & Weber, B. (2012). *Enabling Flexibility in Process-Aware Information Systems - Challenges, Methods, Technologies*. Springer. URL: https://doi.org/10.1007/978-3-642-30409-5. doi:10.1007/978-3-642-30409-5.

Rosemann, M., & vom Brocke, J. (2015). The six core elements of business process management. In *Handbook on Business Process Management 1* (pp. 105–122). Springer.

Shleifer, A., & Vishny, R. W. (1997). A survey of corporate governance. *The journal of finance*, *52*, 737–783.

Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A. B., Weber, I., Xu, X., & Zhu, L. (2017). *Risks and opportunities for systems using blockchain and smart contracts*. Technical Report Data61 (CSIRO), Sydney.

Štemberger, M. I., Buh, B., Glavan, L. M., & Mendling, J. (2017). Propositions on the interaction of organizational culture with other factors in the context of bpm adoption. *Business Process Management Journal*, *23*.

Subramanian, S., Thiran, P., Narendra, N., Mostéfaoui, G., & Maamar, Z. (2008). On the enhancement of BPEL engines for self-healing composite web services. In *Proc. SAINT Symposium* (pp. 33–39).

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

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*.

Tassey, G. (2000). Standardization in technology-based markets. *Research policy*, *29*, 587–602.

Telang, P. R., & Singh, M. P. (2012). Comma: A commitment-based business modeling methodology and its empirical evaluation. (pp. 1073–1080). Valencia, Spain: IFAAMAS.

Tran, A. B., Xu, X., Weber, I., Staples, M., & Rimba, P. (2017). Regerator: a registry generator for blockchain. In *CAiSE'17: International Conference on Advanced Information Systems Engineering, Forum Track (demo)*.

Vanwersch, R. J. B., Shahzad, K., Vanderfeesten, I. T. P., Vanhaecht, K., Grefen, P. W. P. J., Pintelon, L., Mendling, J., van Merode, G. G., & Reijers, H. A. (2016). A critical evaluation and framework of business process improvement methods. *Business & Information Systems Engineering*, *58*, 43–53. URL: https://doi.org/10.1007/s12599-015-0417-x. doi:10.1007/s12599-015-0417-x.

Venkatesh, V. (2014). Technology acceptance model and the unified theory of acceptance and use of technology. *Wiley Encyclopedia of Management*, .

Walport, M. (2016). Distributed ledger technology: Beyond blockchain. *UK Government Office for Science, Tech. Rep*, *19, 2016*.

Weber, I., Haller, J., & Mülle, J. (2008). Automated derivation of executable business processes from choreograpies in virtual organizations. *International Journal of Business Process Integration and Management (IJBPIM)*, *3*, 85–95.

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Mendling, J. (2016). Untrusted business process monitoring and execution using blockchain. In *Business Process Management - 14th International Conference, BPM 2016, Rio de Janeiro, Brazil, September 18-22, 2016. Proceedings* (pp. 329–347). Springer volume 9850 of *Lecture Notes in Computer Science*.

Weske, M. (2012). *Business Process Management - Concepts, Languages, Architectures, 2nd Edition*. Springer. URL: https://doi.org/10.1007/978-3-642-28616-2. doi:10.1007/978-3-642-28616-2.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? – A systematic review. *PLoSONE*, *11*, e0163477.

Zeng, L., Benatallah, B., Ngu, A., Dumas, M., Kalagnanam, J., & Chang, H. (2004). Qos-aware middleware for web services composition. *IEEE TSE*, *30*, 311–327.