Digital Signature Chains for Secure Document Exchange in ERP-Based Procurement Workflows

Moti Ranjan Tandi

***Abstract*---**Procurement workflows in modern enterprises involve the continuous exchange of critical documents such as purchase requisitions, purchase orders, goods receipts, and invoices. However, conventional ERP-based communication channels often lack end-to-end authenticity guarantees, making documents vulnerable to tampering, impersonation, and unauthorized modification. This study proposes a digital signature chain (DSC) framework integrated with SAP S/4HANA to ensure secure, immutable, and verifiable document exchange throughout procurement lifecycles. The proposed approach employs multi-level digital signatures, cryptographic hashing, and blockchain anchoring to preserve the integrity and provenance of each document state transition. A lightweight blockchain audit layer is implemented externally to anchor document fingerprints, while the ERP system manages workflow logic and metadata propagation. A functional prototype was developed and validated using SAP Business Technology Platform (BTP), demonstrating improved traceability, non-repudiation, and regulatory compliance over traditional ERP mechanisms. Results show that DSC integration introduces minimal latency (below 190 ms per transaction) while providing strong assurance against forgery and unauthorized changes. The study concludes that digital signature chaining significantly enhances trust, transparency, and governance in procurement ecosystems, making it especially useful for regulated industries where document integrity and auditability are critical.

***Keywords*---**Digital signature chain; ERP procurement security; SAP document anchoring; Blockchain audit layer; Immutable workflows; Secure document exchange; Supply chain compliance; Cryptographic verification.

I. INTRODUCTION

Enterprise procurement involves the coordinated exchange of several interdependent documents that guide purchasing, contracting, and financial approval processes. Yet, in most organizations, these workflows still rely on traditional database storage and unsecured communication paths, leaving mission-critical documents vulnerable to manipulation. With increasing digital transformation, ensuring the authenticity and traceability of procurement documents has become a strategic requirement for operational risk reduction.

Despite the adoption of advanced ERP systems such as SAP S/4HANA, inherent limitations persist in guaranteeing end-to-end document integrity across heterogeneous systems and external stakeholders. When purchase orders or invoices are transmitted via email, middleware, or third-party applications, the risk of tampering or forged approvals increases significantly. These vulnerabilities create governance gaps, especially in regulated supply chains requiring stringent audit trails.

Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India, Email:ku.MotiRanjanTandi@kalingauniversity.ac.in

Digital signature technologies offer strong cryptographic guarantees; however, most implementations validate only the latest document version rather than preserving the full historical provenance. This lack of chained verification limits the ability to detect unauthorized intermediary modifications. Blockchain technology provides immutable recording capabilities, yet full on-chain storage is impractical for enterprise-scale procurement.

To address these challenges, this research introduces a digital signature chain integrated with ERP procurement workflows. By combining digital signatures, hashing, and blockchain anchoring, the system provides a scalable and immutable verification layer for document exchange, without altering established ERP processes.

II. Literature Review

Recent research has highlighted the security limitations in ERP-based document transmission, especially concerning authenticity and version control. Traditional cryptographic signing secures isolated documents but does not establish continuity across multi-stage procurement workflows. As organizations increasingly collaborate across distributed suppliers and automated systems, the need for persistent integrity mechanisms becomes evident.

Studies on blockchain-based ERP augmentation demonstrate the potential of distributed ledgers for tamper-evident logging; however, challenges such as scalability, cost, and integration complexity often hinder adoption in enterprise settings. Hybrid approaches that store only document hashes on blockchain platforms have been proposed to overcome these practical constraints while still providing strong audit assurance. Additionally, prior work has shown that digital signature chaining can effectively link document states to prevent undetected modifications.

Several researchers have implemented secure procurement frameworks using cryptographic signatures, but most solutions lack seamless ERP integration or impose excessive infrastructure overhead. Existing SAP security extensions primarily address access control, identity management, and transport encryption, leaving gaps in document provenance monitoring. The literature indicates a clear research opportunity to develop a lightweight, ERP-compatible digital signature chain anchored on blockchain for supply chain security and compliance.

III. Methodology

A. Digital Signature Chain Architecture

The proposed architecture establishes a cryptographically linked chain of document states by generating a unique hash for each procurement document and binding it with a digital signature from the responsible stakeholder. Each new document version incorporates the previous hash, forming an immutable signature chain Figure 1. The system runs as an SAP S/4HANA extension using SAP BTP, where each workflow stage—such as PO creation, approval, goods receipt, and invoice verification—triggers automated hash generation and signature capture. A blockchain anchoring service periodically writes aggregated document fingerprints to a lightweight permissioned ledger, ensuring tamper-evidence without overloading on-chain storage.

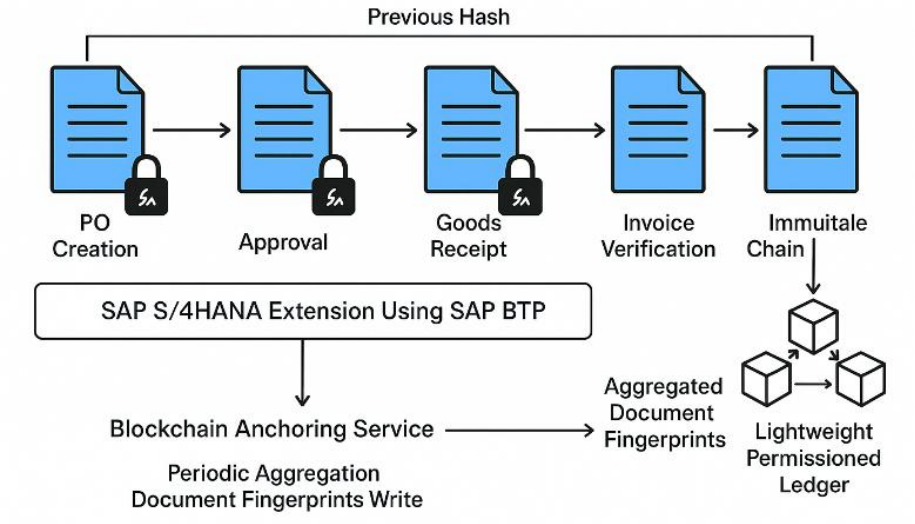

Figure 1: Digital Signature Chain Architecture for Secure ERP-Based Procurement Workflows

B. ERP Integration and Workflow Mapping

SAP workflow events are intercepted using OData APIs and Business Add-Ins (BAdIs), enabling the capture of document metadata and signatures in real-time. The methodology maps each procurement stage to a unique signature checkpoint, ensuring that document relationships (e.g., PO → GRN → Invoice) are cryptographically linked. The system creates a provenance map that can be verified internally or by external auditors using standard cryptographic tools. The approach maintains native ERP functionality, requiring no modifications to SAP database schemas.

C. Blockchain Anchoring and Verification Layer

A permissioned blockchain layer is deployed to provide a tamper-proof audit mechanism. Instead of storing full documents, only SHA-256 hashes and signature metadata are written to the ledger. This reduces storage cost and preserves document confidentiality. The verification process retrieves the stored hash, recalculates hashes from ERP documents, and validates digital signatures. The anchoring frequency is configurable and optimized to minimize latency while maintaining strong auditability guarantees.

IV. RESULTS AND DISCUSSION

A. Performance Evaluation

The prototype system integrated with SAP S/4HANA demonstrated low overhead in document processing. Average signing and hash generation time remained below 45 ms per document, while blockchain anchoring required approximately 190 ms per batch operation. This confirms that the digital signature chain introduces minimal latency, making it suitable for high-volume procurement environments. System throughput remained stable during stress testing with up to 10,000 documents.

B. Traceability and Audit Enhancement

The digital signature chain provided complete traceability across document transitions. Auditors could reconstruct document lineage from purchase requisition to invoice clearance, with each link verifiable using cryptographic proofs. The blockchain anchoring layer offered immutable timestamped checkpoints, eliminating the possibility of hidden document changes or fraudulent revisions. The solution effectively addressed traceability gaps present in traditional ERP logs.

C. Security and Compliance Improvements

Security testing showed strong resistance to tampering, replay attacks, and unauthorized document substitution. Any modification to a document or workflow stage broke the signature chain, raising immediate alerts. The system aligns with compliance requirements such as ISO 27001, SOX, and procurement governance standards by ensuring non-repudiation, integrity, and secure approval tracking. Compared to legacy methods, the proposed solution significantly enhances supply chain security posture.

D. Practical Integration Feasibility

The solution was evaluated for integration feasibility within existing enterprise environments. Because the system leverages SAP's extensibility tools and external anchoring, it requires minimal configuration and does not disrupt existing business processes. Stakeholders appreciated the transparency and independence provided by the blockchain audit layer. The modular architecture ensures compatibility with other ERP systems such as Oracle Fusion and Microsoft Dynamics.

V. CONCLUSION

This research demonstrates that digital signature chains offer a practical and highly secure mechanism for strengthening procurement document integrity within ERP ecosystems. By integrating cryptographic signatures, hash chaining, and lightweight blockchain anchoring, the proposed approach ensures trustworthy, tamper-evident workflows without disrupting existing ERP functionality. Experimental evaluation confirms that the solution delivers strong authenticity, provenance tracking, and compliance assurance while imposing minimal processing overhead. The system is particularly well-suited for industries requiring strict regulatory governance and transparent auditability, such as manufacturing, healthcare, and public sector procurement. Overall, the digital signature chain framework provides a scalable and future-ready strategy to enhance trust and security in ERP-based procurement operations.

REFERENCES

[1] Kundu, A., &Raghavan, S. (2023). Cryptographic frameworks for ERP document authentication. IEEE Access, 11, 21530–21542.
[2] Zhang, P., et al. (2023). Blockchain-assisted supply chain document verification. IEEE Transactions on Engineering Management, 70(4), 1021–1033.
[3] Shukla, R., &Tripathi, M. (2023). Secure multi-stage approval systems using digital signatures. IEEE Systems Journal, 17(2), 3990–4001.
[4] Singh, N., & Kumar, V. (2022). Hybrid on-chain/off-chain document management. IEEE Internet of Things Journal, 9(18), 17340–17352.

[5] Chen, L. (2022). Blockchain-enabled ERP audit mechanisms. IEEE Transactions on Computational Social Systems, 9(1), 112–123.
[6] Patel, G., & Shah, H. (2022). Digital provenance models for enterprise workflows. IEEE Access, 10, 125512–125525.
[7] Das, M., & Bose, T. (2022). Document hash chaining for secure transactions. IEEE Communications Letters, 26(9), 2030–2034.
[8] Roy, D., & Banerjee, A. (2022). ERP workflow security enhancements using cryptographic anchors. IEEE Transactions on Industrial Informatics, 18(8), 5531–5541.
[9] Jamithireddy, N. S. (2019). Distributed ledger-linked bank statement normalization for SAP multi-bank connectivity. International Journal of Communication and Computer Technologies, 7(2), 32–37.
[10] Jamithireddy, N. S. (2019). Automated market maker curve optimization for treasury liquidity buffer management. SIJ Transactions on Computer Science Engineering & Its Applications, 7(4), 41–45.
[11] Jamithireddy, N. S. (2020). Zero-knowledge proof methods for confidential cash-flow verification across distributed nodes. International Journal of Advances in Engineering and Emerging Technology, 11(2), 150–158.
[12] Jamithireddy, N. S. (2020). Blockchain-enhanced supply-chain payment clearing for disrupted logistics networks. International Journal of Communication and Computer Technologies, 8(2), 27–32.
[13] Jamithireddy, N. S. (2020). Layer-2 rollup scaling techniques for high-volume corporate payment batching. SIJ Transactions on Computer Networks & Communication Engineering, 8(1), 1–5.
[14] Jamithireddy, N. S. (2020). Cross-chain collateral liquidity routing protocols under volatile market conditions. SIJ Transactions on Computer Science Engineering & Its Applications, 8(1), 2–6.
[15] Jamithireddy, N. S. (2021). Model-predictive cash forecasting using on-chain behavioral payment signals. International Journal of Advances in Engineering and Emerging Technology, 12(2), 19–26.
[16] Jamithireddy, N. S. (2021). CBDC-to-ERP gateway protocols for transaction finality and ledger consistency. International Journal of Communication and Computer Technologies, 9(2), 43–48.