BPMS Blockchain Technology Soft Integration For Non-Tamperable Logging

Johannes Loebbecke[1], Thomas van Loo[2], Juergen Mangler[1], Zhendong Ma[3], Tomáš Pitner[4], and Stefanie Rinderle-Ma[1]

[1] Technical University of Munich, TUM School of Computation, Information and Technology, Garching, Germany
{firstname.lastname}@tum.de
[2] vanloo.thomas@yahoo.com
[3] Luxoft / DXC Technology, Germany
zhendong.ma@plus.ai
[4] Masaryk University, Faculty of Informatics, Brno, Czech Republic
pitner@muni.cz

Abstract. In contemporary business process management (BPM), the need for secure and transparent interactions between organizations is paramount. Integrating business process management systems (BPMS) with blockchain technology can offer protection against malicious actors and increase trust, e.g., in process mining results, by allowing organizations to share execution traces and associated information. However, hard integration approaches, which we define as execution of processes on the blockchain as smart contracts, have not found widespread application. A hard integration approach, e.g., by utilizing a BPMN to solidity compiler as Caterpillar, has a high barrier of entry since it requires a company to restructure its infrastructure and processes, especially pertaining to potential immutability of smart contracts, and the integration of outside information through oracles. In this work, we instead want to explore a soft integration approach, which allows companies to continue using their existing BPMS infrastructure and integrate blockchain technologies without having to change the overall architecture of the system. The goal is to produce distributed non-tamperable logs, created through the use of private blockchains, serving as basis for compliance checking and, thus, secure and trustworthy execution. In this work, we present two soft integration approaches, which are discussed, implemented, and evaluated regarding their integration complexity and performance. The results suggest that a soft integration approach of blockchain technology can enhance the reliability and traceability of existing BPM systems with low integration effort, thus pointing towards a path for high acceptance within organizations.

Keywords: BPMS, Non-Tamperable Logging, Hyperledger Fabric, Processes and Mining, Blockchain Technology Integration

1 Introduction

Since the conception and deployment of Bitcoin [14], adoption of blockchain technology has been on the rise [2]. Blockchain technology provides an immutable ledger without having to rely on a central authority to maintain data integrity. In contemporary business process management (BPM), the need for enhanced security and transparency between organizations is paramount. Accordingly, there has been widespread interest from both academia and industry to integrate blockchain technology into Business Process Management Systems (BPMS) [4, 12]. The immutable nature of a blockchain's ledger allows observing the process execution and, subsequently, the creation of trustworthy, non-tamperable logs, which store the execution history of processes, including API calls, responses, and data exchanges.

In a traditional system, the execution log is created by a central authority, which becomes a single point of failure and makes it susceptible to tampering by malicious actors. However, for a process that includes multiple business partners, trust among these partners and the accuracy of recorded process transactions is paramount [12]. Furthermore, a tamper-proof log also ensures that malicious actors which interfere with process execution tracking, can not cover their tracks by manipulating execution logs. The popularity of process mining technology [5], including the inclusion of sensor data for process analysis and optimization, further increases the need for trust in execution logs [10, 11].

However, while these advantages are well known, blockchain technology is not widely integrated with, or used for process management. Currently, Business processes are often supported and enacted through traditional Business Process Management Systems (e.g, Camunda[5], Tim Solutions[6], Aristaflow[7], . . .). BPMS allow organizations to design, model, execute, and monitor processes via modeling tools, as well as to integrate with other enterprise systems, simulation engines, execution engines, visualization, and optimization tools. We identified two different approaches in which blockchain technology can be integrated into Process Management Systems: (1) the process itself is stored and executed on the blockchain (like, Caterpillar[8]) or (2) a traditional BPMS (like Camunda) is utilized for modeling and execution, while transaction information is stored on the chain. We call (1) a hard integration approach and (2) a soft integration approach. While (1) requires a paradigm shift in how processes are executed and relies on a separate and different engine, (2) allows to partially and gradually support blockchain technology and continue to utilize existing engines.

For this paper, we discuss the potential of the soft integration approach. For this purpose we analyzed different contributions that applied blockchain technology to BPM problems and implemented two different soft integration prototypes using the Hyperledger Fabric[9] and the Cloud Process Execution Engine CPEE[10]. The different prototypes are evaluated regarding their integration complexity and performance. The results suggest that a soft integration approach allows for the creation of tamperproof logs

[5] `https://camunda.com`, last access 2024-05-2024
[6] `https://tim-solutions.de/`, last access: 2024-04-10
[7] `https://artistaflow.com`, last access: 2024-04-10
[8] `https://github.com/orlenyslp/Caterpillar`, last access: 2024-04-10
[9] `https://hyperledger.org/projects/fabric`, last access: 2024-04-10
[10] `https://cpee.org/`, last access: 2024-05-28

without significant integration complexity and sufficient performance. The complete Implementation details can be found in the Github Repository [11].

The remainder of this paper is structured as follows: in Sect. 2 related work is discussed. In Sect. 3 the properties of hard and soft integration approaches are elaborated in detail. In Sect. 4 considerations regarding the implementation of a soft integration approach are discussed, including the selection of private blockchains and how they allow for different execution scenarios. Finally, in Sect. 5, we discuss the performance of the soft integration approach, as well as its performance properties regarding certain design decisions. The paper concludes with a summary of findings and proposed future work (see Sect. 6).

2 Related Work

While the implementation of cryptocurrencies has led to widespread interest in blockchain technology due to its influence on the financial industry, both academia and industry have been exploring applications in other fields. BPM entails the design, execution, monitoring, and optimization of business processes. In contemporary business process management, the need for enhanced security and transparency amongst inter-organizational process executions is paramount. Accordingly, there has been significant interest in integrating BPMS with blockchain technology.

In 2020, Garcia et al. [4] conducted a systematic literature review of blockchain technology in collaborative business processes. The authors used the methodology proposed by Kitchenham [6] to identify 34 papers addressing BPM using blockchain technology. Out of these studies, 71% are conceptual and theoretical proposals describing how blockchains could be integrated with process management and what advantages and challenges such an integration has. The authors concluded that, while interest of the scientific community is growing, current integration efforts are still in early stages.

Another systematic literature by Stiehle et al. [15] focuses on technical contributions for blockchain integration. They identified 30 studies, out of which they found that 86 percent enforced control flow on the chain which indicates a hard integration approach. Furthermore, they specifically highlight that current integration efforts struggle with flexibility and scalability, due to the immutable nature of the blockchain and performance limitations imposed by the consensus mechanism. In contrast, our approach tries to tackle exactly these two challenges, and thus improve industry acceptance.

The challenges and opportunities for the intersection of BPM and blockchain technology are extensively discussed by Mendling et al. [12], especially regarding inter-organizational processes. They present various technical challenges, including throughput, latency, and bandwidth. As major opportunities, they state three main advantages that blockchain integration can bring: (1) A blockchain acts as an immutable ledger that serves as a trustworthy transaction history for all involved parties. (2) Smart contracts can ensure compliance with the process and offer independent global monitoring. (3) Blockchain technology allows for easy encryption to limit data readability for contexts where such a restriction is necessary.

[11] `https://github.com/thomasvloo/fabric-testnet`, last accessed: 2024-04-10

A soft integration approach is presented by Li et al. in [7]. They present the architecture of their proposal without implementation details, which blockchain network can potentially be used, or which required or delivered performance characteristics their solution has. For their approach, blockchain technology is loosely coupled with the process engine. Each operation conducted by the engine is logged by a separate component to create data reliability and secure transactions between process tasks and connected services. Compared to the approach presented in this paper, Li et al. propose only a single transaction for interaction between the engine and a connected service. Thus data tampering can only be confirmed when a global view is assumed, not independently from the engine's perspective and a potential partner (represented by the connected service).

A major research stream is focused around hard integration with the Caterpillar platform described and developed by López-Pintado et al. [9]. Caterpillar [12] is an open-source business process management system running on the Ethereum Blockchain [13]. Caterpillar provides functionality similar to traditional BPMSs, allowing users to model and execute instances of business process, but additionally uses the Ethereum network to preserve the execution instances on the blockchain and handle workflow routing. The Solidity smart contracts are generated using a BPMN-to-Solidity compiler to represent the workflow routing logic of given process models. Subsequently, an on-chain execution engine is used to deploy these models and create immutable execution logs. Several contributions have extended the Caterpillar project, such as [8] and [13]. López-Pintado et al. [8] proposed dynamically relating actors with collaborative business processes and generating smart contracts to verify role restrictions. Meanwhile, Ercenne et al. [13] outline Blockchain Studios as an extension of Caterpillar, with a focus on process models based on human tasks to incorporate role restrictions. Their hard integration approach allows creation of immutable logs as well as secure and transparent process execution, however, it requires organizations to adapt their entire process management infrastructure and additionally involves significant operating costs due to the use of transaction fees on the Ethereum Platform.

A similar tool, Lorikeet, is presented by Tran et al. [16]. Like Caterpillar, Lorikeet includes the translation of BPMN models to Solidity smart contracts while also incorporating a registry data schema. They also describe a backend component to compile, deploy and interact with the generated smart contract, however low level implementation details are not addressed. Compared to Caterpillar, Lorikeet supports fewer BPMN elements but supports asset control and participation selection [3]. Conclusively, Lorikeet focuses on generating and deploying smart contracts in Solidity from BPMN models, however, it also requires organizations to adapt their existing BPMS leading to a high integration effort, and is not backend agnostic, since Solidity is not used by every blockchain.

Alves et al. [1] present a softer integration approach using the process orchestration platform Camunda and the permissioned blockchain network Hyperledger Fabric [14]. The processes are modeled and executed using the Camunda BPMS, while smart con-

[12] `https://github.com/orlenyslp/Caterpillar`, last access: 2024-04-09
[13] `https://ethereum.org/en/`, last access: 2024-05-27
[14] `https://www.hyperledger.org/projects/fabric`

tracts on the Hyperledger network are used to register and manage generated information. Javascript clients and Hyperledger SDKs are used to integrate the smart contracts with the Camunda outputs. This contribution addresses the soft integration approach and creates immutable data logs of process executions. However, technical details of the implementation are not presented and evaluated. Furthermore, their approach creates additional risks in introducing special proxy services between the process engine and the called services, which are responsible for communicating with the blockchain. Thus, again, tampering might occur before data arrives at the proxy service, and it is hard to confirm by the connected components.

Conclusively, the majority of contributions are theoretical or focused on hard integration, while there are only a few soft integration implementations. However, we argue that a soft integration approach has several advantages, which are presented in the following section.

3 Hard vs. Soft Integration

While integrating blockchain technology with BPMS has clear advantages (e.g., decentralized non-tamperable logging) and disadvantages (e.g., integration effort) regardless of how it is implemented, different integration approaches lead to additional advantages and disadvantages. This section presents advantages and disadvantages of using a soft integration approach, where modeling and execution is handled by a traditional BPMS, compared to a hard integration approach, where processes are stored and executed on the chain. The analysis of both approaches is summarized in Table 1.

Soft Integration	Hard Integration
+ Immutable Execution Log	+ Immutable Execution Log
+ Improved Security	+ Strong Security
+ Improved Compliance Assurances	+ Strong Compliance Assurances
+ Advantages of BPMS (editable, etc)	– Immutable processes
+ Low integration complexity	– High integration complexity
+ Low additional infrastructure costs	– New infrastructure costs
– Additional complexity in process engine	– Trusted triggers needed
– Engine/Communication needs to be secured	

Table 1: Advantages and Disadvantages of Soft and Hard Integration. *Improved* is in comparison with no blockchain integration, while *Strong* can be regarded as stronger than *Improved*

3.1 Hard Integration

For the hard integration approach, the processes are stored and executed on the chain. A major advantage of blockchain technology, the immutable nature of the chain also leads to a major disadvantage for a hard integration approach: The immutable nature of the chain also means that deployed smart contracts, which in the hard integration approach represent the processes, can not be paused, edited nor continued without violating the non-tamperable control flow by allowing migration of the process into a new smart contract. For many domains, an executable business process requires many implementation iterations and a major advantage lies in how it can be easily extended to deal with changes and unforeseen circumstances. Furthermore, additional complexity is added by deploying processes on the chain, and organizations have to adjust their entire infrastructure to work with the chain. Finally, while a purpose of blockchain integration is to increase security and trust among process partners, a hard integration approach leads to additional security vulnerabilities since the triggers (or oracles) that use information from outside the chain have to be trusted.

The advantages of the hard integration approach are the creation of non-tamperable logs and better compliance assurances due to unchangeable processes as long as the triggers are trusted.

3.2 Soft Integration

For the soft integration approach, the processes are modeled, executed, and monitored with a traditional Business Process Management System. This means the advantages of a modern BPMS are kept: processes can be stopped, modified, and continued from their previous execution state. However, it still retains the main advantage of the hard integration approach since a non-tamperable log can be created on the chain. Furthermore, a soft integration approach also comes with additional advantages, most notably, the simpler and less costly integration. Furthermore, for a collaborative process, not all partners have to participate in the blockchain and smart contracts can still be used for independent compliance checking.

If private blockchains are used, the soft integration approach's main disadvantage is added complexity in the process or the process engine (depending on the exact implementation) for initializing the chain and passing info to a chain communication component or direct invocation of chain smart contracts. Furthermore, the process engine and any intermediate components between the process engine and blockchain can be regarded as new single points of failure that need to be secured. A final limitation of the soft integration approach is, that it does not directly enable tamper-proof execution, but only tamper-proof logging, which ensures non-repudiation and traceability.

For soft integration, we propose the two approaches depicted in Fig. 1. If a process engine supports creating transactions in a ledger (Fig. 1(a)), then every execution of an activity for a particular instance leads to a transaction 2 that contains all the data that is sent to the implementation of the activity (e.g., a service). The service itself creates its own transaction 3, that contains both the received data and the data returned to the process engine. After receiving the data, the process engine again creates a transaction 4 with the data it received. 1 represents an optional interaction between the network and the process engine, that potentially initializes the ledger.

The smart contract can check if the data has not been tampered with by having separate transactions 2-4. This approach, of course, assumes a secure connection

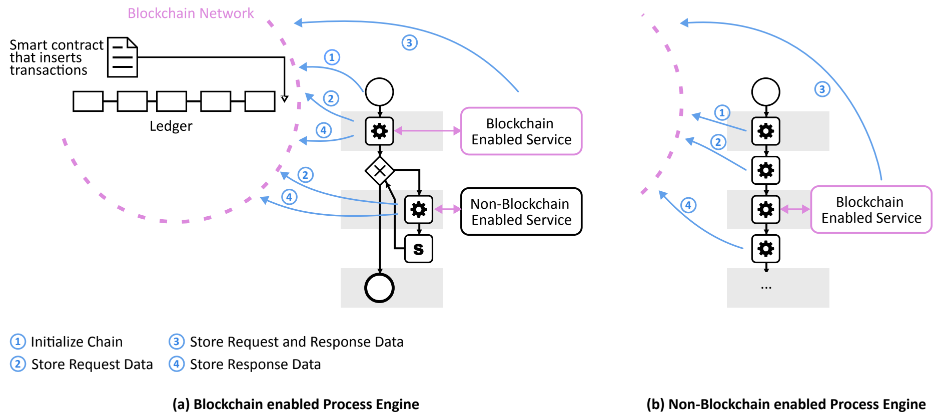

Fig. 1: Soft Integration With and Without Engine Support

between both the process engine and services with the blockchain network. For an attacker, it is arguably difficult to consistently tamper with multiple connections, i.e., the ones between a process engine and a service, as well as the ones to the blockchain network.

Figure 1(a) shows a blockchain-enabled process engine with both a blockchain-enabled service as described above as well as a non-blockchain-enabled service. Such legacy services continue to work fine, 2 and 4 are stored in the ledger (i.e., the non-tamperable log), but consistency checks comparing sent and received data are only possible for a blockchain-enable service.

Figure 1(b) shows the potential implementation for a non-blockchain-enabled process engine. Here additional tasks (potentially automatically generated for given process models), ensure the interactions 2-4 as described above. I.e., the activity from Fig. 1(a), is now represented by 4 activities. This inflates the process model but ensures the broadest possible compatibility.

4 Implementing a Soft Integration Approach

4.1 Blockchain Platform Selection

The first challenge for a soft integration approach is selecting a fitting blockchain platform. For an initial selection, 20 potential candidates are considered based on their academic and industry relevance as well as smart contract capabilities. The complete list of initial candidates can be found in Table 2. It's important to note that very high claimed transaction speeds are theoretical and often rely on unrealistic expectations, such as all participating nodes trusting a single validating node or an extremely high number of validating nodes.

To better structure the selection process, a series of key criteria were identified:

- **Public vs Private:** A public blockchain allows anyone to join and participate in the network, while in a private blockchain, access is restricted to a specific group of par-

Table 2: Initial List of Potential Blockchain Platforms; Etherum and Hyperledger have been referenced before. For all platforms referenced below, the last access date is 2024-04-24

Platform	Type	Smart Contracts	Active Maint.	Strong Community	Enterprise Focus	Stated Max Transactions per Second
algorand.com	Public	Yes	Yes	Yes	No	7500
avax.network	Public	Yes	Yes	Yes	No	4500
bnbchain.org	Public	Yes	Yes	Yes	No	100
cardano.org	Public	Yes	Yes	Yes	No	1000
corechain.tech	Private	No	No	No	No	Not Available
eosnetwork.com	Public	Yes	Yes	Yes	No	10,000
Ethereum	Public	Yes	Yes	Yes	No	15
Hyperledger Besu	Private	Yes	Yes	Yes	Yes	400
Hyperledger Fabric	Private	Yes	Yes	Yes	Yes	2000
near.org	Public	Yes	Yes	Yes	No	2000
nemproject.github.io	Public	Yes	Yes	Yes	No	4000
neo.org	Public	Yes	Yes	Yes	No	10000
polkadot.network	Public	Yes	Yes	Yes	No	1000
consensys.net/quorum/	Private	Yes	Yes	Yes	Yes	750
r3.com/products/corda	Private	Yes	Yes	Yes	Yes	1700
ripple.com	Public	No	Yes	Yes	No	1500
solana.com	Public	Yes	Yes	Yes	No	2000
stellar.org	Public	No	Yes	Yes	No	4000
tezos.com	Public	Yes	Yes	Yes	No	170
zilliqa.com	Public	Yes	Yes	Yes	No	2800

ticipants. For integrating blockchain technology with BPMS, a private blockchain is generally preferred since organizations have a higher level of trust among each other compared to the general public, and smaller chains with higher trust allow for the use of better-performing consensus mechanisms. A downside of private blockchains is that they have to be deployed, configured, and maintained in contrast to the most well-known and most studied blockchains (Bitcoin, Ethereum). In addition, a private blockchain is in general more vulnerable to attacks that require control of a certain number of nodes (e.g., over 51 percent), due to their smaller size. However, for soft integration, the participating actors are well-known to each other, which would make such an attack very difficult.

- **Permissionless vs Permissioned:** In a permissionless blockchain, every participant can participate in all blockchain activities, including transaction validation and block creation. Meanwhile, in a permissioned blockchain, permissions can be assigned to different roles within the network, restricting access to certain activities. For a soft integration approach, we deem a permissioned blockchain to be more suitable since it allows for the creation of access roles, enabling more trust between organizations.

- **Consensus Mechanism:** The choice of consensus mechanism heavily depends on the previous two criteria. In public, permissionless networks, anyone can create and validate blocks, meaning the consensus mechanisms need to be stricter to prevent malicious behavior. Accordingly, in these open networks, the proof of work or proof of stake mechanisms are widely used, while in permissioned networks, other mechanism, like the Practical Byzantine Fault Tolerance (PBFT), are regarded as sufficient. The choice of consensus mechanism influences several key factors, which are summarized in Table 3. It's important to note that several permissioned blockchains permit the use of different consensus mechanism and Byzantine Fault Tolerance is just one example of a deterministic consensus mechanism, however, the differences when comparing proof of work/stake to other deterministic consensus mechanism are largely consistent.
- **Academic and Industry Relevance:** Finally, the chosen blockchain technology needs to be well-known and widely used to maximize acceptance by organizations participating in process orchestration. This criterion was evaluated by analyzing community size, media presence, enterprise focus, and the popularity of smart contracts for each platform.

Feature	**Proof of Work (PoW)**	**Proof of Stake (PoS)**	**PBFT**
Mining/Validation	Computational mining	Staking of assets	Rotating primary node
Finality	Probabilistic	Probabilistic	Deterministic
Throughput	Lower	Moderate	Higher
Security	High	High	High in smaller networks
Suitability	Permissionless networks	Permissionless networks	Permissioned networks

Table 3: Comparison of PoW, PoS, and PBFT Consensus Mechanisms

Having decided on these key criteria, five suitable prominent distributed ledger platforms can be identified (out of the initial 20 candidates): Ethereum, Hyperledger Besu[15], Hyperledger Fabric, Quorum[16], and R3 Corda[17]. The analysis results of the five final candidates and additional scoring based on the criteria to decide on a final choice can be found in Table 4. The scores range from 1-10 and are derived based on the specific requirements for a soft integration with BPMS and the available consensus mechanism. The scoring would be different for different use cases and depending on the choice of consensus mechanism. Based on our scoring, we found the Hyperledger Fabric platform to be the most suitable for a soft integration approach.

[15] `https://www.hyperledger.org/projects/besu`, last access: 2024-05-28
[16] `consensys.net/quorum/`, last access: 2024-04-10
[17] `r3.com/products/corda`, last access: 2024-04-10

Platform	Ethereum	Besu	Fabric	Quorum	R3 Corda
Type	Public	Both	Private	Private	Private
Permissioned	No	Both	Yes	Yes	Yes
Security	9/10	8/10	8/10	8/10	8/10
Privacy	5/10	8/10	9/10	8/10	9/10
Performance	4/10	7/10	8/10	6/10	6/10
Scalability	4/10	7/10	8/10	6/10	6/10
Cost	5/10	8/10	9/10	8/10	9/10

Table 4: Scoring of final 5 candidates for soft integration of blockchain platform with BPMS

4.2 Solution Architecture

Our proposed soft integration implementation aims to devise a reliable method that ensures the entire execution history of processes, including API calls, responses, and data exchanges, is securely logged on the blockchain without significant integration complexity. For this purpose, two different architectural approaches were developed after testing Hyperledger Fabric's functionalities: (1) The REST API-Based Approach and (2) the direct-invocation Approach. For complete implementation details, refer to the GitHub page [18].

REST API-Based Approach The REST API-Based approach consists of several key components: The Hyperledger Fabric (test) network, a smart contract, a REST API server, and the client BPM system. The idea is to use the API server as middleware to communicate between the BPMS and the blockchain, creating a flexible, language-agnostic, and highly decoupled architecture. Since existing BPM systems regularly call API requests for process execution, integrating the API-Based Approach with the processes or BPMS (i.e., Fig. 1) is simple, as knowledge of how to invoke REST services securely is widespread. An overview of the approach can be seen in Fig. 2

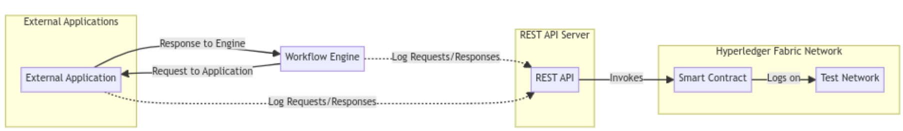

Fig. 2: Architecture of the REST API-based approach. The workflow engine initiates a process that interacts with external applications and logs these interactions through the REST API to a smart contract deployed on the Hyperledger Fabric network.

However, while this approach is extremely easy to integrate with various process management systems, it also adds a new single point of failure in the REST API server

[18] `https://github.com/thomasvloo/fabric-testnet`, last accessed: 2024-04-10

similar to [1]. Furthermore, the server adds additional latency to the execution, which is already a major downside of integrating blockchains with BPMS. The direct-invocation approach aims to solve these problems.

Direct-invocation Approach The direct-invocation approach facilitates a direct connection between BPMS and Blockchain, bypassing the REST API. Since access to the blockchain is not abstracted through the API interface, integration with the process engine is more challenging. The process engine needs to be extended such that every activity also invokes a blockchain call before and after execution with sufficient authentication. This strong coupling also means that any changes to the BPMS or the process might require adjustment to the integration code. However, removing the middleware between the engine and the blockchain network can enhance the performance, and security risks related to adding an additional component (i.e., the API server) can be minimized. Figure 3 shows an overview of the approach.

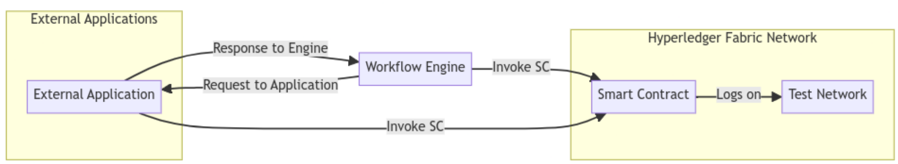

Fig. 3: Architecture of the direct-invocation approach. The workflow engine initiates a process that interacts with external applications and logs these interactions by directly invoking a smart contract deployed on the Hyperledger Fabric network.

While this approach offers the desired enhanced performance, security, and reduced latency, it requires additional integration and maintenance effort since the different systems are now strongly coupled and language-specific. An extensive evaluation was conducted to evaluate the performance differences, which is presented in the following section.

5 Performance Evaluation

As process engines are used in many domains that rely on a high number of potential transactions, it is important to explore potential limitations to the number of transactions that can be made. For example, in the manufacturing domain, processes interact at high velocities and produce high data volume (which translates to transaction payload volume).

5.1 Methodology

The performance of both the direct-invocation approach and the API-based approach was evaluated by simulating API requests to the Hyperledger Fabric test-network. The objective was to measure the throughput in terms of transactions per second (TPS) when faced with increasingly larger batches of transaction submissions. In addition, the payload sizes were varied between 1000 and 10000 characters to simulate the variance in data size typically observed within production environments. Other aspects, such as integration complexity, flexibility, and security, were considered qualitatively through discussions with domain experts.

5.2 Performance Evaluation

The performance evaluation results can be seen in Fig. 4. While the REST-API-based approach maintains a relatively consistent TPS rate, the direct-invocation approach shows consistently higher throughput, albeit with higher variability. These results reflect the prior expectations since the latency added by the middleware is removed in the directly connected direct-invocation approach. The results also point towards a maximal throughput of around 170 TPS when using the hyperledger test network, however this is likely a limit of the hyperledger test network, considering that hyperledger themselves state a maximal throughput of 2946.7 TPS [19]. That being said, 170 TPS can be considered more than sufficient for process orchestration in many domains.

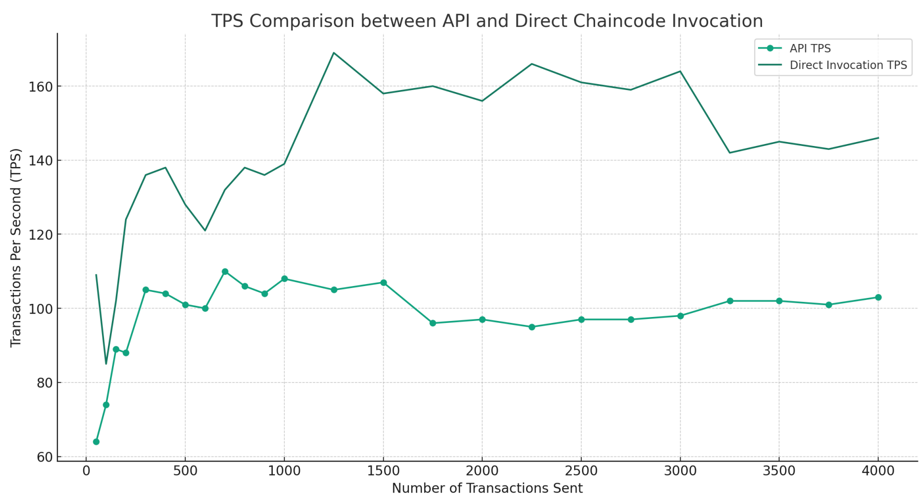

Fig. 4: Transactions Per Second (TPS) comparison between API and Direct Chaincode Invocation approaches.

[19] `https://www.hyperledger.org/blog/2023/02/16/benchmarking-hyperledger-fabric-2-5-performance`, last access: 2024-05-28

5.3 Complexity, Flexibility, and Security

The main benefit of integrating blockchain technology with business process engines is to enable decentralization with enhanced security, transparency, and trust amongst participating organizations. Furthermore, a blockchain-capable BPMS opens many possibilities for potential decentralized use cases and application scenarios. The main reason for a soft-integration approach is to reduce the barrier of entry by having very little integration complexity. Accordingly, these factors are analyzed in this section. Table 5 summarizes the results of this analysis.

	REST-API	Direct-Invocation
Ease of Integration	+	-
Flexibility	+	-
Performance	-	+
Security	=	+

Table 5: Comparison

The direct-invocation approach has better performance and as discussed in Sections 2 and 4 is also more secure since it has fewer failure points. Here it is important to note, that the security of the REST-API approach can be extended with well-known methods, however, this could in turn lead to a further decrease in performance. Meanwhile, when it comes to integration complexity and flexibility, the REST-API approach is preferred since it has low coupling, is BPMS technology stack agnostic, and is already supported by some existing process engines, while the direct-invocation approach needs to be adjusted to the used engine and requires significant knowledge of blockchain technology and smart contract coding. Overall, these results stress that the correct soft integration approach depends on the application domain. Furthermore, both soft integration approaches are still significantly easier and less costly than a hard integration approach.

We found that the transaction payload size (up to sizes of 100's of MiB) has no unexpected impact on TPS.

6 Conclusion

While blockchain technology has become widely known both in industry and academia due to its influence on the financial domain, there has been no widespread integration of blockchain technology with business process management systems. We analyze related work and identify the high barrier of entry in transitioning the existing BPMS an organization is already using onto the blockchain as well as the disadvantages of immutable processes as the main reasons for this low adaption rate. Therefore, we propose a soft integration approach, which allows for the creation of immutable execution logs with low integration complexity.

Our work aims to use blockchain technology to create distributed, non-tamperable process execution logs without significant integration efforts. We discuss the advantages and disadvantages of using a soft integration approach, where the process is modeled, executed, and monitored using a traditional BPMS, compared to a hard integration approach, where the process is executed on the chain in the form of a smart contract. By logging the entire execution history, including API calls, responses, and data exchanges on a permissioned blockchain, we create an immutable execution log that can be used as a reliable basis for compliance management, process mining, and optimization and also improves trust amongst organizations participating in the process. Furthermore, security is improved since malicious actors can not hide tampering with data that is sent over the wire during process execution (which leads to manipulated process logs). In addition, existing functionalities and tools, such as modeling, execution, error handling, and monitoring/dashboarding, can still be used. We analyzed 20 different blockchain platforms and found 5 suitable platforms on which we used an extensive scoring system to determine the Hyperledger Fabric platform as most suitable for our research. The Cloud Process Execution Engine (CPEE) was selected for process execution and connected to Hyperledger test networks through both, a REST server as well as direct chaincode invocation. Both the REST API and the direct invocation approach are easier to integrate and the interaction costs less compared to a hard integration approach. Through a quantitative evaluation, we show that the performance of both approaches is sufficient for process execution. We also discuss strengths and weaknesses of both implementation strategies. While the direct invocation approach has noticeably higher performance, it requires significantly more integration effort than the REST API-based approach. All created software artifacts are provided for future research and testing.

A limitation of the soft integration approach is, that it does not directly enable tamper-proof execution. However, immutable processes, as a result of hard integration, have considerable disadvantages due to their static nature as discussed in Section 3. In addition, tamperproof execution is difficult to achieve even with a hard integration approach for many processes that rely on information from outside of the chain provided via oracles. If tamperproof execution is still required for well-established processes with little changes and reliance on outside information, related work [9, 16] can be used to integrate a BPM to Solidity Translator with the process engine. A further limitation is that the tests were done using the Hyperledger test network. Accordingly, throughput values measured during the performance evaluation should be seen as lower bounds rather than upper bounds of the throughput possible with the Hyperledger Fabric platform. However, the observed performance was already sufficient for process orchestration for typical application domains (e.g., we never saw more than 300 TPS for real-world processes in the manufacturing domain).

In the future, we plan to test the prototypical implementations in a production environment and demonstrate mechanisms that automatically detect deviations between immutable log, client-side log, and expected execution behavior to detect compliance violations or tampering. Furthermore, moving away from the Hyperledger test network to a custom, production-grade network would allow for a more accurate evaluation.

References

1. Alves, P.H.C., Paskin, R., Frajhof, I.Z., Miranda, Y.R., Jardim, J.G., Cardoso, J.J.B., Tress, E.H.H., da Cunha, R.F., Nasser, R., Robichez, G.: Exploring blockchain technology to im-

prove multi-party relationship in business process management systems. In: ICEIS (2). pp. 817–825 (2020)
2. Clohessy, T., Acton, T., Rogers, N.: Blockchain adoption: Technological, organisational and environmental considerations. In: Business transformation through blockchain, pp. 47–76. Springer (2019)
3. Di Ciccio, C., Cecconi, A., Dumas, M., García-Bañuelos, L., López-Pintado, O., Lu, Q., Mendling, J., Ponomarev, A., Binh Tran, A., Weber, I.: Blockchain support for collaborative business processes. Informatik Spektrum **42**, 182–190 (2019)
4. 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). `https://doi.org/10.1109/ACCESS.2020.3013911`
5. Grisold, T., Mendling, J., Otto, M., vom Brocke, J.: Adoption, use and management of process mining in practice. Business Process Management Journal **27**(2), 369–387 (2021)
6. Kitchenham, B., Charters, S.: Guidelines for performing systematic literature reviews in software engineering **2** (01 2007)
7. Li, M., Huang, G.: Blockchain-enabled workflow management system for fine-grained resource sharing in e-commerce logistics. In: 2019 IEEE 15th International Conference on Automation Science and Engineering (CASE). pp. 751–755 (2019). `https://doi.org/10.1109/COASE.2019.8843250`
8. Lopez-Pintado, O., Dumas, M., Garcia-Banuelos, L., Weber, I.: Dynamic role binding in blockchain-based collaborative business processes. In: Advanced Information Systems Engineering: 31st International Conference, CAiSE 2019, Rome, Italy, June 3–7, 2019, Proceedings 31. pp. 399–414. Springer (2019)
9. Lopez-Pintado, O., Garcia-Banuelos, L., Dumas, M., Weber, I.: Caterpillar: A blockchain-based business process management system. In: International Conference on Business Process Management (2017), `https://api.semanticscholar.org/CorpusID:3629238`
10. Mangler, J., Grüger, J., Malburg, L., Ehrendorfer, M., Bertrand, Y., Benzin, J.V., Rinderle-Ma, S., Serral Asensio, E., Bergmann, R.: Datastream xes extension: embedding iot sensor data into extensible event stream logs. Future Internet **15**(3), 109 (2023)
11. Mangler, J., Seiger, R., Benzin, J.V., Grüger, J., Kirikkayis, Y., Gallik, F., Malburg, L., Ehrendorfer, M., Bertrand, Y., Franceschetti, M., Weber, B., Rinderle-Ma, S., Bergmann, R., Asensio, E.S., Reichert, M.: From internet of things data to business processes: Challenges and a framework (2024)
12. Mendling, J., Weber, I., Aalst, W.V.D., Brocke, J.V., Cabanillas, C., Daniel, F., Debois, S., Ciccio, C.D., Dumas, M., Dustdar, S., et al.: Blockchains for business process management-challenges and opportunities. ACM Transactions on Management Information Systems (TMIS) **9**(1), 1–16 (2018)
13. Mercenne, L., Brousmiche, K.L., Hamida, E.B.: 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. IEEE (2018)
14. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review p. 21260 (2008)
15. Stiehle, F., Weber, I.: Blockchain for business process enactment: a taxonomy and systematic literature review. In: International Conference on Business Process Management. pp. 5–20. Springer (2022)
16. Tran, A.B., Lu, Q., Weber, I.: Lorikeet: A model-driven engineering tool for blockchain-based business process execution and asset management. In: BPM (Dissertation/Demos/Industry). pp. 56–60 (2018)