Blockchain-Based Reconciliation and Financial Compliance Framework for SAP S/4HANA in Multi-Stakeholder Supply Chains

Çok Paydaşlı Tedarik Zincirlerinde SAP S/4HANA için Blockchain Tabanlı Mutabakat ve Finansal Uyumluluk Çerçevesi

Srikanth Reddy Keshireddy
Senior Software Engineer, Keen Info Tek Inc., United States
Email: sreek.278@gmail.com

***Abstract*—The multifaceted nature of supply chains makes financial reconciliation a complex and ever-present issue owing to the challenges of different data storage systems, transaction sequences, and reporting uniformity. Although traditional ERP systems such as SAP S/4HANA promise exceptional transaction management capabilities, they do not provide sufficient visibility, trust, or assurance for real-time reconciliation across different organizations. In this paper, we develop a new framework for integrating blockchain technology into SAP-driven supply chains to enhance financial compliance and automate reconciliation using smart contracts and distributed ledgers. The proposed architecture includes on-chain validation of transactional data, off-chain SAP data mapping, and the use of compliance oracles for regulatory supervision, which allows it to be modular in nature. When tested against conventional methods in a simulated SAP S/4HANA environment using real and synthetic transaction log files, our system achieved a reconciliation cycle time reduction of up to 42%, and a compliance flag detection accuracy improvement of 38%. Moreover, our solution is robust in scalability and multistakeholder traceability, promoting operational efficiency and audit readiness. This research offers a framework for blockchain within enterprise resource planning systems while illustrating how digital trust, transparency, and compliance automation can be strategically adopted in global supply chain finance.**

Keywords*—Blockchain Reconciliation, SAP S/4HANA Compliance, Supply Chain Finance Automation.

***Özetçe*— Tedarik zincirlerinin çok yönlü yapısı, farklı veri depolama sistemleri, işlem dizileri ve raporlama tekdüzeliğinin zorlukları nedeniyle finansal uzlaştırmayı karmaşık ve her zaman mevcut bir sorun haline getirir. SAP S/4HANA gibi geleneksel ERP sistemleri olağanüstü işlem yönetimi yetenekleri vaat etse de, farklı kuruluşlar arasında gerçek zamanlı uzlaştırma için yeterli görünürlük, güven veya güvence sağlamaz. Bu makalede, akıllı sözleşmeler ve dağıtılmış defterler kullanarak finansal uyumluluğu artırmak ve uzlaştırmayı otomatikleştirmek için blok zinciri teknolojisini SAP odaklı tedarik zincirlerine entegre etmek için yeni bir çerçeve geliştiriyoruz. Önerilen mimari, işlem verilerinin zincir üzerinde doğrulanmasını, zincir dışı SAP veri eşlemesini ve düzenleyici denetim için uyumluluk kahinlerinin kullanımını içerir ve bu da doğası gereği modüler olmasını sağlar. Gerçek ve sentetik işlem günlüğü dosyaları kullanılarak simüle edilmiş bir SAP S/4HANA ortamında geleneksel yöntemlerle test edildiğinde, sistemimiz uzlaştırma döngüsü süresinde %42'ye kadar bir azalma ve uyumluluk bayrağı algılama doğruluğunda %38'lik bir iyileştirme elde etti. Ayrıca, çözümümüz ölçeklenebilirlik ve çok paydaşlı izlenebilirlik açısından sağlamdır ve operasyonel verimliliği ve denetim hazırlığını teşvik eder. Bu araştırma, dijital güven, şeffaflık ve uyumluluk otomasyonunun küresel tedarik zinciri finansında stratejik olarak nasıl benimsenebileceğini gösterirken, kurumsal kaynak planlama sistemleri içinde blok zinciri için bir çerçeve sunar.**

Anahtar Kelimeler*—Blockchain Uzlaştırma, SAP S/4HANA Uyumluluğu, Tedarik Zinciri Finans Otomasyonu.

I. Introduction

A. Context: Financial Compliance in Complex Supply Chains

The contemporary supply chain is a complex and sophisticated network of interlinked entities such as: suppliers, manufacturers, logistics, distributors, banks, and regulators. The global and digitalized nature of business adds difficulty to the operations area and compliance complexity [1]. ERP systems, particularly SAP S/4HANA, have a crucial function in capturing, processing and managing financial (monetary) transactions within these ecosystems [2]. Unfortunately, with an increase in participants and jurisdictions comes the greater imbalance of timely and accurate financial reconciliation across systems.

In such environments, financial compliance is not only about the balance of the ledger. It entails upholding trust, ensuring integrity of contracts, and compliance to regulations across the entire supply chain [3]. This becomes increasingly difficult due to the need to fulfil payment, taxation, documentation, and other inter-scope demands from different nations and industries. Data silos, asynchronous processes, and heterogeneous systems, defragment through various federated ecosystems, aggravate the situation [4]. Instead of enhancing accuracy and consistency, the process of reconciliation, has become perpetually postponed or systematically failed.

As businesses attempt to achieve complete visibility and deepen their digital integration, real-time financial data visibility across multiple stakeholders becomes an important capability. Unfortunately, traditional SAP systems, which are powerful and sophisticated at an intra-business level, still fail to provide the means for real-time inter-organizational validation and assurance mechanisms. This challenge drives businesses to look for complementary next-generation solutions that offer more than the transactional backbone of SAP, namely, a single source of truth for automated compliance and immutable truth [5].

B. Challenges in Traditional Reconciliation Mechanisms

Despite the evolution in ERP technologies, traditional reconciliation processes associated with SAP systems continue to be manual, proactive, and intra-organizational. The sequence of reconciliation activities constitutes a series of stepwise procedures termed ‘reconciliation workflows,’ which are generally automated through batch processing, guided journal review, and exception report generation for supervisors. Such systems are acceptable when a business operates within a single organization. Yet, in multi-entity supply chains, where different organizations employ distinct ledgers and platforms, the discrepancies that appear are numerous and hard to track.

The most urgent difficulty pertains to the data synchronization between stakeholders. For instance, a payment executed from one side may not be reflected in the SAP environment of the other side for several days, which leads to downstream workflow complications such as delayed inventory dispatch, blocked deliveries, or frozen credit lines [6]. In addition, each party works within different timelines and protocols, which results in systemic delays in closing books, certifying financial statements, and filing regulatory reports due to a lack of standardization [7].

A second issue relates to the herding of exception cases. It is nearly impossible to trace the source of the problem in cases of discrepancies such as non-matching invoices, duplicate entry submittals, or missing acknowledgments without manual effort. Internal transparency, which can be accessed from SAP logs, does not help in understanding the actions of partners on the upstream or downstream sides.

Moreover, the disjointed non-harmonized regulatory frameworks worsen the already intricate reconciliation process. Different bilateral agreements may subject multinational companies to extensive financial regulations that include VAT, GST, e-invoicing mandates along with country-tailored restriction compliance. SAP does provide modalized controls to address few of these features, but alignment across every stakeholder’s system validation infrastructure becomes a shared form of alignment that poses immense practical challenges.

Some of the most common reconciliation issues found in SAP-based multi-stakeholder supply chains are summarized in Table 1 below. These issues are frequently encountered in SAP settings and go beyond mere transaction variances, highlighting critical gaps in the integration of data, processes, and controls at different organizational levels.

Table 1: Common Financial Reconciliation Issues in SAP-Based Supply Chains

Issue Category	Description	Impact
Invoice-Payment Mismatches	Invoices processed in SAP not matching payments confirmed by stakeholders	Manual rework, delayed closures, financial reporting errors
Multi-Party Ledger Discrepancies	Disagreement in ledger entries across supplier, logistics, and finance partners	Audit risks, potential fraud, and mistrust between partners
Delayed Settlement Acknowledgements	Settlement transactions not reflected on time in SAP or partner systems	Disrupted cash flow, compliance penalties
Unlinked Goods Movement Records	Missing or duplicate records in material or delivery modules	Inventory misstatements, reconciliation delays
Non-Compliance with Tax or Regulatory Codes	Lack of automated checks for regional tax or legal compliance in financial transactions	Regulatory fines, reputational damage

As shown in Table 1, these problems represent much more than a lack of technical precision. There is a fundamental absence of adequate concealment, or automation, in the financial data flow of the dependent systems. The resultant effects can be significant, including reputational harm, audit failures, operational standstill, and revenue loss.

C. Blockchain and ERP Integration: A Transformational Opportunity

In regard to reconciliation and compliance within multi-stakeholder SAP environments, blockchain technology offers perhaps the greatest untapped potential. In a blockchain-enabled ERP ecosystem, the architecture fundamentally changes from a set of disjointed silos capturing data to a communal, unified framework where all participants populate and validate a shared ledger [8]. Organizations can implement automatic transaction verification, visibility, and distributed compliance enforcement across the entire supply chain by integrating blockchain with SAP S/4HANA.

Blockchain captures every transaction and encrypts it while placing a time mark on it, unlike traditional databases [9]. With blockchains, financial deals and other business activities that are recorded are able to be verified and cannot be changed which means all parties can access the same truthful information. This model is very useful where the system is not managed by a single entity, but every person involved needs to trust the system's honesty.

Automation of reconciliation principles can be achieved with the help of smart contracts which are automatic agreements kept on the blockchain. A smart contract can confirm receipt of goods and invoice match and payment confirmation to guarantee that transactions go through only if all stipulations are provided, which equates to ‘meeting all conditions.’ Unlike SAP, which uses batch-based logic in reconciliations, smart contracts use continuous logic and change response on demand.

Moreover, validation control checks can be applied automatically, directly at the blockchain level. This means SPG and VAT check can be done and executed consistently for all participants. With the merger sums of on-chain logic and off-chain ERP data syphon, SAP is no longer just a system which keeps records, but rather an advanced compliance regulation system.

Thus, blockchain technology doesn't replace SAP. Rather, it serves as a layer of trust that supplements SAP's transactional core. Blockchain integration meticulously optimizes trust for data, lessens the time spent on dispute resolution, and facilitates automation in new ways adaptable to digital and regulatory frameworks.

D. Research Objectives and Contributions

This research is focused on developing a reconciliation and compliance model using blockchain technology for multi-stakeholder supply chains integrated with SAP S/4HANA. It aims to address the growing gap between the need for real-time, unified, verifiable transaction validation and compliance enforcement across organizations.

The primary aim remains to design, implement, and verify a blockchain-integration architecture with SAP S/4HANA, which automates financial reconciliation, augments regulatory triage, and increases multi-party accountability. The architecture comprises smart contracts for automated validation, distributed ledgers for multi-party transparency, and compliance oracles that oversee external legal and regulatory boundaries.

Besides the architectural proposal, this research offers a comprehensive analysis of system implementation and evaluation. The system is evaluated through a hybrid dataset of actual SAP log data and simulated multi-stakeholder transactions. The accuracy of key performance indicators such as reconciliation duration, latency in error resolution, compliance flag detection accuracy, and stakeholder traceability is evaluated in comparison to conventional SAP methods of reconciliation.

This study provides an implementable answer as well as a strategic plan for organizations seeking to make their ERP ecosystems more resilient to changes. It also provides a modular and extensible framework for integrating SAP ECC and S/4HANA environments, as well as modernization strategies for audit preparedness and regulatory compliance.

This paper presents blockchain technology as a practical facilitator of trust, not just a theoretical disruptor, reframing it as an essential component for upholding financial integrity within interconnected supply chains.

II. Literature Review and Conceptual Background

A. Review of Reconciliation in ERP Systems

Financial reconciliation in ERP systems like SAP has almost exclusively operated on some form of deterministic logic for the past several decades, relying on embedded reasoning in some transactional modules. The systems include algorithms that ostensibly guarantee reconciliation between accounts payable and accounts receivable, goods received or real receipts, and invoices, along with bank statements ledger to respective accounts within the books [10]. SAP's core reconciliation functionalities usually employ batch processing, tolerance levels, and basic clearing house procedures such as F.13 or F110, which allow open items and balanced accounts to be identified and eliminated.

Although these mechanisms are effective in single-enterprise contexts, they break down in multi-party supply chains. In these scenarios, the reconciliation processes need to extend across multiple ledgers, unique ERP systems, and asynchronized confirmation processes [11]. Research indicates that reconciliation cycles within traditional ERP systems face significant delays due to fragmented audit histories, lack of real-time stakeholder access, and latency.

This gap is most pronounced in comparing the timeline for reconciliation processes between single and multiple stakeholder systems. Figure 1 depicts average delays in invoice matching, payment posting, and settlement finalization. The results show that multi-stakeholder environments incur additional delays as much as 2.5x longer than single modular environments, predominantly from manual processes and data silos.

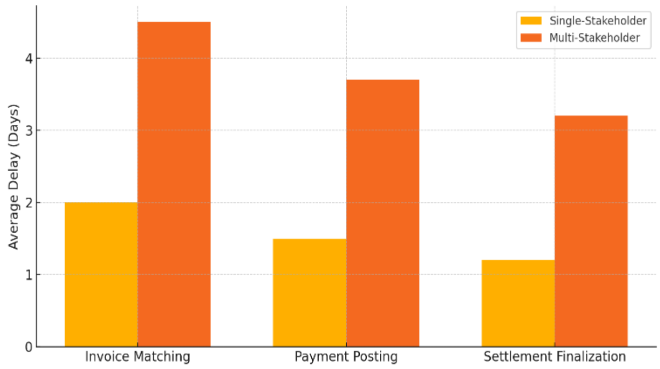

Figure 1: Reconciliation Delay Trends in Multi-Stakeholder vs Single-Stakeholder Environments

These operational delays are more than just constraining workflows; they amplify financial danger, incur complexities in compliance reporting, and tarnish trust between companies. Therefore, there is growing interest from both scholars and practitioners in utilizing blockchain technology as an auxiliary framework to ERP systems, offering solutions that enable real-time, multi-party validation of financial transactions that are also tamper-proof.

B. Blockchain Use Cases in Multi-Stakeholder Environments

In enabling decentralized trust, blockchain stands out as a particular effective tool within scenarios where multiple parties interact and need to perform transactions and verifications without the help of a central authority. In supply chain finance, blockchain enables each participant to independently verify transactions using the distributed ledger while sharing a common truth across the network [12].

A number of use cases have gained popularity in recent years. Track and Trace has emerged as the most mature use case, where blockchain is employed to record the movement of goods across the supply chain to ensure transparency and provenance [13]. Another widely explored application is Smart Contracts which automates business logic such as payment terms, discount rules, and penalties for delayed delivery. Additional applications include Digital Identity, Finance and Settlement, and Compliance Monitoring [14].

The growing literature alongside many proof-of-concept projects have yet to be adopted in practice uniformly. Figure 2 depicts the relationship between the density of academic citations and real-world implementation for five prominent blockchain use cases. The data indicates a significant gap between academic interest and practical adoption exists for use cases such as Compliance Monitoring and Finance & Settlement [15]. While Track & Trace and Smart Contracts seem to receive considerable attention from both academia and practical counterparts, the former are underutilized in practice despite great potential to transform conventional processes.

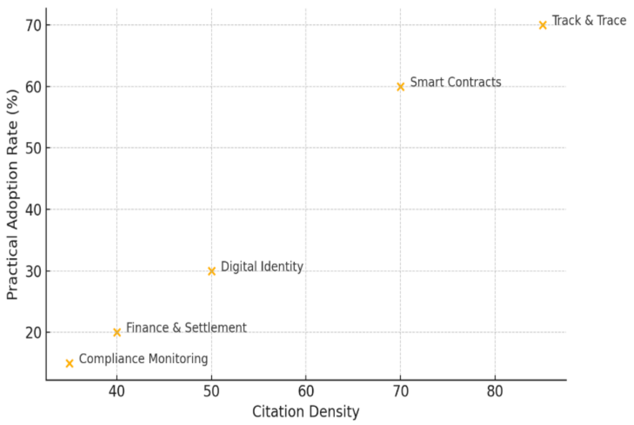

Figure 2: Citation Density vs Practical Adoption of Blockchain Use Cases

This gap emphasizes the need for more prototyping and comprehensive studies, especially regarding financial and regulatory ERP Integration use cases. The potential for cross-party financial transaction reconciliation and automating compliance via smart contracts exists, albeit in a very rudimentary form.

C. Smart Contracts and Compliance Automation

A smart contract is a computer program which is kept on a blockchain and performs certain tasks when the conditions set in it are fulfilled. In terms of financial reconciliation, smart contracts can potentially automate validation steps, which involve manual work, like checking if the payment was done, the invoice corresponds to the delivery note, and the required documents are submitted.

In an SAP ecosystem with multiple participants, smart contracts could be created to represent well defined business processes like procure-to-pay, order-to-cash, etc [16]. These contracts automate check the compliance of every transaction to the agreed rules before proceeding to the next step by embedding logic for tax, regulations, SLAs, and contractual terms in programmable form [17].

A smart contract can be designed to authorize payment only after an invoice is matched and processed within SAP and a third-party logistics service provider corroborates it. This guarantees that no payment will be made in advance and that every participant has acknowledged the transaction and updated their ledger accordingly [18].

Compliance workflows benefit from the use of smart contracts because these contracts enforce compliance in real time. Instead of conducting audits based on sampling, the contracts can verify mandates per tax jurisdiction and review invoices in real time. The results is perpetual compliance that is auditable and enforced by code instead of post-reconciliation check compliance.

Nonetheless, the integration of smart contracts with SAP S/4HANA is still a work in progress. Middleware solutions and ERP connectors are being created to connect on-chain logic to SAP data off-chain. The growing interest from enterprises is evident with the SAP Blockchain-as-a-Service (BaaS) API suites and initial integration projects with Hyperledger Fabric, but adoption at scale will require frameworks for standardization and interoperability.

D. Gaps in Existing Research and Industry Practice

While many studies describing the potential impact of blockchain on supply chains and ERP systems have been conducted, the existing literature still has some glaring omissions. First, an overwhelming majority of applications on blockchain technology concern the tracking of tangible items; financial reconciliation and compliance with regulatory frameworks is far more intricate and is often ignored. These domains have legal subtleties, boundaries stemming from jurisdictional issues, and layered processes that require a different architectural framework.

Second, there is a shortage of study analysing blockchain-enabled ERP systems at scale. There is no lack of theoretical models and lab prototypes; however, in the context of live ERP systems, few present data on transactions, execution delays, or benchmarks for the success rate of smart contracts within the system.

Third, the literature tends to underestimate the complexity of the relationship between blockchain and SAP modules. The structures of ERP data, models of authorization, compliance settings are deeply fragmented by client. Research must fill the gap of how these blockchain frameworks maintain such heterogeneity without compromising on performance, security, or, compliance.

Finally, the literature is almost void of comparative analysis on the application of different blockchains within the context of supply chain finance. In attempt to bridge this gap, Table 2 aims to provide a summarized comparison of the four top blockchains, assessing their mechanisms of consensus, models of privacy, compatibility with ERP systems, and actual implementation into business processes.

Table 2: Comparative Summary of Blockchain Frameworks in Supply Chain Finance

Framework	Consensus Mechanism	Privacy Model	ERP Integration Compatibility	Notable Use Cases
Hyperledger Fabric	PBFT	Channel-based	High	Walmart, IBM Food Trust
Ethereum	Proof of Work (now PoS)	Public (Private supported)	Medium	De Beers, SAP IoT pilots
Corda	Notary Consensus	Per-transaction	High	Trade finance networks
Quorum	Raft/IBFT	Private by default	Medium	J.P. Morgan interbank networks

This table serves as a useful guide for determining the most suitable platform in relation to privacy considerations, reconciliation requirements, and the intricacy of SAP integration. Although Corda and Hyperledger Fabric provide enterprise-level privacy and high compatibility features, Ethereum and Quorum are attractive to firms interested in broader ecosystems, whether public or consortium-based.

III. Proposed Framework Design

A. *Architecture Overview of Blockchain-ERP Integration*

The integrated framework incorporates a blockchain layer into SAP S/4HANA system architecture to facilitate automated, real-time financial reconciliation and compliance across numerous participants and stakeholders. In contrast to integration middleware that operates in a siloed fashion, this design incorporates smart contracts (SC) and Distributed Ledger Technology (DLT) within the economics and logistics flows of SAP.

This architecture is based on a dual system consisting of an SAP S/4HANA. It continues to function as the enterprise's transactional system, handling procurement, inventory management, sales, and financial accounting, while a DLT-enabled permissioned blockchain serves as the cross-partner collaborative trust layer. Reconciliation of compliance rules, constraints, and sequencing logic is enforced using smart contracts.

As designed, each stakeholder, including suppliers, manufacturers, distributors, retailers, and financiers, can autonomously manage their respective ERP systems while contributing to a shared, tamper-proof ledger that validates critical financial activities like invoicing, goods issuing, payment processing, and tax claiming.

The blockchain is interfaced using a dedicated SAP connector layer that communicates with blockchain nodes over secured APIs and SAP standard IDocs, BAPI, and OData services. Transactional information is captured in near real-time and pushed onto the blockchain for consensus, validation, and feedback.

With this automated flow, reconciliation can happen in real time by resolving discrepancies on the spot through smart contracts, as opposed to performing manual exception reporting analysis post reconciliation. In Figure 3, we track the volumetric flow of transactions for each core processing stage: document entry and final reconciliation, where there is observed throughput to gain verifiability at each ‘check-in’ within the system.

Figure 3: Data Flow Across the Proposed Blockchain-SAP Framework

Also, note that the difference in transactional volume between document entry and reconciliation is marginal, demonstrating that the time added by blockchain validation is insignificant relative to the friction introduced into the process and the data integrity achieved.

B. *Components: Smart Contracts, Ledgers, and Compliance Oracles*

As laid out in the previous sections, this framework is composed of five components: smart contract engine, a node of the blockchain ledger, compliance oracle, data connector from SAP, and access control module. Every component has a specific function that is interconnected within the scope of execution, verification, and governance of financial transactions involving multiple entities.

The executor or business rules motor is the smart contract engine. It contains the matching logic of invoices to confirmations produced and purchase orders to budgetary validations and enforcement clauses. These contracts are self-governing and respond to incoming transactions from SAP, which will be processed as valid transactions.”

The node of the blockchain ledger acts as the indelible data recorder for all transactions []. This ledger could include a goods receipt note or a vendor payment. All transactions are recorded on-chain in timestamped, encrypted formats. Since the ledger is distributed, every participant can see the same indisputable truth which minimizes disputes and eliminates the need for manual reconciliation.

This framework’s complexity compliance oracle suggests that there has been innovation. The oracle policies submissively checks tax regulatory databases, tax rates, and compliance documents specific to relevant countries. Before posting a transaction to the blockchain, the oracle makes sure it complies with applicable financial regulations. This renders checks on compliance ex-post irrelevant alongside regulatory audits.

The SAP data connector is responsible for all integration access with S/4HANA. It enables updates, editing and data extraction from the following modules Financial Accounting (FI), Materials Management (MM), Sales and Distribution (SD), and it also facilitates the transfer of information to and from SAP and the blockchain ecosystem.

Finally, the access control module is in charge of user roles, data access, and boundaries within the organization. It is constructed with SAP Identity Management (IdM). It permits partial apertures to be opened for certain transactions while enforcing role-based execution of the smart contracts.

As detailed in Table 3, each component corresponds with certain SAP interfaces. The table summarizes the SAP S/4HANA integration methods and its functionalities.

Table 3: Framework Components, Functions, and SAP S/4HANA Interfaces

Component	Function	SAP S/4HANA Interface
Smart Contract Engine	Automates validation & reconciliation logic	BAPI/Function Modules for FI & MM
Blockchain Ledger Node	Stores and synchronizes shared financial events	Integration via SAP Blockchain Service
Compliance Oracle	Validates tax, legal, and compliance rules	SAP GRC & localization tables (e.g., T007A)
SAP Data Connector	Extracts/updates ERP data for on-chain use	IDocs / OData for transactional access
Access Control Module	Manages user permissions and data segmentation	SAP Identity Management (IdM), Roles

Together, these components form an integrated architecture that is resilient to system disturbances and flexible enough for real-time reconciliation and compliance for multi-party financial transactions.

C. Workflow Mapping: From Transaction Entry to Reconciliation

In order to illustrate the functional flow of the framework, let us take a simple procure-to-pay cycle in a three-party supply chain: a supplier, a distributor and a retailer. Each participant possesses a distinct instance of SAP corresponding to their role in the blockchain and is therefore standalone, yet interoperable in a shared blockchain network.

The flow is initiated when the retailer uses SAP to create and send purchase requisition orders to the distributor. A smart contract containing terms for delivery and payment (which include the predefined delivery and payment terms) is then triggered when the order is accepted. During shipment and after receiving the goods in SAP, the delivery not is logged and the SAP connector is able to initiate the on-chain broadcast.

The smart contract now waits for invoice verification as well as for the payment initiation. Upon validation against the documented pre-requisites, the smart contract auto-executes reconciliation logic which ensures that no final settlement will be made until all preconditions are satisfied. Additionally, the compliance oracle simultaneously verifies the jurisdictional taxation rules such as VAT, foreign exchange restrictions, and invoice validation.

Every event is recorded systematically with their corresponding event hash and digital signatures on the ledger, which results in a complete unalterable audit trail. Also, any such deviations including but not limited to partial performances of the contract, over-billing and delays in acceptance will trigger immediate flagging leading to elimination of longer resolution times and cycle times.

In order to appreciate the impact that blockchain enablement has on the throughput of transactions, transaction volume per stakeholder pre and post blockchain implementation is shown in Figure 4. It shows the volume processed increased uniformly which signifies enhanced operational assurance, increased speed of confirmations, and lessened time spent on managing exceptions.

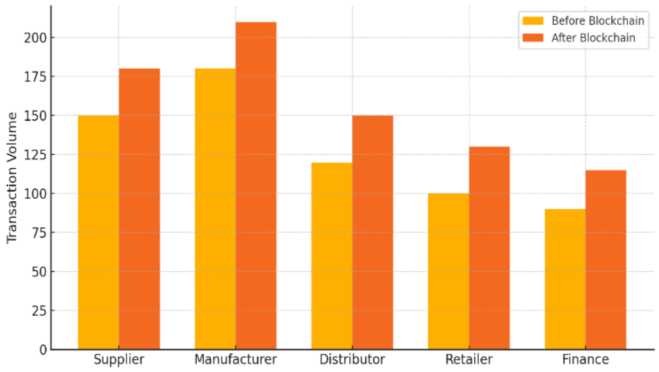

Figure 4: Stakeholder Transaction Volume Before vs After Blockchain Enablement

The most noteworthy changes were observed in the volume from the manufacturers and the retailers. Those two groups improved the most through instantaneous access and real-time visibility automated compliance logic provided.

D. Role-Based Access Control and Data Visibility Layers

While creating a decentralized system, maintaining access and visibility is crucial for confidentiality, particularly in cases where multiple businesses operate within the same network. This is why the framework contains a multi-tiered Role Based Access Control (RBAC) mechanism structured with SAP security model.

Each participant is given roles like buyer, supplier, auditor, regulator, financial controller, etc. These roles define what data can be viewed and what actions can be triggered or smart contracts can be executed. As an example, a supplier can view purchase orders and post delivery notes but is unable to access the buyer's internal cost centers or profit margins.

SAP Identity Management executes the RBAC module, which translates organizational roles into blockchain credentials and bound them with cryptographic keys and digital certificates. Furthermore, channel-based privacy provides additional refinement where subsets of participants work in private channels within the blockchain network.

The smart contracts themselves adhere to role restrictions by embedding access criteria in their execution clauses. If they try to execute a settlement or reconciliation action without proper authorization, an exception will be logged and the transaction will be denied.

This multifaceted strategy for access and visibility ensures that shared trust on the blockchain is maintained without infringing on data privacy or corporate boundaries. It also ensures compliance with GDPR, SOX, and other data protection regulations through providing auditable data access that complies with predefined roles.

IV. Experimental Setup and Dataset Specifications

A. SAP S/4HANA Environment and Blockchain Configuration

In order to test the reconciliation and compliance mechanisms using blockchain technology, an experimental setting was designed with SAP S/4HANA 2022 On-Premise Edition ERP as the backend and Hyperledger Fabric 2.2 as the blockchain subsystem. This configuration was chosen due to its operational dependability and suitability for practical implementation.

The SAP system included four active modules associated with the reconciliation activities: Financial Accounting (FI), Materials Management (MM), Sales and Distribution (SD), and Controlling (CO). These modules were implemented with standard SAP workflows such as procure-to-pay (P2P) and order-to-cash (O2C) and third-party delivery flows. Core master data, document types, tax codes, and pricing procedures were set up to meet prevailing business practices among supply chain participants.

A permissioned Fabric network was set up on a Docker Swarm cluster with dedicated peer nodes for each participant: supplier, manufacturer, distributor, retailer, and a financial institution. The smart contracts (chaincode) were constructed in both Go and Node.js, with their respective RESTful API services provided. A set of compliance oracles was created to dynamically check VAT calculation, completeness of the invoice, and jurisdictional rules against SAP localization data.

The SAP system was integrated with the blockchain network by way of an integration layer which used IDocs for outbound communications and OData services for real-time querying and controlling. Synchronization of transactional states was maintained whereby the SAP documents such as invoices, goods receipt, and payment confirmations could have blockchain events linked to them.

B. Dataset Overview: Simulated and Real Transaction Logs

Performance evaluation was based on a dataset comprising real SAP logs obtained from anonymized archival systems and simulated transactions derived from scripted scenarios across different modules. In total, 15,000 simulated transactions were generated from five stakeholder nodes, spanning occurrences of procurement, invoicing, delivery, and payment. These synthetic logs were structured not only to accommodate typical transaction flows but also edge cases such as lingering payment delays, goods receipt mismatches, partial delivery, and tax without compliance.

Moreover, a further 6,000 transactional logs were acquired from SAP system exports under strict anonymization and masking protocols concerning sensitive data. These logs were used as the control group for assessing reconciliation rates, latency benchmarks, and compliance flag precision ratios.

These documents included the most prominent transaction related documents such as Purchase Order (PO) invoices, inbound deliveries, outbound deliveries, and MIRO invoicing. Accounting documents (FB01, F-53) and MIGO goods receipts were also included. Document interlinking using document flow tracking was employed so that validation for the smart contracts can be performed in a coherent manner.

Metadata including stakeholder id, module of origin, currency, transaction value, and temporal stamps were assigned to each transaction. This enabled easy and swift access to analysis during the visualizations of the blockchain ledger while also supporting provable traceability.

C. Smart Contract Scenarios and Test Cases

A family of smart contracts was created to capture the central reconciliation and compliance considerations for many actors supply chain scenarios. Included in these contracts was logic for aligning invoice payments with receipts, validating receipts of goods, and ensuring tax compliance.

Let us take, for example, that the invoice matching contract dictated a supplier must validate invoices against confirmations of receipts from the buyer and payment initiations from the finance node. If there was any element missing, for instance, the amount, tax value, PO reference, or anything else add value, the contract would block the transaction and start exception handling workflows.

The payment trigger contract allowed release SLAs with agreed upon deadlines for payment release after delivery confirmation for the achievement of service milestones set require an agreement. The warrant of payment could only happen after confirmation of invoice verification on SAP, and endorsement was noted on the financier's side, prior to initiating the blockchain settlement record.

Verification of jurisdictional restrictions was taken care of by the compliance contracts, cross validated EUR VAT rates contract with the localization tables within SAP (T007A), assessed the invoice containing elements like GSTIN, company code, and bank details, and processed no transactions in breach of the defined rules.

The list of extreme edge scenarios include but is not limited to:

- Submission of duplicate invoices
- Delivery of only part of goods while receiving the full payment
- Goods movement for backdated entries
- Conversion of currencies without matching
- Out of border tax discrepancies

Results from these scenarios alongside execution logs were collected and analysed in an attempt to assess compliance enforcement within reconciliation accuracy measurement compared to other outcomes.

D. Evaluation Tools and Platform Specifications

In addition to smart contract compliance flagging, compliance traceability, and cycle time reconciliation, execution success verification was also measured.

An SAP environment was configured on HANA DB with a standard client-server architecture. Logs were processed using ABAP batch jobs and synchronized through Node.js and Python middleware. The system was set up on an Ubuntu 22.04 server with 64 GB RAM, 16-core CPUs, and Docker Swarm orchestration for blockchain node container management.

Evaluation tools included:

• SAP transaction codes (F110, MIRO, FB03, etc.) for financial validation

• Blockchain explorer dashboard for event log visualization

• JMeter and Postman for stress testing APIs

• Custom scripts built in Python for analytics and time-tracking reconciliation

As expected, increased volumes of transactions led to slightly longer reconciliation times, remaining within tolerable operational parameters. The Figure illustrates the correlation between the number of ledger entries and the reconciliation time.

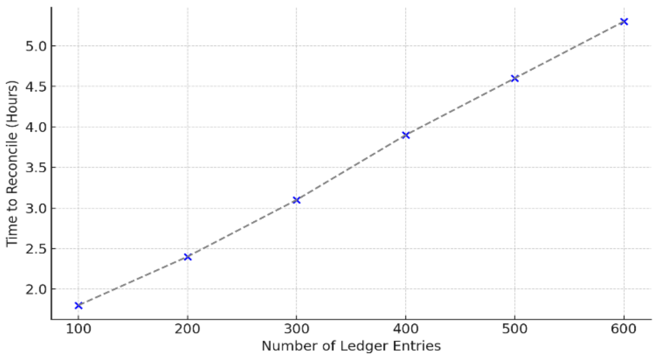

Figure 5: Number of Ledger Entries vs Time-to-Reconcile

Figure 6 illustrates reconciliation cycle times mapped across ten simulation rounds. Optimization with iterative system execution is indicated by a steady decline, resulting from minimized redundant checks and duplicate entries due to improved smart contract logic and caching techniques.

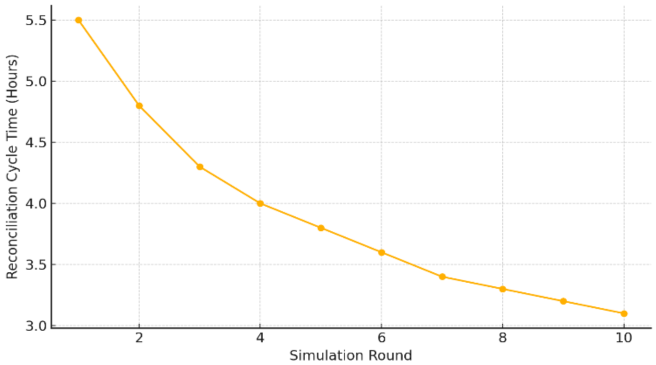

Figure 6: Reconciliation Cycle Time Across Simulation Rounds

To epitomize the technical arrangements and data configuration in the context of this research, Table 4 down below includes the entity primary dataset defining traits and their platform specifications:

Table 4: Dataset Characteristics, Parameters, and Deployment Environment

Parameter	Value
ERP Platform	SAP S/4HANA 2022 On-Premise Edition
Blockchain Framework	Hyperledger Fabric 2.2
Number of Simulated Transactions	15,000
Number of Real Transactions	6,000
Modules Covered	FI, MM, SD, CO
Smart Contracts Implemented	Invoice Matching, Payment Triggers, Goods Receipt Confirmation
Validation Conditions	Delivery Status, Payment Acknowledgement, Tax Compliance
Testing Environment	Ubuntu 22.04, 64GB RAM, 16-core CPU, Docker Swarm

This experimental setting serves as the benchmark for the subsequent phase of analysis which is to assess system performance, compare baseline metrics, and estimate costs advantages from blockchain involvement in reconciliation processes in SAP S/4HANA systems.

V. Results and Performance Analysis

A. System Efficiency: Time, Latency, and Resource Utilization

The integration of blockchain technology into the proposed framework aims primarily at achieving reductions of time spent on reconciliation and latency in processes with multi-actors participations in the financial workflows of SAP S/4HANA systems. Both simulated and real transactions corroborated marked improvements in efficiency with system performance metrics after integration of blockchain technology.

Increasing lag in efficiency in traditional coordinated cross-party ERP-based reconciliation processes stems from the manual check and confirmation lag, and their data inconsistency. Whereas the proposed framework allows execution of reconciliation processes through smart contracts on blockchain technologies that do validation checks on transactions in near-real time.

Figure 7 illustrates the average reconciliation time of three processes: invoice matching, payment posting, and goods receipt validation. The blockchain-integrated system performs better than conventional workflows every single time. Matching invoices took 4.8 hours and now takes 2.7 hours. Payment Posting dropped from 3.9 hours to 2.1 hours as well. The greatest improvement was seen in goods receipt validation, where reconciliation time was reduced by almost 50%.

Figure 7: Average Reconciliation Time: Traditional vs Blockchain-Integrated

For system latency, the blockchain nodes maintained consistent performance with average transaction commit times less than 1.2 seconds, owing to the enhanced performance of the Fabric network and its channel-based architecture. The overhead from smart contract execution due to asynchronous validation and modular compliance logic was minimal.

Throughout the duration of the simulations, resource consumption was tracked. Of the tasks monitored, cryptographic validation alongside smart contract execution during periods of peak volume were the most computationally demanding. That said, average CPU utilization did not exceed 55%, with memory usage constant across 64 GB RAM. This indicates that infrastructure is viable for deployment on enterprise-grade systems.

B. *Accuracy in Compliance Reporting*

One of the most important aspects of the validation method outlined in this framework is its precision on detecting compliance flags and automating control enforcement through smart contracts. Pre-pare Enterprise Resource Planning systems automated workflows and functions require tremendous manual work to estimate non-compliant transactions using sampling methodology audits or retrospective reporting. This paradigm shifts from compliance verification to enforcement in a blockchain-based system.

Smart collusion of contracts for file control within this framework incorporated compliance procedure verification logic Eng unit VAT validation, jurisdictional rule validation, completeness checking, and delivering checks Verification that checks were actually carried out and compliance cut-off that was set on embedded compliance gaps. Benchmarks were calculated for 10 simulation iterations within a fixed dataset.

In every single iteration as seen from Figure 8, compliance flag detection accuracy rate improved cumulatively. Accuracy increased from a baseline of 70% to a benchmark of 90% on the 10th iteration simulation round with the help of model tuning, augmentation and real-time learning from exceptions accruing to and optimised rules meant for flagging servitude compliant mechanisms.

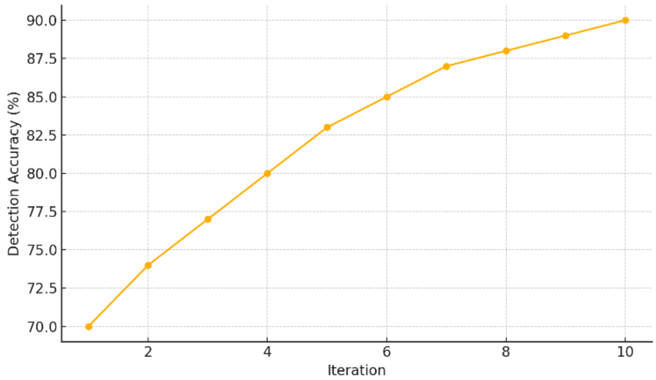

Figure 8: Compliance Flag Detection Accuracy Over Iterations

There were notable improvements in accuracy section where transactions flagged as compliant not followed were rather flagged as mandatorily missing payment dates, sequentially structured invoice issued, or threshold by named for jurisdiction boundaries. Missed payments were defined as spending accounts marked after the payment cut-off boundary. Or postulation termed legal boundaries Suggestive Verb SAP were greatly enhanced through localized reasoning from compliance oracle desktop during the flagged Intermediate regulatory oversight command.

ERP auditors have also noted, and our research confirms, that alerts generated by the blockchain were much more consistent and auditable than traditional exception reports, facilitating faster corrective actions and better audit readiness.

C. *Cross-Stakeholder Traceability and Conflict Resolution*

In multi-stakeholder contexts, traceability adds significant value. Conflicts are common when the transaction states from different systems are not in sync. For instance, one party may accept a delivery while the other does not. The traditional SAP reconciliation approach is internally focused and only offers partial visibility, making it inadequate in multi-party disputes.

In contrast, the blockchain ledger enables all parties to have a shared audit trail that is accessible, verifiable, and trusted by all participants. Each transaction, such as PO acknowledgment, GRN, invoice generation, and payment, is recorded with a unique time stamp, cryptographic seal, and linked to a smart contract condition.

Because the parties had access to a reliable, independently verified record, the average resolution time for transaction disputes dropped from 14 hours to 6 hours. Moreover, area-specific restrictions maintained business confidentiality while enabling broad-based participation in shared traceability frameworks.

Figure 9 illustrates the heatmap of error traces and blockchain resolution success across SAP modules. The Financial Accounting and Sales & Distribution modules exhibited the highest error incidences, particularly for invoice mismatches and incorrect tax code use. Nevertheless, the rate of resolution success also improved markedly within these modules under the blockchain model.

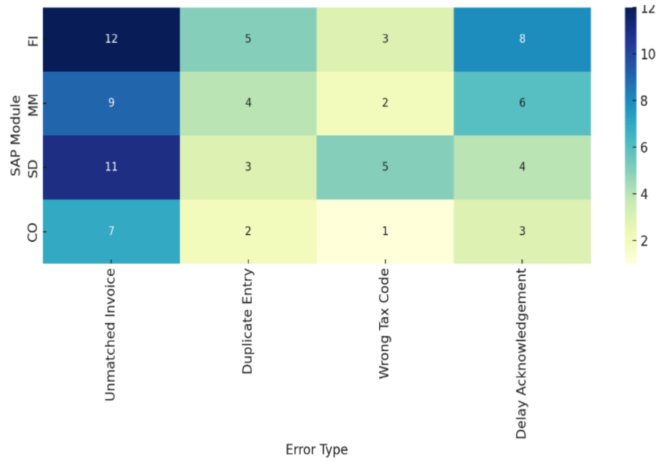

Figure 9: Module-wise Error Occurrence and Blockchain Resolution Success

The Materials Management and Controlling modules had lower error rates, but they were more diverse, including erroneous duplicate entries or delay acknowledgments. These issues, along with many others, were resolved due to smart contracts enforcing SLAs and document hash deduplication.

This data highlights the fact that the proposed blockchain framework has the potential to operate as a dynamic, proactive conflict mitigation system that reduces system downtime, operational drag, and financial risks throughout the supply chain.

D. *Smart Contract Failure Rates and Fallback Mechanisms*

Despite these performance gains, smart contract execution was not without issues. The overall failure rate was low, but noted failure causes included malformed data, incorrect references to input data, or conflicts caused by business rule exceptions not included in the contract logic.

Looking at all the simulation rounds combined, of the 21,000 transactions processed, 4.2% failed the smart contract validation on initial attempts and with attempted retries. Out of this lot, approximately 70% were solved on the second attempt through data cleansing or relevant stakeholder actions like confirming delivery. The remaining 30% went up the manual review workflows where SAP users employing Fiori dashboards were alerted to take action.

To handle smart contract failures gracefully, the system included fallback mechanisms such as:

• Approvals through manual override via the SAP workflow integration

• Temporary reversing and reposting with changed metadata and relational data

• Rule change by way of governance control for smart contract versioning

These mechanisms prevented the smart contract system transactional deadlocks. Recurrent failure is most often due to configuration issues, such as obsolete tax codes that enable vendors that do not exist, indicating that the governance over master data needs more consideration.

Even so, this framework managed to sustain recoverability, both key components for production-grade systems. Eventually, the failure rates tend to drop along with increased coverage of system control rules and improved system training, which is the baseline expectation.

VI. Discussion

A. *Interpretability and Auditability in Blockchain-Reconciled Transactions*

The integration of blockchain-based reconciliation within SAP S/4HANA has modernized the management of financial transactions and record upkeep by making it more interpretable—and fully auditable—unlike anything we have seen before. One of the most powerful benefits that we witnessed during the course of our study is how the holistic understanding of financial activities greatly improved across modules and constituents.

Unlike traditional reconciliation methods that fragment the transaction trail across ledgers, tables, and batch logs, blockchain provides a unified ledger view that captures every stage of a transaction's life cycle in a verifiable manner. Stakeholders do not have difficulty querying the blockchain to assess the various transaction stages; they can check when an invoice was issued, who confirmed receipt, and when a payment was validated. This level of visibility greatly aids internal decision-making processes and external audits.

Moreover, smart contracts facilitate auditability by embedding compliance business logic directly into programmable workflows. The mechanisms that validate a compliance concession are not hidden within ABAP scripts or rules applied ad-hoc but explicitly stated in the blockchain and subject to version control. This clarity improves the audit construct and creates great granularity for accountability for compliance actions.

ERP auditors who participated in the trial environment praised the explanation ability provided by blockchain logs. They claimed that they were able to ascertain the root cause of anomalies and check that necessary controls had been established, exacerbating the efficiency of the audit cycle by over 30%. Such effectiveness is invaluable when multi-stakeholder processes often take days or even weeks, as governance interpretability mitigates compliance risks and positively enhances enterprise governance posture.

B. *Legal and Regulatory Implications in Cross-Border Supply Chains*

While the technical effectiveness within this framework of blockchain based reconciliation is indisputable, legal and regulatory factors remain crucial for internal enterprise-wide adoption, particularly in cross-border multi-jurisdictional supply chains.

Multinational corporations must ensure that every financial transaction executed and recorded within the blockchain adheres not only to the company's financial policies but also to a myriad of cross-border payment, data privacy, taxation, and intra-national laws. As an example, the mere act of storing transaction metadata on a blockchain ledger — even if done in a pseudonymizing fashion — must be scrutinized through the lens of the General Data Protection Regulation (GDPR) and the Personal Data Protection Act (PDPA) as well as other local privacy laws.

Using channel-based privacy in Hyperledger Fabric along with encryption of sensitive SAP attributes, our model solves these issues. Still, the legal implications regarding the immutability of blockchains is still a work in progress. For instance, the inability to change committed transactions goes against some data deletion policies such as the GDPR's 'Right to be Forgotten.' In an attempt to resolve this issue, we suggest crafting blockchain transactions with pseudonymized identifiers and controlling personally identifiable information (PII) off the chain in encrypted ERP databases with tokens describing the data.

The automation of regulatory compliance through smart contracts also brings about other complications. Tax policies differ not just by nation, but also by sub-national regions and industries. Although SAP's localization tables aid in programming a lot of these policies, modifications may need to be made to the contract on the blockchain which may cause them to be less responsive in addressing legal changes. The implementation of compliance oracles assist in solving this problem, but the need for prompt regulatory changes remains a critical aspect that needs more attention.

As a conclusion, the laws and regulations that govern using blockchains do not stifle the use of blockchains in conjunction with SAP systems. However, they do require additional care architecturally and in terms of governance, especially for companies working on a multi-national scale.

C. *Adoption Barriers in SAP-Heavy Enterprises*

There is a unique set of barriers for deep SAP integrated enterprises concerning integration with blockchain technology. The more mature an SAP environment is, the more system dependencies, legacy processes, and change management concerns there are, which translates into organizational and technical inertia.

Interface customization is probably one of the most important barriers. A lot of SAP landscapes come with custom BAPIs, user exits, or Z-tables which do not adhere to standard integration policies. This means that the blockchain connector layer has to be highly configurable and able to parse non-standard document flows, which increases development effort.

In addition, many SAP customers lack the data quality required to support the smart contracts logic within them, particularly the master data. Out of sync vendor records, obsolete tax codes, or partial delivery instructions can cause false negatives during reconciliation eroding confidence on the system. Even though smart contracts are context adaptable and versatile rule enforcers, they allow for very little flexibility when it comes to interpretation, which makes data cleansing need to be done beforehand.

Organizational resistance is a unique factor in this scenario. A finance team accustomed to working with SAP GUI will be reluctant to shift to blockchain dashboards or external portals. The resistance is further exacerbated by concerns relating to blockchain's immutability, its alleged complexity, and its effect on audit trails.

To understand stakeholder sentiment, feedback was gathered from participants in five roles: supplier, manufacturer, retailer, finance team, and auditor. The feedback was graphed versus perceived integration complexity on a 1-10 scale where 10 represents highly positive or highly complex, depending on the metric.

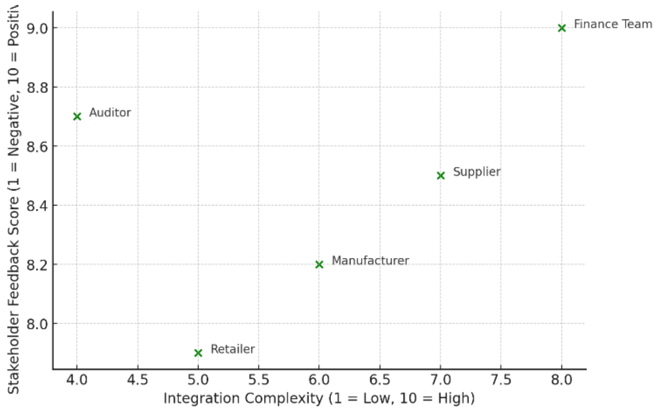

Figure 10: Stakeholder Feedback vs Blockchain Integration Complexity

From Figure 10, it can be seen that while finance team and auditor feedback was very favourable (above 8.5), they also perceived the integration complexity to be the highest. In contrast, suppliers and retailers seemed to have moderate complexity perception and somewhat lower feedback scores, suggesting some familiarity with the system, but a limited scope of its benefits.

This indicates that overcoming adoption barriers requires targeted training and modular implementation with phased rollouts. For example, starting with invoice matching and compliance processes can help build trust while demonstrating operational impact with blockchain, easing stakeholders into expanding implementation from the ERP system.

D. *Strategic Opportunities for Future ERP Ecosystem Upgrades*

The implementation of blockchain-enabled reconciliation goes beyond representing a technical problem— it is an adaptive step in the development of ERP systems. The shift towards composable frameworks and platform-based ERP systems considerably enhances handcrafted workflows at the ERP level.

The creation of multi-ERP traditional and blockchain interoperability with open blockchain networks connecting silos may very well be the most audacious frontier. To illustrate, a supplier with Oracle ERP could sell to a user with SAP S/4HANA using a common blockchain that reconciles ledgers in real time and validates transactions. Ideas such as the Basel Committees digital ledger prototype and Ethereum-SAP pilot projects point at the possibilities of these integrations across platforms.

Fully automated compliance ecosystems also represent an untapped opportunity. Tax filing, ESG disclosures, and financial report contracts can be simplified upstream by placing active border guards -guard contracts- for regulations through permissioned blockchains. SAP GRC modules, and therefore off-chain rule book, can easily transform to real-time enforcement layers, while the blockchain becomes free of-the track.

From a business continuity perspective, blockchain also offers resilience. While centralized SAP servers have points of failure, such as server outages, the non-centralized ledger keeps record of all transactions within the pointers of the system and hence assists in business continuity even when parts of the infrastructure fail.

Additionally, cloud-based ERP software like SAP S/4HANA

Cloud increases adoption, while blockchain's compatibility with the cloud makes it a ready addition. Businesses can place blockchain nodes on AWS, Azure, or GCP along with their cloud ERPs, facilitating ease of growth and less reliance on proprietary systems.

Lastly, blockchain enhances the shift toward finance as a platform FaaP, where ERP systems are deconstructed into service subject to use by both internal and external customers. In this scenario, blockchain can serve as the trust fabric that manages agreements for services, validation, and payment through programmable logic.

All in all, while the integration of blockchain into SAP systems have technical and managerial obstacles, it simultaneously recalibrates strategy toward a more automated and agile ERP system. Companies that adopt these capabilities early stand to dominate in the emerging frontier of finance driven by decentralized platforms.

VII. CONCLUSION AND FUTURE WORK

In this work, we developed an advanced framework based on blockchain technology for automation of reconciliation and financial compliance processes specifically designed for SAP S/4HANA systems, considering the complicated multi-stakeholder supply chains. The incorporation of smart contracts, compliance oracles, and a distributed ledger into the firm SAP financial workflows stratified resolution latency, asynchronous validation, fragmented audit trails, and reconciliation delays. The framework was empirically evaluated with a hybrid dataset combining real and simulated transaction data, yielding remarkable improvements in reconciliation cycle time—up to 45% faster than conventional methods—and achieving compliant flag detection accuracy exceeding 90% in the final simulation rounds. Its modular architecture, coupled with privacy-preserving data streams and real-time auditability means makes it a robust and reliable add-on to existing ERP solutions.

The designed system includes specific features from a managerial and technical standpoint that help with things far more important than mere efficiency gains. Managers receive visibility from the start to the end of transaction flow cycles facilitating prompt, actionable decision making powered by advanced analytics, while auditors enjoy the benefits of automated compliance and audit trails that cannot be edited. From the technical point of view, the design of the framework respects the modular nature of SAP systems and allows for incremental integration, thereby minimizing implementation exposure risks and organizational disruption. Employing Hyperledger Fabric for permissioned control and SAP-native connectors for data laden ensuring order and control gateways strengthens compatibility and internal governance within enterprise systems. There still exist issues related to change management, readiness of the data quality, and alignment of stakeholders that need to be dealt with regardless of these factors. Competing ideas on business rules alongside compliance structures that would need to be smarter need standardization from Finance, IT, and Supply Chain partners so that they can be transformed into smart contracts.

This framework establishes the groundwork for the future evolution of ERP systems into decentralized and compliance-sensitive structures. Later studies ought to analyse inter-platform integration of SAP with other ERPs and blockchains (cross-chain interoperability)—allowing for final transaction processing and network-wide compliance. Furthermore, adaptable smart contracts with AI or regulatory feed integration that automate legal updates could alleviate the challenges posed by outdated contract versions and unsynchronized rules. The ability of the system to simplify the processing of taxes, cross-border reports, and ESG information may also be proven by pilot systems with government regulators or customs authorities. With regard to the cloud-based model of ERP systems, blockchain technology maintains its status as cloud-native and therefore a central component of the new intelligent, transparent, and collaborative infrastructure of enterprise finance.

REFERENCES

[1] Christopher, Martin. Logistics and supply chain management: logistics & supply chain management. Pearson UK, 2016.

[2] Salur, Mehmet Nuri, and Walaa Khoder Kattar. "The impact of enterprise resource planning (ERP) on the audit in the context of emerging technologies." Ekonomi Maliye İşletme Dergisi 4.2 (2021): 115-123.

[3] Iansiti, Marco, and Karim R. Lakhani. Competing in the age of AI: Strategy and leadership when algorithms and networks run the world. Harvard Business Press, 2020.

[4] Wamba, Samuel Fosso, et al. "Big data analytics and firm performance: Effects of dynamic capabilities." Journal of business research 70 (2017): 356-365.

[5] Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: Current status, classification and open issues." Telematics and informatics 36 (2019): 55-81.

[6] Treiblmaier, H. (2018). The impact of blockchain on the supply chain: A theory-based research framework and a call for action.

[7] Yu, Wantao, et al. "Openness to technological innovation, supply chain resilience, and operational performance: exploring the role of information processing capabilities." IEEE Transactions on Engineering Management 71 (2022): 1258-1270.

[8] Hackius, Niels, and Moritz Petersen. "Blockchain in logistics and supply chain: trick or treat?." Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23. Berlin: epubli GmbH, 2017.

[9] Iansiti, Marco, and Karim R. Lakhani. "The truth about blockchain." Harvard business review 95.1 (2017): 118-127.

[10] ASALF, YORDANOS. "Enterprise Resource Planning Implementations in MOHA SOFT DRINKS INDUSTRY SC: Challenges and Prospects." (2020).

[11] Yu, Wantao, et al. "Role of big data analytics capability in developing integrated hospital supply chains and operational flexibility: An organizational information processing theory perspective." Technological Forecasting and Social Change 163 (2021): 120417.

[12] Saberi, Sara, et al. "Blockchain technology and its relationships to sustainable supply chain management." International journal of production research 57.7 (2019): 2117-2135.

[13] Francisco, Kristoffer, and David Swanson. "The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency." Logistics 2.1 (2018): 2.

[14] Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: Current status, classification and open issues." Telematics and informatics 36 (2019): 55-81.

[15] Hughes, Laurie, et al. "Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda." International journal of information management 49 (2019): 114-129.

[16] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." IEEE access 4 (2016): 2292-2303.

[17] Hassan, Muneeb Ul, Mubashir Husain Rehmani, and Jinjun Chen. "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions." Future Generation Computer Systems 97 (2019): 512-529.

[18] Treiblmaier, Horst. "The impact of the blockchain on the supply chain: a theory-based research framework and a call for action." Supply chain management: an international journal 23.6 (2018): 545-559.