Cross-collaboration processes based on blockchain and IoT: a survey

Tiphaine Henry, Nassim Laga, Julien Hatin, Walid Gaaloul, Imed Boughzala

Cross-Collaboration Processes based on Blockchain and IoT: a survey

Tiphaine Henry
Orange Labs
Telecom SudParis,
Institut Polytechnique de Paris
tiphaine.henry@orange.com

Nassim Laga
Orange Labs
nassim.laga@orange.com

Julien Hatin
Orange Labs
julien.hatin@orange.com

Walid Gaaloul
Telecom SudParis
Institut Polytechnique de Paris
walid.gaaloul@telecom-sudparis.eu

Imed Boughzala
Université Paris-Saclay,
Univ Evry, IMT-BS, LITEM,
imed.boughzala@imt-bs.eu

Abstract

Cross-collaboration processes are decentralized by nature and their centralized monitoring can trigger mistrust. Nevertheless, a decentralized monitoring facility such as a blockchain-based and Internet-of-Things-aware (IoT-aware) business process management system can reduce this pitfall. However, concerns related to usability, privacy, and performance, hamper the wide adoption of these systems. To better understand the challenges at stake, this paper reviews the use of blockchain and IoT devices in cross-collaboration processes. This survey sheds some light on standard uses such as model engineering or permissioned blockchains which help adopt cross-collaboration business process management systems. Moreover, with respect to process design, two schools of thought coexist, addressing both constrained and loosely processes. Furthermore, a focus on data-centric processes appears to get some momentum, as many industries go digital. Finally, this survey underlines the need to orient future research towards a more flexible, scalable, and data-aware blockchain-based business process management system.

1. Introduction

Intermediation platforms such as Amazon or Uber are examples of cross-collaboration processes: customers, delivering drivers, and service providers, interact together at different stages of the process. In these settings, contractual trust- the subjective belief that a set of agreements will be fulfilled while respecting a set of constraints (e.g. resource, time, etc.)- is paramount. Trust is embodied by the platform itself: it acts as a mediator in the case of a dispute resolution, it collects the ratings of the clients, it proposes optional insurance, etc. However, these third-party platforms represent added costs for the involved partners. They also create an imbalanced sharing of resources, impede contractual flexibility, and constitute single points of failure that can cause security leakages. The issue has grown in importance in light of recent scandals due to trust abuses that lead to a new working status less socially protected [1, 2]. On the opposite, distributed ledger technologies can offer an alternative to third-party orchestration. By decentralizing cross-collaboration processes, contractual trust is enforced by design; the leadership policy can evolve towards self-governance.

The opportunities linked to the development of IoT-aware blockchain-based BPMS (i.e.Business Process Management Systems) are threefold. Firstly, blockchains can be used as **trustworthy data platforms** [3]. The existence of an immutable public ledger enforces a commonly agreed-upon single source of truth [4, 5]. It eases process monitoring, auditing, and dispute resolution as stakeholder trust improves [6]. For example, in case of a shipment error, the delivery history can be queried with confidence [5]. Secondly, IoT-aware blockchains can be used for the **execution of shared agreements** [7, 4]. With Smart Contracts (SCs), agreed business logic can be openly and confidently enforced: the management of states is distributed and consistent. Moreover, IoT devices can level up the trust and effectiveness of the monitoring facilities in time-critical contexts thanks to continuous sensing and reliable actuation based on IoT feedback loops [8]. Thirdly, **data, and identity privacy** can be enforced with encryption techniques and key management. In an inter-collaborative setting, tenants reveal only what is necessary to the network [5]. The frictions linked

URI: https://hdl.handle.net/10125/71138
978-0-9981331-4-0

to the central execution of choreography process monitoring, in which companies abandon the control of the monitoring to third parties, can consequently be alleviated [9]. Therefore, IoT-aware blockchain-based BPMS pave the way for new trading habits relying on trusted decentralized platforms.

Research has been undertaken on the best ways to model inter-collaborative processes. Several proofs-of-use focus on the execution of business processes on blockchain [10, 11]. However, to the best of our knowledge, there is no comprehensive summary of the use cases and challenges linked to the use of distributed ledger technologies (DLTs) for cross-collaboration processes. This area of research, at the crossroads of BPM, P2P networks, and IoT, is indeed specific to a subset of use cases, oftentimes close to the field of logistics. Thereby, the main objective of this survey is to give a comprehensive overview of the use of the blockchain in cross-collaboration processes. Hence, in this paper, we first propose a categorization framework regrouping the proofs-of-use published in the literature, we then present the main challenges related to the development of blockchain-based BPMS, and we finally compare the identified proofs-of-use with these research challenges and suggest future directions of research.

The remainder of this paper is structured as follows. Section 2 introduces the key concepts related to blockchain-based BPMS. Section 3 presents the method used to build this survey. Section 4 presents the blockchain-based BPMS published in the literature. In Section 5, the challenges that emerge from the analysis of the set of papers are analyzed. An evaluation of the proofs-of-use under the light of the mentioned challenges is proposed in Section 6. These findings are discussed in Section 7. Section 8 concludes the paper with a summary of the results and some considerations on our future work.

2. Background

2.1. Blockchains and Distributed Ledger Technologies (DLTs)

A **DLT** is a distributed database based on a peer-to-peer network, i.e. a database spread across multiple nodes or servers [3]. DLTs keep track of the transfer of assets between multiple parties. They lower the cost of trusted transactions by making databases tamper-proof by design [9].

DLT systems store data transactions hierarchically. At the *transaction level*, accounts keep track of updates [12]. This account-model corresponds to a transaction-based state machine, i.e. each activity changes the state of the involved accounts. Cryptography hashes and asymmetric encryption enforce the non tampering of the transactions. At the *block level*, subsets of transactions are aggregated together. Each block holds (1) the reference to the previous block, (2) a tamper evident digest of the transaction history to attest the integrity and the ordering of the blocks, and (3) the list of the transactions to commit [13]. The type of cryptography block-linkage chosen gives birth to different ledgers. In case of linear linkage, we talk about **blockchains**.

The trusted behavior of blockchain systems builds upon the consensus protocol used to update the chain of blocks, as well as the deterministic scripts (the smart contracts) that can be implemented to propose a given set of services to the users (e.g. launch a transaction under a set of conditions) [7]. On the one hand, **the consensus protocol** states the strategy used by participants to settle on a shared state of truth. This protocol ensures a secured and persistent growth of the database. It fosters the DLT resilience to node failures ([14, 12]). A given protocol ensures that nothing wrong can happen. It processes all the transaction requests, it does not revoke correct committed blocks, and makes possible recovery from faulty nodes [12]. On the other hand, **the smart contracts (SC)** refer to the scripting abilities of DLTs which enact automatic contracts linked to stored assets [15]. For security purposes, at the transaction validation stage, submitted transactions can refer to the SC they were computed with. The miner compiles its own version of the SC and if the obtained output matches with the first transaction, the latter is valid. Applications and services can build on top of SC functionalities [9].

Several identity management and access control schemes characterize DLTs [16]. Public, or permissionless blockchains, do not perform any access control: any user can both submit and mine transactions. Permissioned blockchains set identity guards. In fully private blockchains, only white listed participants can submit and mine transactions, while in consortium blockchains, only a subset of trusted nodes is responsible for mining [14].

2.2. Cyber-physical systems

The integration of devices connected to the internet within the physical world is often called the Internet-of-Things. Sensors, tags, and actuators are spread in the environment; they can sense, monitor, reference items, as well as act on them [17]. Systems merging physical realities and telecom networks are called cyber-physical systems [18]. IoT networks can

Table 1. Search Query Results.

Database	Initial Queries	Filtered Queries
ScienceDirect	316	4
ACM Digital library	54	6
IEEE	25	4
SpringerLink	357	17
AISel	159	6
Total	911	37

Table 2. Identified literature sources.

Zhao et al. 2O19 [22]	Xu et al. 2019 [23]
Park et al. 2019 [24]	Weber et al. 2016 [5]
Brousmiche et al. 2017 [25]	Tran et al. 2018 [26]
Sturm et al. 2019 [27]	Madsen et al. 2018 [28]
Frantz et al. 2016 [29]	Astigarraga et al. 2018 [4]
Meroni et al. 2019 [30]	Falazi et al. 2019 [31]
de Sousa et al. 2020 [32]	Wang et al. 2018 [33]
Bagozi et al. 2019 [34]	

be tuned by varying a given set of service attributes, thereby optimizing business process specifications and compliance checking. The merge of many technological bricks, among them service-oriented architectures, cloud systems, BPMS, or compliance checking [19], paves the way for more ubiquitous manufacturing systems.

3. Methodology

A survey [20] is conducted on the theme of peer-to-peer process monitoring using blockchain and IoT. To get an exhaustive list of blockchain-based BPMS proofs-of-use, we apply a subjective search string to the main databases related to the topic of BPM [21]. We came up with a list of synonyms for each key word (respectively BPM, BC, and IoT), and joined them together into a boolean query. The output search string is *(BPM OR "Business Process Management" OR "Business Process") AND (IoT OR "Internet of Things" OR "Cyber Physiscal Systems" OR Smart) AND (Blockchain OR "Distributed Ledger")*.

We query the main databases related to the topic of BPM with this search string. We remove duplicates and apply the following inclusion criteria: (1) is it a peer-reviewed article? (2) is an empirical study performed? (3) does it mention both blockchain and BPM? We then recursively pursued the related work references included in these papers. Table 1 outlines the number of papers found in each database before and after the inclusion criteria filtering. We get ten papers after removing duplicates. A backward search lead to the retrieval of five more papers. After removing duplicates, the subset of papers kept for further analysis comprises fifteen papers. Table 2 lists the selected peer-reviewed conference or journal articles.

We classify each work using a concept matrix presented by Webster and Watson [20] as a way of systematically collecting and analyzing the different blockchain-based BPMS. Table 4 gathers the results of the analysis.

4. Blockchain-based BPMS: A Synopsis

This section presents existing works related to the topic of decentralized BPMS using blockchain and IoT (cf. Table 2). We analyse these works with respect to the design method used to build these systems, the modelization paradigm, the sequencing of activities, and the use of external services.

4.1. Design method

We categorise the design method used to develop blockchain-based BPMS into two schemes, namely empirical and model-driven schemes.

Several approaches empirically show the usefulness of blockchains for asset management. In these approaches, SCs are developed from scratch and designed according to the business need. For instance, a luxury supply chain [22] mimics an asset monitoring process using a Hyperledger Fabric chaincode (a SC variant) derived from a BPMN collaboration diagram. There, an EPC-based IoT network composed of RFID chips is used to track assets. Similarly, a food delivery process is successfully implemented using a Quorum-based private blockchain [23]. However in both cases, the scalability and privacy challenges come into play. In reaction to these pain-points, block-free directed acyclic graphs, such as IOTA have been proposed [35]. By removing blocks (each new transaction verifies former transactions), miners are removed. By removing miners, the threat of centralization implied by mining pools vanishes. This DLT has been empirically used to trade energy in a peer-to-peer fashion though this architecture increases transaction time [24].

The empirical development of process SCs require strong development skills, the design stage is therefore costly and time-consuming. This issue can be circumvented by abstracting SCs into sublayer stacks [36, 37, 34]. By abstracting the underlying SC code to the eyes of the business modelers, the design process is faster and more reliable [10].

4.2. Sequencing of activities

Both imperative and declarative activity sequencing figure in the proofs-of-use surveyed.

The imperative approach consists of approaching business processes as an ordered sequence of enforceable tasks. BPMN is the standard notation used to depict processes in an imperative fashion. The literature reports two BPMN-based BC monitoring systems. Caterpillar [5] executes business processes fully onchain. Its focus is on control flows: a translator component maps BPMN diagrams into a simplified Petri net translated into Ethereum's Solidity SC. On the execution side, process and party instances are generated. To ensure trust, each involved party computes its own version of the contract, to be compared latter on. At runtime, a local trigger links API calls to blockchain transactions, and process history is stored using IPFS, a decentralized network protocol providing storage facilities [38]. Moreover, data structure optimizations have been implemented to cut execution costs [39, 10]. Similarly, Lorikeet [26] focuses on the mapping of BPMN choreography processes into SCs. Only the message flows between partners are stored onchain. In both Caterpillar and Lorikeet approaches, though at different degrees, security and privacy issues are taken into account: for example through participant binding and asymmetric data sharing [36].

Declarative processes stand in reaction to the limits of imperative and semi imperative processes. Modelization consists of specifying the set of rules to be followed by the process: the sequencing of the tasks is indirectly enforced. One protocol, ADICO, focuses on institutional grammar. On the semantic side, institutions embody behavioral patterns among a group of people. Strategies, rules, and norms, frame these patterns. On the translation side, the semi-automated translation of textual inputs generates SCs [29]. The execution has two facets. First the translation is semi-automatic: the developer can customize the generated SC to prevent deviating cases. Then, SCs are instantiated: they are compiled into an EVM bytecode. The complexity of the contract and the predicted gas consumption are provided to the user before being committed to the blockchain network. Another protocol, BCRL (Business Collaboration Rule Language), focuses on controlled English sequences of the form when-if-then [4, 40]. The user declares the set of business rules to be ingested in a rule parser, which will, in turn, instantiate a RETE algorithm (a pattern-matching algorithm adapted to rule-based systems). A SC hosted on Hyperledger Fabric embeds the rule engine. A dedicated API triggers the engine when needed. Finally, Dynamic Condition Response (DCR) graphs build on declarative event process flows [41, 42, 43, 28]. On the modelization side, each node represents an event. The ordering of the events is made through role assignment (person or machine) and causal or conflictual relationships. The strength of this approach is the ease of modelization, and the flexiblility of process execution paths.

4.3. Modelization paradigm

Process and artifact-centric flows are used to sequence the business processes in the proofs-of-use surveyed. In this section, we focus on the rise of artifact-centric flows.

To address the rise of data-centric processes and increased interleaved constraints, the artifact-centric approach leaves aside the control-flow paradigm [32]. Instead, it sheds light on artifacts, the set of objects used during the process enactment. Pre and post state conditions of the artifacts indicate the completion of an activity. The artifact-centric process modeling rely on the guard-stage-milestone principles. The guards are the set of conditions to be met to trigger a stage activation. The milestones are the set of conditions to be met to settle a stage. The stages are the set of tasks to be executed. Two blockchain-based BPMS implementation of this approach prove the validity of the model [30, 32]. Flexibility and ease of implementation are advocated in both approaches. The degree of implementation varies in both cases. In the first case, the whole pipeline, from the BPMN diagram ingestion, to the runtime execution are proposed. In the second case, the choice of the model and execution schemes are left to the end user: authors propose an interface between the information system and the BP.

4.4. External services

External communication with other blockchains services underline the need for blockchain-based BPMS interoperability.

Blockchain-agnostic BPMS enable companies to combine together the benefits of various technologies, for example permissioned and permissionless blockchains, in the prospect of multi-BC scenarios. Blockchains are approached as external services. In BlockMe2 [31, 44], a blockchain access layer isolates the different ledgers from the BPMS. At the execution level, a subscription and a callback manager organize the interactions between the blockchain and the BPMS. Each ledger and its SCs are triggered using a URI scheme. At the modeling level, a blockchain task is introduced in BPMN diagrams. This task references

the SC function targeted by means of the URI scheme, the parameters needed by the smart contract, and the transaction validation confidence score. The latter provides for transaction durability. Also, timeout and invocation errors trigger alternative flows.

5. Research Challenges

The blockchain technology is an avenue worth exploring for an enhanced business process decentralization. Nevertheless, this technology comes at the expense of added constraints, be it on trust, contractualization, or data and identity privacy. Table 3 states the challenges triggered by the development of blockchain-based BPMS that are outlined in the literature. In this section, we detail each one of these challenges.

5.1. Challenges induced by the blockchain technology

The challenges induced by the blockchain technology relate to the incentive mechanism, the non-reversibility of transaction commits, transaction latency (Table 3).

Trust can be insufficient or very expensive depending on the chosen blockchain-based BPMS design (proof-of-work, proof-of-stake and alike, on-chain and off-chain monitoring, etc) [45]. For example, the on-chain storage of data can be costly compared to cloud-based solutions as many systems use pay-per-instruction mechanisms [46]. Reaching a decentralized trust should come at a reasonable cost in terms of initial and rolling investment, lock-in effect risks[1], privacy compromises, and scalability performance. The latter is even more important when IoT devices are involved in the business process design and implementation as the number of transactions soars proportionally to the monitoring needs. A way to assess the relevance of a blockchain-based BPMS is embodied by decision trees, be it in an IoT setting [47], or in a more general scope [16]. Among the criteria to be checked are the need for decentralization, the existence of a trust issue, and the existence of peer-to-peer exchanges occurring between IoT devices (P2P exchanges occurring between IoT devices are often used for intelligent swarms as well as for computing with local gateways).

The blockchain enforces an irreversible commit of its code [6]. At design time, the SCs should therefore be deployable, that is error-free, compilable, and resistant to attacks. The parallel setup of choreography processes among different peers should also to be tackled [48, 5]. To this end, empirical and formal methods can be used for testing and verification [49]. For example, companies can test and elect trustworthy SC patterns and cryptocurrencies they consider reliable enough for business use [49]. Formal proofs are also being developed on the SC and business modelization sides to prove the soundness of the models [50, 13].

At run time, each process transaction should be executed with a high degree of confidence. It is only at this condition that the following stages can be trustfully enacted. Nonetheless, attacks exist, such as the 51% attack where a party holding at least 51% of the overall mining resources set a tampered version of a branch as the shared truth [51].To reduce this risk of attack, protocols such as the proof-of-work protocol have been proposed [51, 52]. The latter requires each miner to compute an expensive puzzle in order to validate a block. However, as a counter-effect, the validation step takes time. Latencies appear. Such phenomenon can be harmful in a business setting [53] where time is limited. To circumvent this issue, companies are advised to elect a preferred consensus to prevent any degree of conflict of interest among dishonest parties [18]. Moreover, two metrics assess the confidence of execution of a transaction, namely the *rate of effective commits* [49], and the *DoC* (degree of confidence that an attack will fail) [31].

Companies often need to leverage the functionalities offered by a wide spectrum of blockchain systems. For example, permissionless blockchains are useful for auditing purposes or financial deals via cryptocurrency exchange. However, their low scalability is not a good fit for more data intensive processes, or confidential exchanges, issue tackled with permissioned blockchains

Table 3. Overview of the challenges triggered by the development of trusted BPMS.

Challenges	Sub-challenges	Papers
Blockchain	Performance trade-offs	[45, 46, 47, 16]
	Code deployment	[5, 6, 48, 49, 50, 13]
	Transaction durability	[18, 31, 49, 51, 52, 53]
	Multi-BC integration	[18, 31, 53]
Business	User interaction	[4, 6, 29, 36]
	Privity	[25, 49, 54, 55, 51, 52, 53, 56]
	Flexibility	[8, 11, 24, 57, 58, 59, 60, 61, 62]
IoT	Modeling	[27, 63, 64, 65, 54]
	Scalability	[18, 30, 38, 55]

[1]Lock-in effects can occur due to the use of a single blockchain. That is, companies can become dependant to a single type of blockchain, and therefore suffer the limitations of using a single technology.

[53]. The need for integration standards, in a perspective of easier joint-engineering, therefore rises [18, 31]. It nevertheless questions the quality of portability, functionality and decentralization services.

5.2. Challenges induced by the business needs

We identified three challenges induced by the business needs (Table 3): the seamless integration of SCs in BPMS, the privacy-vs-transparency trade-off, process flexibility.

The integration of blockchain functionalities within BPMS depends on the usability of the blockchain technology. The tuning of SCs should be fast, reliable, and comprehensible [4, 36]. However the high diversity of blockchain technologies and the need for strong cybersecurity and development skills for SC development can be overwhelming for the target users of BPMS. Consequently, SCs, which embody process stages, should preferably be integrated in a seamless fashion into BPMS. Their versioning management should also be eased. The separation of the design and implementation stages would therefore help business analysts bridge more easily the barrier linked to development skills, limiting implementation errors and security faux-pas, [6, 29].

The strategic deployment of blockchain-based BPMS requires a trade-off between transparency and privacy. All transactions are not shareable, especially when competitors are involved in the process, sharing their efforts to decrease production and logistic costs [49]. This kind of collaboration is therefore unbalanced as competing partners might use shared data to discover industrial secrets [56]. Thus, there is a need to strike a balance between confidentiality, integrity, and availability of the broadcasted data. Privity, that is, the habit of disclosing information only to the contractual tenants who need to, should be innate [57]. The responsibility of each party for the maintenance of the confidentiality requirements should be acknowledged, though it is not sufficient to ensure a thorough enforcement of privity requirements. Therefore, the asymmetric visibility of the processes within the different users should be stated at design time [58, 25]. An architectural approach to multitenant challenges, for example using permissioned blockchains, can answer the needs for "data privacy and performance isolation" [59]. Zero-knowledge-proof architectures could also enable partners to reach an agreement without requiring partners to share their monitoring secrets: in this setting, off-chain and non-interacting proofs attest the execution of transactions [60, 61].

The need for ad-hoc, on the run, modifiable processes is motivated by the will to ease knowledge work processes [62, 66]. blockchain-based BPMS should therefore provide monitoring facilities for these processes. Research efforts focus on the development of new model standards, that is event-based or declarative [11, 67]. These approaches are claimed to be more convenient to link data and process flows. The decreased model complexity eases the understandability and the maintainability of the process pipeline [68]. IoT-dedicated blockchain-based BPMS frameworks are being developed in this direction [8]. For transaction-intensive processes, alternative distributed ledger architectures can be taken into account, such as directed acyclic graphs [24]. Other investigation paths are the ease of change at runtime [69], heterogeneous data integration [70].

5.3. Challenges induced by the IoT

We identified two challenges related to the IoT: a lack of IoT-awareness in BPMS, and a latent need to scale BPMS to transaction-intensive processes (Table 3).

Blockchain-based BPMS should be resource-aware in the context of IoT-based industrial pipelines [27]. Such awareness is motivated by the need to tune each device according to specific energy consumption schemes, or privacy policies. To this end, a semantic mapping of IoT and process variables has been proposed [63]. Notations such as BPMN or BPEL have also been extended with an IoT layer, BPMN using a UML profile with stereotypes [64] and BPEL for the orchestration and choreography of IoT devices [65]. Additionally, the behavior of IoT devices (activity assignment, data replication and shareability) can be tuned according to the business needs [54].

The shared transaction focus of DLTs and modern industrial supply chains motivates the coupling of DLTs and BPMS. Nevertheless, such flow impacts the number of blocks to be validated before being committed to the blockchain. The combination of IoT and blockchain-based BPMS can hamper the overall system performance, as the broadcasting of the transactions and blocks to the whole network lowers the scalability of the system [55]. To counterbalance this effect, side-chains can be used to reduce and smooth the computing load [30]. IPFS [38] or cloud storage [55] can decrease the costs of storing data onchain. Proof-of-stake and alike can also make the protocol lighter: the consensus algorithm, which ensures the validation of new transactions, can be an adjustment variable for a more responsive network [18]. Indeed, it plays a crucial role with respect to the latency and scalability of a given system.

6. Comparison

In this section, we compare the BPMS proofs-of-use that leverage blockchain capabilities against the criteria detailed in the *challenges* section. Table 4 compares the aforementioned proofs-of-use. The framework columns summarize the works with respect to the categorization proposed in Sect. 4.

The blockchain challenges are evaluated with respect to cost optimization, execution correctness, transaction durability and multi-blockchain integration. *Regarding cost optimization*, the execution of SCs is realized off-chain in [5, 28, 25]. Both off and on chain processing are proposed in [4]. Off and on chain storage are chosen in [23, 26, 30, 34]. *Regarding execution correctness*, the majority of the presented works adopts a model engineering approach. A preliminary verification step of the models to be translated into SCs deals with the verifiability issue. The correct execution of SC schemes is oftentimes ensured by the use of templates that are empirically checked by the developers of the BPMS. *Regarding transaction durability*, a dedicated confidence of execution threshold can be set to control the sequences to be executed [31]. This work is developed for public blockchains where malicious behaviours can more often occur. The other BPMS studied thus do not take into consideration this confidence of execution challenge. Indeed, the use of permissioned blockchains implicitly decreases the fear of a risk of attacks among the tenants. Again, *regarding multi-blockchain integration*, the proof of service of [31] is to be noticed. Multi-blockchain integration is not addressed in the remaining analyzed prototypes. In these works, mono-blockchains are considered as internal facilities for the execution of process stages. Preliminaries to chose the most adequate blockchain for a given use case often appear.

The BPMS challenges are evaluated with respect to usability, privacy and flexibility. *Regarding usability*, and barring the empirical works of [22, 23, 24, 33], model-driven engineering appears as a standard for blockchain-based BPMS development. A concern for an ease of use for business modelers end-users appears as a common explanatory factor for this design scheme. Usability is approached with a different lens in [31]. The latter externalises blockchain services and encourages multi-blockchain interactions. *Regarding privacy*, the asymmetric key encryption is enforced as it is one of the key building blocks of the DLT protocols. The majority of use cases also implement a permissioned ledger to limit privacy leakage risks. Finally, role-based access control appears mainstream to enforce legal requirements. One paper [24] implements key encryption only as it targets a public use, and therefore a public blockchain. Another [31] offers the same service only, as it considers the blockchain as an external service to exchange with. Role-based access control is not addressed in this work. *Regarding process flexibility*, two modelization schools can be distinguished in the literature. The first one, the oldest, focuses on imperative control-flows. BPMN schemes, used as a standard of notation, provide an activity-centric view. In parallel, GSM schemes provide a data-centric view. The second school of thought, not yet unified, wagers on flexible notations. Among the supported notations are DCR, ADICO, or BCRL.

The IoT challenges are evaluated with respect to model integration and system scalability. *Regarding IoT integration*, sensor devices are introduced in four of the identified works. Three domain-based adhoc implementations demonstrate the feasibility of IoT integration within blockchain-based BPMS. It is to note that [30] is the first paper that intends to provide IoT integration with a model engineering approach. These works however underline scalability issues that an architectural change could tackle [24]. *Regarding scalability*, the notion of acceptable scalability is mentioned in [23]. In this work, Quorum is judged as the best fit for the minimum performance requirements of agricultural pipelines. The IOTA architecture is also explored in [24]. The use of additional platforms such as IPFS and other offchain storage is also advocated in several works [10, 26, 30]. Finally, the scalability challenge can be delegated by considering the blockchain as an external service in [31].

7. Discussion

In this paper, the current efforts devoted to building blockchain-based cross-collaboration BPMS have been broken down into four analytical perspectives. The identified implementations are classified based on the design method, the sequencing of activities, the modelization paradigm, and the use of external services (cf Section 4).

To the question, on what conditions may cross-collaboration processes using blockchain be trusted?, the survey underlines nine challenges. The development of decentralized cross-collaboration processes depends on the degree of **blockchain-based BPMS adoption** within companies. The latter should find appropriate use cases for decentralized trust, and the blockchain technology should be seamlessly integrated in their information systems. Furthermore, the elaboration of **secured execution mechanisms**, translated in terms of verifiability, transaction durability,

Table 4. Assessment of the surveyed papers with respect to BC, business, and IoT maturity. (E/M = Empirical/Model-driven, I/D = Imperative/Declarative, A/P = Artifact/Process-centric).

Papers	Framework			BC/ DLTs				BPMS			IoT	
	Design Method	Sequencing of activities	Modelization	Cost optimization	SC correctness	Durability	Interoperability	Usability	Privacy	Flexibility	IoT-awareness	Scalability
[22]	E	I	A	-	-	-	-	-	x	-	x	-
[23]	E	I	A	x	-	-	-	-	x	-	x	x
[24]	E	I	A	-	-	-	-	-	-	-	x	x
[5]	M	I	P	-	x	-	-	x	x	-	-	x
[25]	M	I	P	-	x	-	-	x	x	-	-	-
[26]	M	I	P	x	x	-	-	x	x	-	-	-
[27]	M	I	P	-	x	-	-	x	x	-	-	x
[28]	M	D	A	x	x	-	-	x	x	x	-	-
[29]	M	D	A	-	x	-	-	x	x	x	-	-
[4]	M	D	A	x	x	-	-	x	x	x	-	-
[30]	M	I	P	x	x	-	-	x	x	x	x	x
[31]	M	I	P	-	x	x	x	x	-	-	-	+/-
[34]	M	I	P	x	-	-	-	x	-	x	-	-
[33]	E	I	P	-	-	-	-	x	x	-	-	-
[32]	M	-	A	-	x	-	-	x	x	x	-	-

and data privacy is necessary to circumvent any system mistrust. Moreover, scaling the process management capacities to intensive data flows appears as an **industrial requirement**. Blockchain-based BPMS should answer real life constraints related to IoT management, and transaction scalability. The integration of cyber-physical systems into BPMS is for now hindered by the absence of standardized IoT modelizations into BPMS, as well as by mainstream DLTs' performance limitations. Finally, the remaining challenges underline a gap of BPMS support for both **flexible** and **data-intensive** processes.

The generalization of these findings may be hindered by the small number of publications retrieved. The search string and the selection process may have excluded studies not mentioning the terms queried, thus the small subset of literature studies found. Moreover, a non negligible proportion of blockchain applications developed in the private sector are not published in the literature. Finally, our selection criteria were oriented towards peer-reviewed papers and empirical implementations. The disparity of experiments proposed -from a process execution to the study of task latency- makes it hard to propose a detailed and thorough evaluation. As research on blockchain-based BPMS progresses, a more objective and thorough evaluation of the system trust should be systematically performed by comparing quantitatively and qualitatively the proposed platform to former studies.

8. Conclusion and Future work

In this paper, we investigated the literature maturity with respect to trusted, blockchain-based BPMS. For this purpose, we conducted a survey aiming to determine the challenges linked to trusted decentralized process monitoring, identify the proofs-of-use developed in the literature and compare them to outline existing research gaps. This survey shows that: (i) blockchain-based BPMS proofs-of-use focus on usability and simplicity of use by means of model engineering, (ii) a paradigm shift towards data-centric processes emerges in the literature, (iii) the declarative approach, which aims towards the simplification of the modeling stage, and the flexibility of the process execution, has not been standardized yet, (iv) the inclusion of IoT data flows is still on the go, be it with respect to adequate modelizations, or system scalability, (v) multi-blockchain integration, which is paramount in order to gather the potential of each blockchain, is still to be included in blockchain-based BPMS. Our future work is motivated by the latent need for tools adapted to data-centric processes. For example, in the context of smart logistics, one should be able to monitor the temperature of a truck during the delivery stage, and flexibly trigger invoices or dispute cases according to the values monitored. Our research will focus on the modelization challenges related to flexibility, usability, and IoT-awareness. To this end, we aim to implement a resource and IoT-aware, model-driven, declarative-based BPMS. More particularly, we plan on building our platform with a DCR-based approach. As research direction guidelines for the development of blockchain-based BPMS, we foresee the need for more flexibile, scalable, and data-aware BPMS.

References

[1] K. Hara et al., "A data-driven analysis of workers' earnings on amazon mechanical turk," *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2017.

[2] A. A. Casilli and J. Posada, *The Platformization of Labor and Society*, pp. 293–306. Oxford University Press, 2019.

[3] H. Wang et al., "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, p. 352, 2018.

[4] T. Astigarraga et al., "Empowering business-level blockchain users with a rules framework for smart

contracts," in *Service-Oriented Computing*, pp. 111–128, Springer, Cham, 2018.

[5] I. Weber et al., "Untrusted business process monitoring and execution using blockchain," in *Business Process Management*, pp. 329–347, Springer, Cham, 2016.

[6] R. Hull, "Blockchain: Distributed event-based processing in a data-centric world: Extended abstract," in *Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems*, DEBS '17, pp. 2–4, ACM, 2017.

[7] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

[8] C. Janiesch et al., "The internet-of-things meets business process management: Mutual benefits and challenges," *arXiv:1709.03628 [cs]*, 2017.

[9] J. Mendling et al., "Blockchains for business process management - challenges and opportunities," *ACM Transactions on Management Information Systems*, vol. 9, no. 1, pp. 1–16, 2018.

[10] O. López-Pintado et al., "CATERPILLAR: A business process execution engine on the ethereum blockchain," *arXiv:1808.03517 [cs]*, 2019.

[11] J. Mendling, "Artifact-driven process monitoring: Dynamically binding real-world objects to running processes," *CAiSE 2017 Forum and Doctoral Consortium*, 2017.

[12] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[13] A. Singh et al., "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Computers & Security*, vol. 88, p. 101654, 2020.

[14] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, EuroSys '18, (New York, NY, USA), 2018.

[15] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[16] K. Wüst and A. Gervais, "Do you need a blockchain?," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 45–54, 2018.

[17] I. Mistry et al., "Blockchain for 5g-enabled IoT for industrial automation: A systematic review, solutions, and challenges," *Mechanical Systems and Signal Processing*, vol. 135, p. 106382, 2020.

[18] L. D. Xu and W. Viriyasitavat, "Application of blockchain in collaborative internet-of-things services," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1295–1305, 2019.

[19] V. Pureswaran, "The business of things: Designing business models to win in the cognitive IoT," p. 24, 2015.

[20] J. Webster and R. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quarterly*, vol. 26, 06 2002.

[21] H. Zhang et al., "Identifying relevant studies in software engineering," *Information and Software Technology*, vol. 53, no. 6, pp. 625–637, 2011.

[22] R. Zhao, "An empirical analysis of supply chain BPM model based on blockchain and IoT integrated system," in *Web Information Systems and Applications*, pp. 539–547, Springer, Cham, 2019.

[23] X. Xu, I. Weber, and M. Staples, *Case Study: AgriDigital: Blockchain Technology in the Trade and Finance of Agriculture Supply Chains*, pp. 239–255. Springer International Publishing, 2019.

[24] J. Park, R. Chitchyan, A. Angelopoulou, and J. Murkin, "A block-free distributed ledger for p2p energy trading: Case with IOTA?," in *Advanced Information Systems Engineering*, pp. 111–125, Springer, Cham, 2019.

[25] L. Mercenne et al., "Blockchain studio: A role-based business workflows management system," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 1215–1220, 2018.

[26] A. B. Tran et al., "Lorikeet: A model-driven engineering tool for blockchain-based business process execution and asset management," in *BPM*, 2018.

[27] C. Sturm et al., "A blockchain-based and resource-aware process execution engine," *Future Generation Computer Systems*, vol. 100, pp. 19–34, 2019.

[28] F. Madsen et al., "Collaboration among adversaries: Distributed workow execution on a blockchain," in *Symposium on Foundations and Applications of Blockchain*, p. 8, 2018.

[29] C. K. Frantz and M. Nowostawski, "From institutions to code: Towards automated generation of smart contracts," in *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*, pp. 210–215, 2016.

[30] G. Meroni et al., "Trusted artifact-driven process monitoring of multi-party business processes with blockchain," in *Business Process Management: Blockchain and Central and Eastern Europe Forum*, pp. 55–70, Springer, Cham, 2019.

[31] G. Falazi et al., "Process-based composition of permissioned and permissionless blockchain smart contracts," in *2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC)*, pp. 77–87, 2019.

[32] V. A. De Sousa et al., "B-merode: A model-driven engineering and artifact-centric approach to generate blockchain-based information systems," in *International Conference on Advanced Information Systems Engineering*, pp. 117–133, Springer, 2020.

[33] Z. Wang et al., "Distributed ledger technology for document and workflow management in trade and logistics," in *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*, pp. 1895–1898, 2018.

[34] A. Bagozi et al., "A three-layered approach for designing smart contracts in collaborative processes," in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pp. 440–457, Springer, 2019.

[35] M. Divya and N. B. Biradar, "Iota-next generation block chain," *International Journal of Engineering and Computer Science*, vol. 7, pp. 23823–23826, 2018.

[36] C. Di Ciccio et al., "Blockchain support for collaborative business processes," *Informatik Spektrum*, 2019.

[37] M. Kurz et al., "Leveraging CMMN for ACM: Examining the applicability of a new OMG standard for adaptive case management," in *Proceedings of the 7th International Conference on Subject-Oriented Business Process Management*, S-BPM ONE '15, pp. 4:1–4:9, ACM, 2015.

[38] S. Krejci et al., "Blockchain- and ipfs-based data distribution for the internet of things," in *Service-Oriented and Cloud Computing - 8th IFIP WG 2.14 European Conference, ESOCC 2020, Proceedings*, Springer, 2020.

[39] L. García-Bañuelos et al., "Optimized execution of business processes on blockchain," *arXiv:1612.03152 [cs]*, 2016.

[40] R. Hull et al., "Towards a shared ledger business collaboration language based on data-aware processes," in *Service-Oriented Computing*, vol. 9936, pp. 18–36, Springer International Publishing, 2016.

[41] T. Hildebrandt et al., "Declarative event-based workflow as distributed dynamic condition response graphs," *Electronic Proceedings in Theoretical Computer Science*, vol. 69, pp. 59–73, 2011.

[42] T. Slaats, "Flexible process notations for cross-organizational case management systems," 2015.

[43] S. Debois et al., "Concurrency and asynchrony in declarative workflows," in *International Conference on Business Process Management*, vol. 9253, pp. 72–89, 08 2015.

[44] G. Falazi et al., "Modeling and execution of blockchain-aware business processes," *SICS Software-Intensive Cyber-Physical Systems*, vol. 34, no. 2, pp. 105–116, 2019.

[45] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[46] P. Rimba et al., "Quantifying the cost of distrust: Comparing blockchain and cloud services for business process execution," *Information Systems Frontiers*, 2018.

[47] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[48] G. Meroni et al., "Combining artifact-driven monitoring with blockchain: Analysis and solutions," in *Advanced Information Systems Engineering Workshops*, pp. 103–114, Springer, Cham, 2018.

[49] I. Weber, "Software architecture and engineering for blockchain- based applications," *Symposium on blockchain and distributed ledger technology, UNSW Sydney*, p. 38, 2017.

[50] I. Weber, "Beyond soundness: On the semantic consistency of executable process models," in *In 6th IEEE European Conference on Web Services*, pp. 12–14, 2008.

[51] M. Vukolić et al., "The quest for scalable blockchain fabric: Proof-of-work vs. bft replication," in *Open Problems in Network Security*, (Cham), pp. 112–125, Springer International Publishing, 2016.

[52] A. Gervais et al., "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, p. 3–16, 2016.

[53] G. Falazi et al., "Transactional properties of permissioned blockchains," *SICS Software-Intensive Cyber-Physical Systems*, 2019.

[54] K. Suri et al., *Configurable IoT-Aware Allocation in Business Processes*. SCC 2018: Services Computing, 2018.

[55] A. Dorri et al., "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, 2017.

[56] C. Klinkmüller et al., "Mining blockchain processes: Extracting process mining data from blockchain applications," in *Business Process Management: Blockchain and Central and Eastern Europe Forum*, pp. 71–86, Springer, Cham, 2019.

[57] J. Köpke et al., *Balancing Privity and Enforceability of BPM-Based Smart Contracts on Blockchains*, pp. 87–102. BPM 2019: Business Process Management: Blockchain and Central and Eastern Europe Forum, 08 2019.

[58] G. Meroni et al., "Multi-party business process compliance monitoring through IoT-enabled artifacts," *Information Systems*, vol. 73, pp. 61–78, 2018.

[59] I. Weber et al., "A platform architecture for multi-tenant blockchain-based systems," in *Preprint*, 2019.

[60] J. Groth, "On the size of pairing-based non-interactive arguments," in *EUROCRYPT 2016*, pp. 305–326, 05 2016.

[61] J. Eberhardt and S. Tai, "Zokrates - scalable privacy-preserving off-chain computations," in *2018 IEEE International Conference on Internet of Things*, pp. 1084–1091, 2018.

[62] T. Davenport, "Thinking for a living: How to get better performance and results from knowledge workers," *Boston, Mass.: Harvard Business School Press*, 2005.

[63] S. Schönig et al., "An integrated architecture for IoT-aware business process execution," *Enterprise, Business-Process and Information Systems Modeling*, pp. 19–34, 2018.

[64] R. Petrasch and R. Hentschke, "Process modeling for industry 4.0 applications: Towards an industry 4.0 process modeling language and method," in *2016 13th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, pp. 1–5, 2016.

[65] I. Machorro-Cano et al., "IoT services orchestration and choreography in the healthcare domain," *Techniques, Tools and Methodologies Applied to Global Supply Chain Ecosystems*, pp. 429–454, 2020.

[66] R. Hull and H. R. M. Nezhad, "Rethinking BPM in a cognitive world: Transforming how we learn and perform business processes," in *Business Process Management*, pp. 3–19, Springer, Cham, 2016.

[67] C. D. Ciccio et al., "Knowledge-intensive processes: Characteristics, requirements and analysis of contemporary approaches," *Journal on Data Semantics*, vol. 4, no. 1, pp. 29–57, 2015.

[68] D. Fahland et al., "Declarative versus imperative process modeling languages: The issue of maintainability," in *Business Process Management Workshops*, pp. 477–488, Springer, Berlin, Heidelberg, 2009.

[69] W. Fdhila et al., "Dealing with change in process choreographies: Design and implementation of propagation algorithms," *Information Systems*, vol. 49, pp. 1–24, 2015.

[70] X. Liu et al., "Elastic and cost-effective data carrier architecture for smart contract in blockchain," *Future Generation Computer Systems*, vol. 100, pp. 590–599, 2019.