A Hybrid Cloud–Blockchain Architecture for Secure and Transparent BPM Application Composition

Sadok Lanani[1] [*], Laid Kahloul[2], and Okba Kazar[3]

[1 2] LINFI Laboratory, Biskra University, Biskra 07000, Algeria

[3] Department of Computer Science, College of Computing and Intelligent Systems, University of Kalba, Sharjah, UAE

*sadok.lanani@univ-biskra.dz

l.kahloul@univ-biskra.dz

okba.kazar@ukb.ac.ae

Abstract. Business Process Management (BPM) systems are increasingly employed to automate and coordinate complex, multi-actor workflows across organizational boundaries. However, conventional cloud-based BPM solutions continue to face enduring challenges related to trust, data transparency, and auditability. This paper introduces a hybrid Cloud–Blockchain architecture that integrates the scalability and efficiency of cloud computing with the immutability and traceability of blockchain to enable secure and transparent BPM application composition. In the proposed model, large-scale process data and documents are securely processed and stored in the cloud, while metadata and cryptographic hashes are anchored on the blockchain to ensure integrity, authenticity, and verifiability. The architecture is structured into three core layers: (1) a BPM Orchestration layer responsible for coordinating workflow execution and managing cross-layer communication; (2) a Cloud Layer providing scalable computation and encrypted storage; and (3) a Blockchain Layer ensuring tamper-proof logging, smart contract–based validation, and trusted auditability. By combining cloud scalability with blockchain transparency, the architecture enhances BPM reliability and data integrity while minimizing reliance on centralized intermediaries. Future research will focus on implementing and evaluating the proposed model using Hyperledger Fabric and a BPM engine such as Camunda to assess performance, scalability, and security trade-offs in real-world scenarios.

Keywords: BPM, Blockchain, Cloud Computing, Hybrid Architecture, Transparency, Smart Contracts, Composition.

1 Introduction

Business Process Management (BPM) has become a key discipline for designing, automating, and optimizing complex organizational workflows [1]. Modern BPM systems support BPM application composition by integrating heterogeneous services, data sources, and actors into executable workflows [2]. This capability enables component reuse, faster deployment, and coherent orchestration across distributed environments

D. Agti et al. (eds.), *Proceedings of the International Conference on Artificial Intelligence Applications in Business Administration in MENA Region (ICAIABA 2026)*, Advances in Economics, Business and Management Research 393,
https://doi.org/10.2991/978-94-6239-711-8_31

[3]. However, when processes span multiple organizations, BPM composition faces challenges related to trust, transparency, and integrity [4].
Cloud computing is now the dominant platform for BPM deployment due to its scalability, elasticity, and cost efficiency [5]. Cloud-based BPM engines, such as
Camunda and Flowable, allow dynamic process composition using BPMN models and service orchestration. Nevertheless, in multi-tenant and multi-stakeholder settings, cloud infrastructures provide limited guarantees regarding data authenticity, auditability, and accountability [6]. Consequently, users must rely on the cloud provider to ensure the integrity and immutability of process records, which introduces risks of tampering or insider misuse.
Blockchain technology offers a decentralized trust model that can enhance BPM composition by ensuring immutable, transparent, and verifiable process execution records [7, 8]. Smart contracts enable automated validation of inter-organizational workflows without relying on centralized authorities [4]. However, blockchain's limited throughput and high latency make it unsuitable for executing data-intensive BPM tasks [9].
To overcome these limitations, this paper proposes a hybrid Cloud–Blockchain architecture for secure and transparent BPM application composition. In the proposed approach, large-scale process data are processed and stored in the cloud, while process metadata, states, and cryptographic hashes are maintained on the blockchain. A BPM orchestration engine coordinates workflow execution across both environments, achieving efficient process management while preserving integrity, authenticity, and verifiability.

The main contributions of this paper are:

- A hybrid architecture supporting BPM application composition across cloud and blockchain platforms.
- A trust and security model combining encryption, hash linking, and smart contracts.
- An explanation of BPM orchestration mechanisms ensuring seamless composition, coordination, and auditability.

The remainder of the paper is organized as follows. Section 2 presents the foundations and reviews related work, followed by a clear research gap statement (Sect. 2.1). Section 3 describes the proposed hybrid Cloud–Blockchain architecture, detailing its core layers and components. Section 4 discusses the trust, security, and transparency model enabled by the proposed approach. Finally, Section 5 concludes the paper and outlines directions for future research.

2 Foundations and Related Work

Schulte et al. [10] propose an elastic BPM architecture that dynamically scales process execution in the cloud, addressing scheduling, resource allocation, monitoring, and decentralized coordination. While effective for performance and elasticity, it does not tackle trust, data integrity, or verifiable auditability in multi-tenant environments.

Xu et al. [11] propose a Cloud Service Composition Optimization System (CSCOS) for public and private clouds, considering QoS, compatibility, and process coordination. While their coevolutionary algorithm handles large-scale service composition effectively, it lacks transparent execution tracking and immutable audit trails. Similarly, Kritikos et al. [12] present a multi-cloud BPM architecture with cross-level orchestration and CAMEL to avoid vendor lock-in and leverage heterogeneous clouds. Although flexible in deployment, it does not provide cryptographic verification or immutable logging for cross-organizational trust.

Blockchain has mainly been applied to enhance process transparency in domain-specific scenarios, particularly supply chain management [13]. Its systematic integration into general-purpose BPM systems for application composition remains limited, as most existing studies focus on isolated use cases rather than comprehensive hybrid orchestration frameworks combining cloud execution and blockchain-based validation.

Groe et al. [14] explore trust in inter-organizational capacity exchange platforms, deriving blockchain-based design principles that improve trust among anonymous participants. Similarly, Agrawal et al. [15] propose a blockchain-based traceability framework for textile supply chains, showing how smart contracts and distributed ledgers enhance transparency and reduce information asymmetry. Gupta et al. [16] develop a blockchain platform for intra- and inter-organizational knowledge sharing among software SMEs, using smart contract-based authentication and decentralized access control to strengthen data ownership, authenticity, and transparency.

As cloud adoption for BPM increases, research has explored blockchain–cloud integration to improve trust and accountability. For instance, [17] propose a blockchain-based infrastructure for transparent SLA monitoring in cloud environments, showing how immutable ledgers enable verifiable compliance. However, such approaches typically address specific concerns without providing holistic BPM frameworks.

The survey in [18] reviews Blockchain as a Service (BaaS) platforms that combine cloud scalability with blockchain decentralization, emphasizing deployment and provisioning models that reduce complexity and cost. Similarly, [19] introduce PureChain, a hybrid BaaS framework that improves blockchain scalability through enhanced consensus and on/off-chain coordination, achieving significant throughput gains.

Finally, [20] present a PRISMA-based systematic review of blockchain–cloud integration in electronic health record systems. Their findings show that hybrid architectures effectively balance cloud scalability with blockchain immutability and traceability, offering insights that are directly applicable to BPM systems.

2.1 Research Gap Statement

Cloud-based BPM architectures offer scalability and efficiency but lack trust and auditability [10, 11, 12], whereas blockchain-based approaches ensure security and transparency at the cost of low throughput and high latency [13, 14, 15, 16]. Existing blockchain–cloud integration efforts address isolated concerns such as SLA monitoring or performance optimization without providing a unified BPM orchestration model [17, 18, 19, 20]. **This research investigates how BPM orchestration can leverage cloud**

scalability while integrating blockchain-based security and traceability with minimal performance overhead. Specifically, it proposes a hybrid Cloud–Blockchain architecture for secure, auditable, and high-performance BPM application composition.

3 Proposed Hybrid Cloud–Blockchain Architecture

This section introduces a hybrid Cloud–Blockchain architecture for secure and transparent BPM application composition, combining cloud scalability with blockchain-based immutability for trust and auditability. The model comprises three layers Cloud Computing, BPM Orchestration and Composition, and Blockchain as illustrated in Fig.1.

3.1 Architectural Overview

The proposed hybrid architecture overcomes the limitations of standalone cloud and blockchain BPM systems by assigning responsibilities based on their respective strengths. Data-intensive processing, computational workloads, and temporary process states are handled in the cloud, while cryptographic proofs, immutable logs, and validation logic are maintained on the blockchain. A BPM orchestration engine acts as a central coordinator, composing workflows across both environments and ensuring consistency and auditability. By limiting on-chain storage to essential metadata and hashes, the architecture minimizes overhead while preserving security and trust.

3.2 Cloud Computing Layer

The Cloud Computing Layer provides the elastic computational infrastructure and scalable storage required for executing data-intensive BPM tasks and managing voluminous process artifacts. It consists of three primary components: the Execution Environment, Off-Chain Storage, and the Cloud–Blockchain Interface.

Execution Environment.

The execution environment provides the runtime infrastructure for executing BPM tasks, invoking services, and performing computational operations. Cloud platforms such as AWS, Azure, and Google Cloud offer elastic resources that adapt dynamically to workload variations. In this architecture, the environment executes workflow tasks,

orchestrates microservices and external APIs, and supports compute-intensive activities such as analytics and document processing. Fine-grained execution traces are produced and forwarded to the orchestration layer for selective blockchain recording.

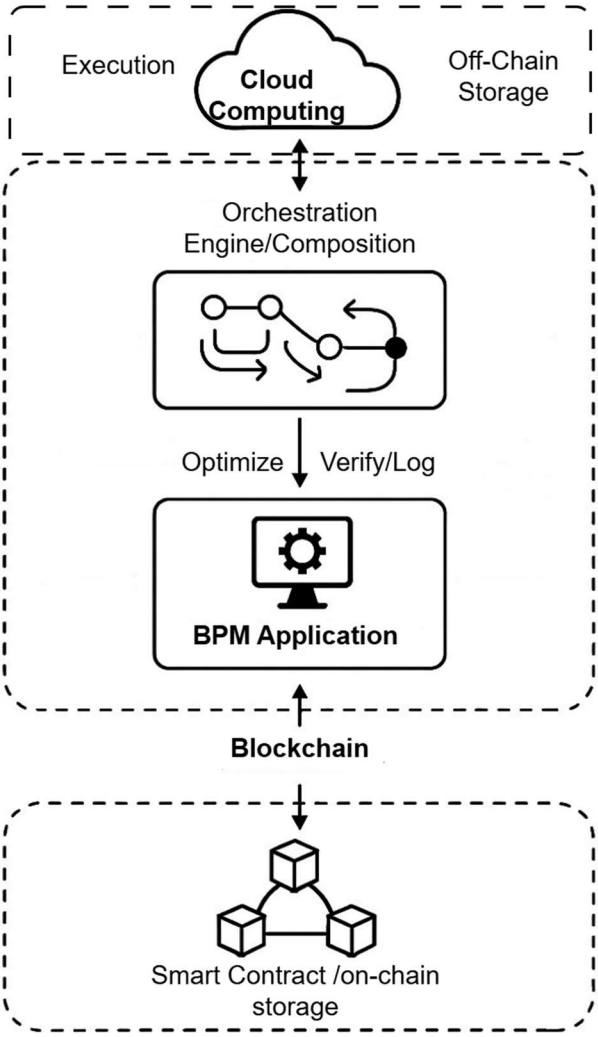

Fig. 1. Hybrid Cloud–Blockchain Architecture

Off-Chain Storage.

Off-chain storage is used for large-scale process data, documents, and intermediate states that are unsuitable for on-chain storage. Data are stored in encrypted repositories and managed through cloud-based document and versioned data systems. For each stored object, a cryptographic hash is generated and anchored on the blockchain, enabling integrity verification and tamper detection without exposing sensitive content.

Cloud–Blockchain Interface.

The Cloud–Blockchain interface enables secure communication between the cloud and blockchain layers under the control of the BPM orchestration engine. It prepares

process metadata and hashes for on-chain submission, applies transaction batching to improve efficiency, and manages asynchronous confirmation and finality tracking. By abstracting blockchain operations, the interface ensures transparent and reliable recording of validated BPM events.

3.3 BPM Orchestration and Composition Layer

The BPM Orchestration and Composition Layer acts as the core coordination component of the architecture, bridging cloud-based execution with blockchain-based verification. It extends a BPMN-compliant engine (e.g., Camunda, Flowable, or Zeebe) with blockchain-aware capabilities to ensure controlled, auditable, and trustworthy process execution.

Composition Engine.

The composition engine dynamically assembles BPM applications from reusable process fragments, services, and data sources. It supports runtime service discovery, modular workflow composition, data flow mapping, and constraint-based selection driven by QoS, security, and compliance requirements. Each finalized composition is cryptographically hashed and anchored on the blockchain, providing verifiable proof of the application configuration.

Orchestration Engine.

The orchestration engine governs distributed workflow execution by instantiating process instances, dispatching tasks to cloud services, users, or smart contracts, and managing process states and events. To balance performance and auditability, critical state changes are first persisted off-chain and then asynchronously recorded on the blockchain using a dual-write strategy.

Blockchain Integration Module.

This module abstracts blockchain interactions from the orchestration logic. It handles transaction submission, smart contract invocation, blockchain event listening, and confirmation management. By encapsulating consensus and failure handling, it enables seamless and reliable integration without exposing blockchain complexity to the BPM engine.

Verification and Logging Mechanism.

At predefined checkpoints, the orchestration layer generates verifiable process events containing identifiers, timestamps, actors, data hashes, and execution outcomes. These events are committed to the blockchain via smart contracts, ensuring immutable, auditable, and verifiable tracking of process state transitions.

3.4 Blockchain Layer

The Blockchain Layer provides decentralized trust and tamper-proof auditability through smart contracts and distributed consensus. A permissioned blockchain platform, such as Hyperledger Fabric, is adopted to meet enterprise security, privacy, and governance requirements.

Smart Contracts.

Smart contracts encode validation rules and organizational policies. They enforce correct process execution, verify data integrity through cryptographic fingerprints, validate BPM compositions against compliance constraints, and implement fine-grained access control mechanisms.

On-Chain Storage.

The ledger stores lightweight process metadata, immutable event logs, cryptographic hashes of off-chain data, and proofs of BPM composition. Merkle tree structures enable efficient verification while avoiding the disclosure of full execution histories.

Consensus Mechanism.

A Byzantine Fault Tolerant consensus protocol, such as PBFT or Raft, ensures fast transaction finality, high throughput, and low latency. This enables near real-time auditability without compromising consistency or fault tolerance.

Network Topology.

The architecture adopts a consortium blockchain model in which multiple organizations operate nodes. Peer nodes execute smart contracts and validate transactions, ordering nodes create blocks, and channels isolate data flows to preserve confidentiality across participants.

4 Trust, Security, and Transparency Model

The proposed hybrid Cloud–Blockchain architecture establishes an integrated trust, security, and transparency model that ensures authentic, confidential, and verifiable BPM application composition and execution, as illustrated in Fig. 2. Trust is distributed across the cloud, BPM orchestration, and blockchain layers through digital identities, signatures, access tokens, and smart contract–based validation, ensuring that only authenticated and authorized entities can interact across layers. Data confidentiality is preserved by encrypting all sensitive process data and documents in the cloud using strong symmetric encryption (e.g., AES-256), with secure key

management via cloud-native services or HSMs, while only cryptographic hashes and metadata are recorded on-chain to prevent information leakage. Integrity and auditability are guaranteed through hash linking and the blockchain's immutable ledger, which enables tamper detection, non-repudiation, and complete traceability of process events, actors, and timestamps. Transparency and accountability are achieved by allowing authorized stakeholders to independently verify workflow progress, execution outcomes, and composition specifications without reliance on a central authority, as smart contracts automatically enforce policies and compliance rules. By combining cloud scalability and efficiency with blockchain-based immutability and decentralized trust, the model effectively balances performance and security, providing a robust foundation for trustworthy, auditable, and scalable BPM application composition in multi-organizational environments.

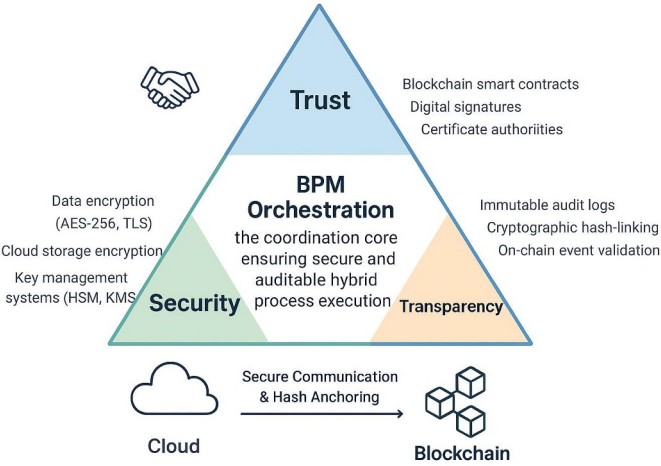

Fig. 2. Trust, Security, and Transparency Model

5 Conclusion and Future Work

This paper presented a hybrid Cloud–Blockchain architecture for secure and transparent BPM application composition. The model integrates three complementary layers—Cloud, BPM Orchestration, and Blockchain—to unify computational efficiency with trust and auditability. Through smart contracts, cryptographic hash linking, and asynchronous coordination, the architecture ensures process integrity, data verifiability, and cross-organizational transparency.

The conceptual framework provides a scalable and trustworthy foundation for distributed BPM ecosystems, redefining how organizations can automate and audit multi-actor workflows. Future work will focus on prototyping the architecture using Hyperledger Fabric integrated with a BPM engine such as Camunda to empirically

assess latency, throughput, and transaction costs. Further exploration will extend toward privacy-preserving techniques (e.g., zero-knowledge proofs), AI-assisted orchestration, and interoperability with edge and Blockchain as a Service environments, paving the way for intelligent, self-verifying BPM systems.

References

1. Rosemann, M., Brocke, J.v., Van Looy, A. et al.: Business process management in the age of AI – three essential drifts. Information Systems and e-Business Management 22, 415–429 (2024)
2. Scheer, A.-W.: Application Composition Platform Architecture. In: The Composable Enterprise, pp. 51–79. Springer, Wiesbaden (2024)
3. Reijers, H.A.: Business Process Management: The evolution of a discipline. Computers in Industry 126, 103404 (2021)

4. Taherdoost, H., Madanchian, M.: Blockchain and Business Process Management (BPM) Synergy: A Comparative Analysis of Modeling Approaches. Information 15(1), 9 (2024)
5. Maddukuri, N.: Trust in the Cloud: Ensuring Data Integrity and Auditability in BPM Systems. IJITMIS 12, 144–160 (2021)
6. Chauhan, M., Shiaeles, S.: An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network 3(3), 422–450 (2023)
7. Stefanescu, D. et al.: Smart Contract Powered Framework for the Next Generation Industry 4.0 Business Model. Distrib. Ledger Technol. 3(4), 28 (2024)
8. Lanani, S., Kahloul, L., Kazar, O.: A Blockchain-Based Framework for Decentralized USIM Identity Management and Regulatory Compliance in Mobile Networks. SN Computer Science 7(3), 272 (2026)
9. Ni, L., Irannezhad, E.: Performance analysis of LogisticChain: A blockchain platform for maritime logistics. Computers in Industry 154, 104038 (2024)
10. Schulte, S. et al.: Elastic Business Process Management: State of the art and open challenges for BPM in the cloud. Future Generation Computer Systems 46, 36–50 (2015)
11. Xu, J. et al.: Business-process-driven service composition in a hybrid cloud environment. Information Systems Frontiers 27(1), 259–281 (2025)
12. Kritikos, K. et al.: Multi-cloud provisioning of business processes. Journal of Cloud Computing 8(1), 18 (2019)
13. Hübschke, M. et al.: Blockchain in supply chain management: a comprehensive review of success measurement methods. Management Review Quarterly, 1–55 (2025)
14. Große, N. et al.: Designing trust-enabling blockchain systems for the inter-organizational exchange of capacity. Decision Support Systems 179, 114182 (2024)
15. Agrawal, T.K. et al.: Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. Computers & Industrial Engineering 154, 107130 (2021)
16. Gupta, C., Gupta, V., Fernandez-Crehuet, J.M.: A blockchain-enabled solution to improve intra-inter organizational innovation processes in software SMEs. Engineering Reports 5(7), e12674 (2023)
17. Khan, K.M. et al.: Blockchain-enabled real-time SLA monitoring for cloud-hosted services. Cluster Computing 25(1), 537–559 (2022)
18. Song, J. et al.: Research advances on blockchain-as-a-service: architectures, applications and challenges. Digital Communications and Networks 8(4), 466–475 (2022)
19. Kim, D.-S. et al.: Blockchain-as-a-Service: A Pure Chain Approach. Blockchain: Research and Applications, 100397 (2025)
20. Lopez, L.J.R. et al.: Hybrid Architectures Used in the Protection of Large Healthcare Records Based on Cloud and Blockchain Integration: A Review. Computers 13(6), 152 (2024)