Towards an Understanding of Trade-Offs Between Blockchain and Alternative Technologies for Inter-organizational Business Process Enactment

Martin Kjäer(✉), Thomas Preindl, and Wolfgang Kastner

TU Wien, Karlsplatz 13, 1040 Wien, Austria
{martin.kjaer,thomas.preindl,wolfgang.kastner}@tuwien.ac.at

Abstract. Several studies have proposed the application of blockchains in Inter-organizational Business Processes (IOBPs), primarily citing the technology's immutability, trust, and transparency as motivating factors. However, there is a notable lack of detailed comparisons between traditional, non-blockchain-based architectures and those incorporating this new technology. Such a comparison is critical for practitioners like software architects to fully comprehend blockchain-based solutions' strengths and their potential trade-offs and suitable scenarios for alternative technologies. This paper endeavors to bridge this knowledge gap by contrasting the attributes of public and private blockchains with those of Trusted Third Parties (TTPs) and Electronic Data Interchange (EDI) – the latter being a widespread method for automated data exchange between organizations. We underscore less explored advantages of blockchains, such as the ability to provide non-equivocation. Conversely, we identify that TTPs offers lower complexity levels and superior flexibility.

Keywords: BPM · blockchain · trusted third party · EDI · architectural concerns · trade-off analysis

1 Introduction

IOBPs have been affected by digital disruption for decades. First, by introducing EDI and proprietary communication networks, and later by the Internet in combination with modern Business Process Management Systems (BPMS). In recent years, the use of blockchains[1] has been considered and several publications in the business process management community have proposed novel architectures which make use of them.

Due to their nature, public blockchains provide some unique qualities which are hard to achieve otherwise. Overarching is the ability to provide a trustable

[1] Blockchains are a particular type of Distributed Ledger Technology (DLT). For the sake of simplicity, we will only use the term 'blockchain'.

J. Köpke et al. (Eds.): BPM 2023, LNBIP 491, pp. 36–50, 2023.
https://doi.org/10.1007/978-3-031-43433-4_3

state machine, whereby trust is achieved through a high degree of decentralization and introducing an incentive-aligned system, ensuring that rational actors behave as expected [17]. Until recently, for use cases requiring the highest level of trust, the use of a TTP was the best possible solution. As the name suggests, TTPs are chosen when a neutral and reliable entity is needed, which behaves [...] *in a well-defined way that does not violate agreed-upon rules, policies, or legal clauses* [...] [11, p. 7].

Measuring trust is, however, not easy and even if various methods have been developed, they are mainly assessed with the help of interviews and are also hardly used in practice [14]. Trust in an external system can be enhanced through various techniques such as audits, monitoring, and a comprehensible governance structure. Nevertheless, Singer and Bishop [19] go a step further and argue that trust should be considered harmful in the first place and thus minimized wherever possible. Blockchains cannot solve the trust problem per se, as humans will need to interact with them. As long as humans are responsible for signing certain transactions to trigger some action on-chain, the risks connected to the off-chain protection mechanisms that prevent the user from getting tricked into signing something unintentional remains.

However, when employed correctly, blockchains do have the potential to enhance specific guarantees connected to trust. One of them is non-equivocation, which is essential for use cases that require a high level of security [22]. An example where equivocation is problematic is the misuse of trust in certificate authorities (CAs). These have the power to distribute different certificates pointing to the same domain, which happened, e.g., to Google before [2]. Blockchains can solve this issue, as shown by Tomescu and Devadas [22].

Blockchains also provide benefits in the field of IOBPs as they allow trustless execution without the need for a trusted intermediate. However, when designing a system for IOBP enactment, deciding whether to include a blockchain within the BPMS architecture remains challenging. Several sources propose the use of blockchains in this domain when trustability, transparency, or immutability is required [24, Chapter 8], [13]. While these quality attributes are undoubted, we argue that deciding whether to use a blockchain in a BPMS also depends on many other aspects and requires the careful analysis of trade-offs between several concerns.

This work aims to move these concerns to center stage and to contribute towards a common understanding of the influencing factors and how they relate. Our contribution thus aims to provide value to software architects and assist them in making better design decisions. Furthermore, this work adds to research direction 5 of Mendling et al. on opportunities and challenges in this domain [15, p. 4:13]: "*Developing techniques for identifying, discovering, and analyzing relevant processes for adopting blockchain technology. Researchers will have to investigate which characteristics of blockchain as a technology best meet the requirements of specific processes.*"

1.1 Related Work

Van der Aalst [23] contributes to understanding interoperability in IOBPs, mainly focusing on the concept of *capacity sharing*. Stiehle and Weber [20] provide a comprehensive view of business process enactment using blockchains. They introduce a taxonomy that distinguishes between supported capabilities and enforced guarantees, enriching the understanding of enactment facets. Also, Garcia-Garcia et al. [9] conducted a systematic literature review on collaborative business process management using blockchain.

Multiple authors have explored challenges and opportunities in this domain. Mendling et al. [15] provide a broad overview related to the use of blockchains, while Breu et al. [5]. specify four types of general challenges: Flexibility, correctness, traceability, and scalability. Architectures and threat mitigation are other aspects covered in the literature. Ordoñez-Guerrero et al. [16] conduct a systematic mapping study on architectural concerns, and Colwill [8] delves into the concern of insider threats, highlighting the limits of technical mitigation. Trust, a crucial element in this field, is examined by McEvily et al. [14], who summarize different trust measures and their practical application.

1.2 Chosen Approach

The set of possible solutions that aim to tackle challenges in IOBP enactment is significant. Therefore, to explore the trade-offs between blockchain-based architectures and their alternatives, we categorize them into distinct technology groups for comparison. To facilitate a comparison between these groups, we employ architectural concerns, which we subdivide into three categories:

1. Challenges in IOBPs that have been defined by Breu et al. [5]
2. Concerns that are related to blockchain-based architectures
3. Concerns related to TTPs

The challenges related to IOBPs as defined in [5] are flexibility, correctness, traceability, and scalability. Even for traditional technologies such as EDI, these are not easy to address; therefore, we argue that including them in our analysis adds value. Concerns related to blockchain-based architectures are mainly connected to the drawbacks of public blockchains. We choose to include privacy, transaction costs, and finality in our analysis, as these are well-known issues that are also not easy to address [20]. Finally, we include non-equivocation and insider threat prevention, concerns related to TTPs. We include them to foster the discussion of trade-offs connected to the main competitor (TTPs).

The rest of this work is structured as follows: The succeeding section includes a brief overview of EDI, a technology group focused on automating electronic business document exchange. EDI is the technology that is used when no TTP is employed for enactment of IOBPs. In Sect. 3, we briefly describe the other groups of technologies which tackle the challenges mentioned above. In Sect. 4, we discuss the described architectural concerns and trade-offs between technology groups. In the discussion (Sect. 5), we summarize our findings and briefly discuss the next steps.

2 EDI as Alternative to TTPs and Blockchains

Besides the challenges that TTPs and the different types of blockchains aim to address, EDI has enabled the automation of IOBPs for decades. We include this well-established technology group in our work for completeness, mainly because they provide some interesting, sometimes overlooked capabilities. In particular, when considering the use of blockchains for IOBP, we argue that in the first instance, however, it should be carefully evaluated whether the features of a TTP or an EDI-based system are not sufficient. This section briefly discusses EDI and which concerns it can tackle.

Due to various standardization efforts, EDI formats such as UN/EDIFACT[2] or UBL[3] are widely used and allow companies to exchange business documents such as purchase agreements or invoices in an electronic and automated manner. For communication, different messaging standards exist to ensure the secure exchange of business documents whereby several techniques such as message integrity verification, digital signatures, and Public Key Infrastructure (PKI) are used: Message integrity verification provides the ability to verify that electronic messages containing business documents have not been changed during transmission or when stored.

This is guaranteed by using cryptographic hash functions, which are a means to calculate the hash of a message before digitally signing it using electronic signatures. Given that the identity of the sender is undeniably connected to the public key,[4] the receiver can verify that received message has not been tampered with and originates from the expected party. This feature is comparable to transactions on a blockchain, which are also identified by their cryptographic hash value. However, compared to blockchains, where each participant can verify that a transaction has not been modified, EDI uses the concept of messages being exchanged only between individual participants.

Non-repudiation of Origin. Besides the capability of message integrity verification as well as sender authentication, the described mechanisms also provide another guarantee: The content of electronic business documents becomes non-repudiable. This property is also known as *non-repudiation of origin* and allows the receiver of a message in case of a dispute with the sender to prove evidence to a third party that a sender transmitted a particular message [25]. This guarantee makes another business partner liable for the actions taken and does not require any more advanced technology other than the described ones.

[2] https://unece.org/trade/uncefact/introducing-unedifact.
[3] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ubl.
[4] This is usually solved by making use of PKI, but also other approaches such as Decentralized Identifiers (DIDs) exist.

3 Technology Groups for Inter-organizational Business Process Enactment

Technologies for secure IOBP enactment can be grouped into several categories. In this section, we present how we group them together with an overview of these groups. We include public- and private chains, commonly used as differentiation in the blockchain domain. To consider the growing sector of scaling solutions for blockchains, we also include so-called *Layer 2* solutions. TTPs have been added as they remain the main competitor of blockchains due to their trust offering.

3.1 Public Blockchains

Public blockchains such as Bitcoin or Ethereum offer publicly viewable data structures and trustless execution of transactions. As their name suggests, they are a public good and allow anyone to interact with them if a transaction fee is paid for their use. We follow a blockchain-agnostic approach – instead of discussing specific properties of blockchains (Proof-of-Work vs. Proof-of-Stake, etc.), we assume that the following non-functional properties, which have been described by Xu et al. [24] hold: *non-repudiation*, *integrity*, *transparency* and *immutability* of stored data as well as *equal rights*, which describes that every actor that wishes to access or manipulate the blockchain is allowed to do so.

Furthermore, we assume the following properties to be given:

- Programmability, i.e., the possibility to define smart contracts, which are executed on-chain[5]
- High degree of decentralization, nodes are distributed across many actors and nation-states
- High economic security so that fraudulent behavior such as double spending[6] becomes economically unattractive

3.2 Layer 2 Blockchain Solutions

Scalability of public blockchains is a challenge, which is not easy to solve, at least when the decentralization and security properties should be noticed [10]. One possibility to tackle this issue is the use of layer 2 solutions. Development in this segment has steadily progressed and several designs have been tried. The most promising ones are rollups, which maintain their own state machines but aim to derive the security guarantees of their connected 'base' layer, i.e., a public blockchain. [21]. This is achieved by using the base layer as a data availability layer, which stores an ordered list of all layer 2 transactions without executing them. With the transactions, rollup providers also publish a commitment of the updated rollup state. At this point, two different designs are used, which we briefly describe here.

[5] This property is only supported by second-generation blockchains such as Ethereum.
[6] In a double spending attack, a malicious actor attempts to spend owned tokens twice, e.g., by enforcing the re-ordering of already finished blocks.

Zero Knowledge Rollups. These types of rollups employ Zero Knowledge (ZK) proof schemes to calculate proofs of correct execution of new transactions. A smart contract deployed on layer 1 verifies this proof, which accepts it only if it is correct. The on-chain verification of state updates on layer 1 is the most critical aspect of this design, even if it requires higher complexity due to the use of ZK proofs. Due to the high costs of on-chain verification of ZK proofs, there is a trade-off between fast settlement and low transaction fees. Therefore sequencers only create proofs for batches of transactions to distribute the cost of verification.

Optimistic Rollups. In contrast to ZK rollups, optimistic rollups commit only the state root of the rollup, but no proof of correct execution. This design requires external actors to verify if a newly published state root is correct. They can do so by executing all new transactions before comparing the calculated new state root of the rollup with the claimed state root published on-chain. An external actor can publish a so-called fraud-proof in case of a deviation, which is then automatically verified on-chain [21]. If the fraud-proof is correct, the sequencer, the node that maintains the rollup, has to pay a penalty fee, and the state machine of the layer 2 solution gets *rolled back* to the point before the incident.

3.3 Private Blockchains

Private blockchains have emerged as an alternative design approach after public blockchains became popular. Compared to their public pendant, they can only be advanced by a group of known participants that maintain it, which is the reason why private blockchains are also named permissioned blockchains. The advantages of private blockchains are that only the chain's contributors have access, which is why the concept has been especially interesting for business use cases. Furthermore, the nodes of a private blockchain can use professional server infrastructure. That means that throughput is only limited by server expenses, and transaction fees can be kept low, which are further advantages for businesses.

3.4 Trusted Third Party

A TTP can act as an intermediary and coordinate processes between multiple parties. Interoperability is enabled through *capacity sharing* and several entities make use of a centralized workflow manager [23]. For example, some of the largest and most trusted entities, which execute financial workflows, so-called Real-Time Gross Settlement System (RTGS) platforms, can be named. These systems, which central banks typically operate, execute transactions between banks on behalf of their customers.[7] Besides these highly payments-specialized systems, many other systems exist for other use cases, ranging from generic trustable BPMS service providers to use-case-specific implementations.

[7] An example for an RTGS is *T2* of the European Central Bank (ECB): https://www.ecb.europa.eu/paym/target/.

4 Architectural Concerns

This chapter analyzes different architectural concerns and how they relate to the technologies discussed in the previous section. In Table 1, we include selected technology groups (in columns) as well as the selected architectural concerns (in rows). It is important to note that the assessment does not claim completeness. Instead, it should indicate whether a specific concern can be addressed better or worse by a given technology group and how that relates to other technology groups.

We base the estimation shown in Table 1 on our argumentation, which forms the remainder of this chapter. For each concern, the scaling is adjusted relatively between the individual technology groups between zero and four points. This means that each concern has at least one technology group with a value of zero points and one with a value of four points. The table also shows ranges (visualized with hatched circles), as in some cases, the ability to address an architectural concern depends heavily on specific design decisions. An example is privacy on public blockchains: most public blockchains do not offer privacy natively, so if no other arrangements are made, everyone has visibility of all transactions. Nevertheless, sophisticated privacy protection mechanisms exist that leave only small amounts of metadata on the blockchain. In this case, we show a range from zero (no privacy protection) to three (privacy protection, but metadata left on the blockchain).

4.1 Flexibility

Achieving flexibility in IOBPs is challenging and requires carefully designing systems capable of responding to extraordinary situations. An example of flexibility is, e.g., the ability to adapt a process instance due to an allergic reaction of a patient in a treatment process within a hospital [18, Chapter 3]. For processes that require strict enactment, such as enforcing the compliance to anti-money laundering provisions, flexibility needs to guarantee that changes to the process or a process instance follow specific rules so that the process is still compliant after the change [18, Chapter 10]. These examples show how complexity increases when flexibility needs to be implemented correctly.

For IOBPs that are enacted by utilizing a public blockchain, flexibility presents an even more complicated issue: As application code on public blockchains is by default immutable, flexibility is hard to achieve in that context. Any necessary changes in the behavior have to be foreseen at the development time and reconfiguration capabilities have to be explicitly included in the application.

The same holds for layer 2 solutions as these instances are also designed to operate as intended, so every form of flexibility must be provided at design time. Also, in the case of private chains, the same level of flexibility can be achieved, with one exception: If an agreement between the participating parties can be achieved, it becomes possible to update the blockchain, which means that even historic transactions could be changed retroactively.

Table 1. Architectural concerns and how different groups of technologies can address them. More filled circles mean that the technology group is more capable of tackling the concern. Additional hatched circles show a range, with the minimum being the last filled circle (if there is any) and the maximum being the last hatched circle.

Architectural Concern \ Technology Group	Public Blockchains	Layer 2 – ZK Rollups	Layer 2 – Optimistic Rollups	Private Blockchains	Trusted Third Parties (TTPs)	Electronic Data Interchange (EDI)
Concerns Related to IOBPs [5]						
Flexibility	⊘⊘○○	⊘⊘○○	⊘⊘○○	●●●○	●●●○	●●●●
Correctness	●●●●	●●●●	●●●●	●●●○	●●○○	○○○○
Traceability	●●●●	●●●●	●●●●	●●○○	●●○○	○○○○
Scalability	○○○○	●●○○	●●○○	●●●⊘	●●●●	●●●●
Concerns Related to Blockchains						
Privacy	⊘⊘⊘○	⊘⊘⊘○	⊘⊘⊘○	●●⊘○	●●●○	●●●●
Transaction Costs	○○○○	●●○○	●●○○	●●●○	●●●○	●●●●
Finality	●●○○	●○○○	⊘○○○	●●●○	●●●●	●●●●
Concerns Related to TTPs						
Non-equivocation	●●●●	●●●●	●●●●	●●●○	●●○○	○○○○
Insider Threat Prevention	●●●○	●●●○	●●●○	●●●○	●○○○	○○○○

In the case of TTPs, flexibility depends on the willingness and capability of the TTP. Since the unique selling point of a TTP is *literally* trust, all types of flexibility need to be defined upfront.

We summarize that all listed technology groups need to consider the flexibility of process enactment at design time, with public blockchains and layer 2 solutions being the technology groups that are the least forgiving if flexibility is not properly considered during design time. An exception to this statement are EDI solutions, as they provide only the data exchange layer between the local BPMS and the external actors. This setup allows to adapt flexibility internally, which cannot be achieved by the other technology groups.

4.2 Correctness

Achieving correctness of IOBP enactment is another challenge that is hard to tackle, especially when many parties are involved in a process [5]. In the case of public blockchains, the correct enactment of an IOBP can be guaranteed, given that the process is correctly implemented on-chain. Transactions sent to the blockchain advance the state of the process engine on-chain and are only

accepted if they follow pre-defined rules. Adapting a process that stores its state on-chain becomes possible only if governance mechanisms or alternative explicit possibilities have been implemented to enable such a change. This presents, however, also a correct evolvement, as these kinds of capabilities have to be provided before deployment.

Layer 2 solutions also provide correct execution guarantees, as only valid layer 2 transactions are accepted on layer 1 (in the case of ZK-rollups) or eventually finalized (in the case of optimistic rollups). That means that correct enactment of an IOBP, which uses a layer 2 solution, can be assured. Private blockchains can enforce correctness within their closed group of participants. This means they provide lower guarantees than public blockchains, which do not restrict their set of participating nodes. Compared to private blockchains, the correctness of process enactment on a TTPs depends on the capabilities of this single external party. Correctness, therefore, indirectly relates to the level of trust associated with the TTP. In the case of EDI solutions, correctness can only partly be guaranteed, e.g., with non-repudiation of origin. Other guarantees, such as *non-repudiation of receipt* or *non-repudiation of delivery*, require a third external party [25].

4.3 Traceability

Due to the distributed enactment of IOBPs, traceability presents a subsequent stumbling block, as processes are spanned across many companies. Not every party of a more extensive process receives and sees all necessary events [5]. Since public blockchains offer the possibility that anyone can investigate all transactions, they provide a suitable answer to this problem.[8] As the ledger is also immutable, public blockchains guarantee that process traceability is also provided retrospectively for parties not involved during process enactment.

Layer 2 solutions provide the same properties, as their transactions are accessible to anyone, finalized on a public blockchain and therefore also offer immutability. Compared to that, private blockchains cannot grant the same level of traceability, as transactions are only shared between the approved participants that maintain it. This means that traceability is only offered to these parties, while external actors must trust the consortium. TTPs are very similar in this respect, as they make data available to all parties with access rights. Similarly, like with correctness, EDI solutions offer only limited possibilities due to the abovementioned reasons.

4.4 Scalability

Public blockchains, which follow the principle of maximal decentralization, deliberately restrict transaction throughput whereby computational resources are spared. This maxim allows more participants to operate a blockchain node that

[8] At this point, we neglect the concern of privacy, which is discussed in Sect. 4.5.

verifies and stores all blockchain transactions and allows increased decentralization and higher security. Obviously, for enacting IOBPs on public blockchains, this presents a significant obstacle since only the use cases that can operate under these limited resources can be implemented.[9]

In contrast, layer 2 solutions are, at the time of writing, able to achieve a throughput that is approximately two orders of magnitude higher than their base layer [21]. This represents a significant advantage compared to public chains, even if scalability is still limited (approx. 3000 transactions per second [21]). It is important to note that this figure refers to the throughput of only one rollup, with multiple rollups in operation on a public blockchain. It remains to be seen if these metrics can be further increased, as research in this field is only a few years old. In contrast, private blockchains, TTPs and EDI solutions do not share the issue of artificially restricted throughput with their competitors. Scalability is thus only restricted by the limits of hardware and software components but not by other factors, representing a significant advantage over the other technology groups.

4.5 Privacy

Privacy is a necessary pre-condition for almost all electronic business communication use cases. These range from the desire of companies not to disclose their purchase prices to legal prohibitions concerning antitrust law [12]. Most public chains do not natively support privacy, as their ledger of transactions is not encrypted. Privacy-preserving solutions such as zero-knowledge proof schemes,[10] which can be built on top of them have the potential to tackle this problem. However, they also have drawbacks, as they demand higher computational resources and imply higher complexity levels. Research on this topic is ongoing and mainly focused on increasing performance [7].

As their name suggests, private chains allow better protection for privacy, as the blockchain itself is not publicly accessible. This increases privacy substantially, but the participants that maintain the blockchain can still view the transactions of all parties. For most companies, this is an issue they cannot accept, which is why different designs have been proposed to overcome this issue by establishing an additional private environment between actors that is only linked to the private chain [6].

TTPs provide a high level of privacy, as data is only shared with parties that have been granted access explicitly and EDI solutions allow even higher levels of privacy since information is only shared between the parties that necessarily need the information (compared to TTPs).

[9] Aside from the risk of inducing higher transaction costs if the application requires a substantial part of these resources.

[10] It is essential to note that privacy based on zero knowledge should not be confused with zero knowledge *rollups*, which usually do not provide privacy, even if they are based on the same group of technologies.

4.6 Transaction Costs

Transaction costs can be a significant drawback for using IOBP enactment on public blockchains. As previously shown, some blockchains have become very expensive and fee prices can be highly variable [20], both serious business issues.

In contrast, private blockchains and TTPs are substantially better, as they are only limited by computational and infrastructure costs. Private blockchains have a disadvantage compared to TTPs, as several instances need to operate computational infrastructure, whereas a TTP only needs to host one instance. Nevertheless, for use cases requiring the highest security standards, the costs of a TTP might be considerable due to the system's complexity and security requirements. E.g., the previously mentioned Real Time Gross Settlement (RTGS) system of the European Central Bank charges up to EUR 0.8 per transaction, which is an amount that is much higher than any other high-volume transactional [3]. This example highlights the importance of the required security level, which impacts the willingness to pay higher transaction fees.

4.7 Finality

Reaching transaction finality presents an issue connected to distributed systems, especially public blockchains. Finality in the context of blockchains describes the point in time when a previously proposed block cannot be removed from the canonical chain of blocks anymore. Different blockchains offer different types of finality (deterministic or probabilistic [4]), but the issue cannot be removed completely, as the need to reach consensus remains.

This issue is worse for optimistic rollups, as the finality can only be reached after a longer time, during which fraud proofs can be submitted [21]. Therefore, this more extended time period presents an intentional design decision necessary for the system to function. The only possibility to lower this time period is if a full copy of the optimistic rollup is maintained and verified locally. The independent off-chain execution of all transactions provides the ability to verify the correctness of the updated state root and thus to identify de-facto finality before fraud proofs can be submitted.

ZK rollups, in contrast, provide finality once the ZK proof gets published on the layer 1 blockchain. This provides an advantage compared to optimistic rollups Independent from the specific implementation, all rollups lag behind their connected layer 1 blockchains and thus require longer to reach finality.

Lower finality times can only be offered by all other technology groups (private blockchains, TTPs and EDI solutions). Private chains have a minor disadvantage compared to the other two technologies, as they also need to reach consensus within the set of nodes.

4.8 Non-equivocation

Due to their logically centralized yet organizationally decentralized data structures [1], public blockchains offer good protection against equivocation. ZK

rollups provide similar guarantees, as transactions are verified on layer 1 once the proof is submitted. This contrasts optimistic rollups, where state updates are published optimistically and opens a short time window (until a fraud proof gets published), where equivocation would theoretically be possible.

Private chains can also be considered to tackle this issue, as equivocation would require that the participating nodes collude. Nevertheless, collusion is easier to achieve in private blockchains than in an architecture that is based on a public blockchain. Compared to that TTPs don't require any form of consensus between multiple nodes when storing and distributing data. Unfortunately that also makes equivocation easier, as the TTP could deliver different versions of the data to different participants. To prevent such a Byzantine behaviour, participants could gossip messages received from the TTP in order to detect this type of attack. Nevertheless, these kind of techniques require significant additional networking and are not easy to apply in practice [22]. EDI message exchange protocols don't provide non-equivocation protection natively, so any more advanced capabilities such as consensus or gossiping of exchanged messages would need to be added on the application layer.

4.9 Insider Threat Prevention

Insider threats are a challenge related to TTPs that is not easy to overcome. They can partly be mitigated by employing technical control mechanisms such as access control or allowing only minimum privilege [8]. All technically possible security precautions should be applied, especially in areas where the highest security standards are required due to potentially disastrous outcomes in case of an insider attack. Public and private blockchains, as well as layer 2 blockchains, all provide some possibilities to defend against insider threats: Everything encoded on-chain (in smart contracts or enshrined in the blockchain protocol) will be executed as defined. This capability provides the parties that are interacting with an application hosted on-chain with the guarantee that operations that are not permitted on-chain will not be executed. However, it is still necessary to employ high security controls such as minimal access to all off-chain components. Blockchains (public and private) and layer 2 blockchains cannot mitigate these risks.

Compared to blockchain-based architectures, TTPs have fewer capabilities to protect themselves against insider threats. As they act as a single source of truth, a malicious insider can, if all other security precautions are overcome, manipulate information. At the same time, external parties may not be able to notice it. Depending on the use case, these kinds of manipulations may pose a severe risk. EDI solutions do not provide protection mechanisms against insider threats, as they are usually not the technology of choice for use cases that require high security between several businesses (where TTPs are usually chosen).

5 Discussion

Our analysis sheds light on various architectural concerns related to technology groups in the field of IOBP enactment. We identified several implications associated with certain architectures. One of them is that a BPMS that makes use of public blockchains requires the design of systems with higher levels of complexity, e.g., to address the need of flexibility as this presents an issue that can't be added after on-chain deployment. The same holds true for layer 2 solutions, which at least offer some relief in regards to transaction costs and scalability. Nevertheless this novel technology also induces higher complexity and dependencies, as new components (rollups) as well as additional actors (sequencers) have to be added.

One of the objectives of this work is to provide software architects with a means to identify trade-offs between different technology groups in the area of IOBP enactment. Table 1 summarizes our findings and offers a first step towards this vision. Our approach does not only cover well-known drawbacks of blockchain-based solutions, such as privacy or transaction costs, but also concerns related to TTPs, such as insider risks or the risk of equivocation. We argue that our approach enriches the discussion by placing the emphasis on these specific capabilities which are only indirectly related to the more generic quality attribute *trust*.

In addition to the architectural concerns discussed, practical aspects such as technology maturity must also be considered when choosing the most appropriate architecture. EDI solutions and TTPs are the most mature technology groups in our comparison, as a set of EDI standards and also well-established TTPs exist. On the other hand, e.g., ZK- or optimistic rollups are still relatively early, even if they might hold great future potential. Both public- and private blockchains fall in between, although they are more early-stage in maturity.

Finally, we argue that conventional technologies such as EDI should be moved closer to the center of the discussion of blockchain-based architecture for IOBP enactment. These technologies are well-established in the industry and will likely be around for longer. Including them in the discussion adds value, especially for industry experts and practitioners.

Limitations and Future Work. Our approach does not claim completeness about the selected architectural concerns. Also, the estimation of how well these architectural concerns can be addressed by the discussed technology groups (Table 1) is not based on metrics. However, we plan to include metrics related to concerns in future works.

Furthermore, some solutions that tackle challenges in this domain do not fit in our technology groups (e.g., if only commitments of an off-chain BPMS are published on a public blockchain). However, considering all possible architectures is beyond the scope of this work and provides an opportunity to expand upon it in future contributions. We also plan to extend our approach by including further architecturally relevant concerns such as composability or service uptime.

6 Conclusion

Enactment of IOBPs is challenging due to several influencing factors, ranging from a lack of standardization and automation to technical limitations that prevent adoption. Various literature sources argue that a need for increased transparency, trust, and immutability are reasons for employing blockchains in this field. Our analysis of architectural concerns and trade-offs between them goes beyond the state of the art by including concerns related to the field of IOBPs as well as concerns connected to specific technologies that aim to tackle some of the challenges of this domain. We also move traditional systems such as TTPs and EDI into the spotlight and compare them against blockchain-based solutions. We identify several critical issues, such as the need for complex setups when a certain level of flexibility is required in a blockchain-based architecture. Overall, our work is the first step towards a more holistic approach to architectural concerns in this domain.

Acknowledgements. This research has been partially supported and funded by the Austrian Research Promotion Agency (FFG) for the research project "DiCYCLE – Reconsidering digital deconstruction, reuse and recycle processes using BIM and Blockchain" under the contract number 886960.

References

1. Bitcoin: Clarifying the foundational innovation of the blockchain. https://continuations.com/post/105272022635/bitcoin-clarifying-the-foundational-innovation-of. Accessed 04 May 2023
2. Further improving digital certificate security. https://security.googleblog.com/2013/12/further-improving-digital-certificate.html. Accessed 4 May 2023
3. TARGET services pricing guide. https://www.ecb.europa.eu/paym/target/consolidation/profuse/shared/pdf/ecb.targetservicespricingguide_v1.0.en.pdf. Accessed 04 May 2023
4. Anceaume, E., Del Pozzo, A., Rieutord, T., Tucci-Piergiovanni, S.: On finality in blockchains. In: 25th International Conference on Principles of Distributed Systems (OPODIS 2021). Dagstuhl Publishing (2022)
5. Breu, R., et al.: Towards living inter-organizational processes. In: 2013 IEEE 15th Conference on Business Informatics, pp. 363–366 (2013)
6. Brotsis, S., Kolokotronis, N., Limniotis, K., Bendiab, G., Shiaeles, S.: On the security and privacy of hyperledger fabric: challenges and open issues. In: 2020 IEEE World Congress on Services (SERVICES), pp. 197–204 (2020)
7. Capko, D., Vukmirovic, S., Nedic, N.: State of the art of zero-knowledge proofs in blockchain. In: 2022 30th Telecommunications Forum (TELFOR). IEEE (2022)
8. Colwill, C.: Human factors in information security: the insider threat - who can you trust these days? Inf. Secur. Tech. Rep. **14**(4), 186–196 (2009)
9. Garcia-Garcia, J.A., Sánchez-Gómez, N., Lizcano, D., Escalona, M.J., Wojdyński, T.: Using blockchain to improve collaborative business process management: systematic literature review. IEEE Access **8**, 142312–142336 (2020)
10. Halpin, H.: Deconstructing the decentralization trilemma. In: Proceedings of the 17th International Joint Conference on e-Business and Telecommunications. SCITEPRESS (2020)

11. Baseline identity management terms and definitions: Standard. ITU-T, Geneva, CH (2021)
12. Kim, K., Justl, J.M.: Potential antitrust risks in the development and use of blockchain. J. Taxation Regul. Finan. Inst. **31**(3), 5–16 (2018)
13. Ladleif, J., Weske, M., Weber, I.: Modeling and enforcing blockchain-based choreographies. In: Hildebrandt, T., van Dongen, B.F., Röglinger, M., Mendling, J. (eds.) BPM 2019. LNCS, vol. 11675, pp. 69–85. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26619-6_7
14. McEvily, B., Tortoriello, M.: Measuring trust in organisational research: review and recommendations. J. Trust Res. **1**(1), 23–63 (2011)
15. Mendling, J., et al.: Blockchains for business process management - challenges and opportunities. ACM Trans. Manage. Inf. Syst. **9**, 1–16 (2018)
16. Ordoñez-Guerrero, A.C., Muñoz-Garzon, J.D., Roberto Dulce Villarreal, E., Bandi, A., Ariel Hurtado, J.: Blockchain architectural concerns: a systematic mapping study. In: 2022 IEEE 19th International Conference on Software Architecture Companion (ICSA-C), pp. 183–192 (2022)
17. Pass, R., Seeman, L., Shelat, A.: Analysis of the blockchain protocol in asynchronous networks. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10211, pp. 643–673. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56614-6_22
18. Reichert, M., Weber, B.: Enabling Flexibility in Process-Aware Information Systems. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30409-5
19. Singer, A., Bishop, M.: Trust-based security; or, trust considered harmful. In: New Security Paradigms Workshop 2020, pp. 76–89. ACM (2021)
20. Stiehle, F., Weber, I.: Blockchain for business process enactment: a taxonomy and systematic literature review. In: Marrella, A., et al. (eds.) BPM 2022. LNBIP, vol. 459, pp. 5–20. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-16168-1_1
21. Thibault, L.T., Sarry, T., Hafid, A.S.: Blockchain scaling using rollups: a comprehensive survey. IEEE Access **10**, 93039–93054 (2022)
22. Tomescu, A., Devadas, S.: Catena: Efficient non-equivocation via bitcoin. In: 2017 IEEE Symposium on Security and Privacy (SP), pp. 393–409 (2017)
23. van der Aalst, W.M.: Process-oriented architectures for electronic commerce and interorganizational workflow. Inf. Syst. **24**(8), 639–671 (1999)
24. Xu, X., Weber, I., Staples, M.: Architecture for Blockchain Applications. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-03035-3
25. Zhou, J., Gollmann, D.: Evidence and non-repudiation. J. Netw. Comput. Appl. **20**(3), 267–281 (1997)