# Anchoring ERP Open Items on Distributed Ledgers: A GDPR-Compliant Approach for Enhanced Audit Trust

Jovan Dragojlovic[1][0009-0008-5158-2211] and Alexander Redlein[1][0000-0002-1659-6369]

[1] Institute of Management Science, TU Wien, Vienna, Austria

**Abstract.** The automation of business processes is a primary objective in contemporary management to address skilled labor shortages and minimize operational costs. In particular, invoice verification offers significant optimization potential, as the current process is characterized by extensive manual intervention, media discontinuity and inherent compliance risks. While blockchain offers a viable solution through immutable record-keeping, its practical application is hindered by a lack of practical knowledge, technical overhead and strict privacy regulations. Following the Design Science Research methodology, this paper addresses these challenges by introducing an optimized integrated process and a four-layer architecture to automate manual process steps of validating financial data and documents on a systemic level. The evaluation encompasses a functional proof of concept implementation utilizing a legacy ERP system and a government-managed consortium blockchain, followed by a qualitative comparison. The findings indicate that (legacy) ERP systems can be effectively combined with a decentralized trust layer to automate this process on a corporate scale. Furthermore, the architecture establishes a foundation for near real-time auditing and reduction of manual verification and reconciliation efforts.

**Keywords:** Open Item Verification, Process Automation, Blockchain, Enterprise Application Integration, Audit Automation.

## 1 Introduction

In today's increasingly interconnected global economy, the integrity of financial reporting sets the foundation of trust between corporations. Despite the rapid digitization of corporate finance, the auditing profession remains heavily reliant on manual processes, using sampling methods that leave a significant portion of transactions unverified [1], [2], [3]. In many organizations, Enterprise Resource Planning (ERP) systems support core functions by providing a range of tools for automation, organizational overviews, and processes for improved auditing [4]. However, recent studies [5], [6] indicate that the invoice verification process still relies heavily on manual intervention and suffers from media discontinuity. It lacks a comprehensive IT support of several process steps, prohibiting a fully automated verification of unresolved invoices (Open Items) prior to a corporate audit. Consequently, to mitigate the risk of subsequent data manipulation, regulatory frameworks such as the International Standards on Auditing (ISA) [7]

the case seems clear, albeit the mentioned problems notwithstanding. I hope it will get clearer afterward



mandate rigorous verification procedures to obtain sufficient audit evidence. Thus, providing measures and guidelines to adequately examine and report financial precision of both Accounts Receivable (debtors) and Accounts Payable (creditors). Ultimately, the crucial point for disputes in audits often pertains to the verification and acceptance of invoices by the debtor and creditor. The practical execution of such verification procedures can become increasingly time-consuming, often requiring weeks of data reconciliation and verification at the end of every fiscal year [5], [6], [8].

This paper focuses specifically on the Sales and Collection Cycle, which is regarded as one of the most resource-intensive phases of an organization's audit due to high volumes of individual transactions and the necessity of external compliance [3], [6], [9]. Given their susceptibility to fraud [5], [10], open items are of particular relevance under ISA 240 [11], requiring auditors to disclose irregularities in financial statements, risk management, and structured procedures. From an auditor's perspective, the pivotal aspect for disputes and discrepancies evolves around the communication between the examinee and its debtors [12]. As open items must accurately reflect valid yet unsettled invoices, this leads to a more granular audit trail of transaction statuses that is not automatically recorded by the underlying ERP systems. The process of traditional manual verification not only delays operational lead times within the audited company but also demands additional resources at the debtor's side and introduces new challenges to latency and manipulation risk into the auditing process.

To address these limitations, this work explores blockchain as an exemplary Distributed Ledger Technology (DLT) for securely logging and sharing missing transactions, enlarging the simple value chain by Redlein et al. [13]. This approach targets the following subset of activities where blockchain-based optimization offers the highest added value for automated audit compliance:

- Verification of Purchase Orders and Invoices (Account Payable)
- Validation of Sales Invoices (Accounts Receivable)
- Record of the Accepted Invoices and Incoming and Outgoing Payments

Complementary, expert workshops and interviews with international auditors, technicians, and domain experts were conducted to identify specific pain points in contemporary process and corporate audits. Consistent with theoretical insights, auditors frequently lack verifiable proof of explicit invoice acceptance by the debtor, necessitating manual verification.

In this context, blockchain is not only positioned as a technical tool but as an enabling technology for a new type of process using smart contracts for automating data verification, while providing trust for inter-organizational collaboration. To bridge the gap between the theoretical blockchain potential and a practical audit application, the following research are questions (RQ) are answered in this paper:

*RQ1: To what extent can the current manual process for invoice verification and auditing of open items be automated using blockchain and smart contracts?*

*RQ2: How should a system architecture be designed to ensure data integrity in ERP systems using Distributed Ledger Technologies (DLT) without passing on sensitive data to third parties?*

The research was designed according to the Design Science Research (DSR) framework by Peffers et al. [14], which follows a structured process and thus enables clarity and reproducibility. Finally, by integrating DLT and automating the open items verification and auditing process, this paper demonstrates a significant reduction in redundant process steps, manual exchange, media inconsistency and fraud risks. This approach not only minimizes the time required for manual data handling but also establishes a robust "single source of truth" that streamlines entire audit procedures within this subset.

The remainder of this paper is organized as stated accordingly. Section 2 sets the theoretical basis by describing fundamental concepts of ERP, blockchain, and financial auditing. In addition, it explores the current state of art. The underlying methodological approach is summarized in Section 3 including the steps taken to ensure practical relevance and scientific rigor. The next section, Section 4 details the problem analysis and requirements engineering to formulate a newly integrated reference process, serving as the structural basis for the proposed model. Accordingly, Section 5 delineates the design, development, and demonstration phases of the technical artifact. Then, Section 6 conceptually evaluates the proposed model and Section 7 discusses the findings and the broader implications for the auditing profession. Lastly, Section 8 concludes the key contributions of this paper and provides a brief outline future research.

ERP are important auditing often crucial

vs

but it's costly

## 2 Theoretical Background & Related Work

Traditional ERP systems integrate and support core business processes of companies, while providing a variety of features and options to connect to third party applications. This includes the context of auditing, in which ERP systems e.g. generate lists displaying issued but unpaid invoices or costs, which can be directly checked by auditors [15]. Therefore, auditors are often granted read-only permission in these systems to track and comprehend payment processes [16]. In the same instance, auditors are obliged to follow ISA 240 [17], to report fraudulent activities and conduct cross-checks with creditors or debtors retrospectively. According to Peng et al. [6] this process step is highly dependent on sufficient documentation and subsequent evidence by all included parties. In practice, the verification process frequently entails multiple iterative cycles – discrepancies between the issued invoice and the debtor's records necessitate revisions by the affected creditor before final and mutual approval can be achieved [18].

Research by Peng et al. [6] demonstrates that this circulation of documents requires 68% of the total time of the settlement cycle. Thus, relying on institutional trust rather than structural integrity creates an inherent "trust gap", rendering the traditional invoicing process both inefficient and insecure.

Although current theoretical and conceptual studies in cryptoeconomics [19], [20] advocate the integration of blockchain as a transformative force in accounting, industry-specific solutions remain sparse. A few pioneering studies have begun to address the mentioned systemic vulnerabilities, introducing novel blockchain-based schemes for bank audit confirmations [5] by integrating smart contracts for automated authorization and data acquisition. Further approaches [6] combine blockchain networks and

some advocate that BC can help in related fields

There are some success stories in other domains

BC needs still empirical evidence to prove it's useful

It's integrated with various systems including ERP

but we need to make it better

Bass is a way



smart contracts with Robotic Process Automation to create real-time settlement models in the aviation fuel supply chain, reducing compliance and cost due to shortened payment cycles. In this instance, the implementation of a blockchain-based real-time settlement model at China Southern Airlines successfully mitigated systemic inefficiencies, ultimately reducing the annual capital tie-up by approximately 1.26 billion CNY, thereby strengthening their bargaining power. A joint research project by employees of the companies X and IBM [21] further showcases the elimination of process redundancies for both Accounts Payable and Receivable and increased transparency using blockchain networks in the transportation domain.

Extant literature also suggests that blockchain technology represents a cornerstone innovation for financial systems, facilitating a transition from manual, error-prone reconciliation toward a model of automated verification [5]. Within this context, a majority of studies offer conceptual or theoretical insights, focusing on superficial blockchain integrations [9], [22], in other instances limiting their study to geographical regions [19], or enumerating key success factors for effectively integrating the technology. The systematic literature review by [20] and case study by [19] underscore a lack of comprehension regarding blockchain technology, call for shift towards more empirical investigations. Thus, expanding the body of practical experience becomes essential to bridge the gap between theoretical potential and industrial application, ultimately creating value for both research and practice.

More in-depth research deals with the integration of blockchain networks with existing procedures for security and validation of goods, services, and claims [21]. Very recent efforts emphasize the digitalization of these workflows by combining blockchain networks with complementary technologies. For instance, combining distributed ledgers with Optical Character Recognition for saving financial records [8] or leveraging Industry 4.0 technologies [23] to drive higher levels of end-to-end automation. An additional cluster of interest considers integrating blockchains and ERP systems to conduct secure and automized applications of payment [2], [24] or enhanced cross-organizational reconciliation [25]. Such decentralized coordination transcends geographical boundaries, enabling multinational corporations to maintain consistent, distributed compliance within differing legal jurisdictions [26]. Despite theoretical benefits, blockchain development encounters obstacles regarding scalability and operational costs compared to centralized solutions. Consequently, recent studies have introduced novel architectures exhibiting higher performance designed to mitigate these bottlenecks and offer substantial data throughput [27], [28]. Collectively, the academic and particularly practical focus is gradually shifting from theoretical exploration to an efficient technical operationalization of blockchain technology as a trust layer within standard enterprise systems. This characteristic can be observed in company reports [29], industrial product launches [30], and partly in academic literature dealing with Blockchain as a Service (BaaS). Hence, BaaS is seen as a truly efficient and effective asset to implement the advantages of blockchain networks into industrial workflows while reducing complexity and technical issues due to networking effects [1].

Accordingly, this paper builds on this state of research by developing an integrative model that optimizes the management of open items through using blockchain technology and smart contracts. The proposed solution addresses the structural vulnerabilities

to me, it's not really that interesting so far



we did a poc

by adding IT supported process steps, that enable automation. This is achieved by integrating blockchain technology, effectively replacing manual oversight with a decentralized foundation, which offers improved financial precision and efficiency.

In the end, this approach strengthens the trustworthiness of the overall process. For the detailed implementation and evaluation, a Proof of Concept (PoC) will be developed, utilizing the established BaaS solution of the Austrian Federal Economic Chamber (WKÖ), which embodies a publicly accessible, secure, and nationally trusted blockchain infrastructure.

## 3 Research Methodology

In summary, theoretical analysis exhibits that traditional audit procedures are reaching their limits due to media discontinuity, manual compliance, and the threat of manipulation of central ERP data. This paper responds by constructing an integrative model for the open item audit, which requires a design-oriented research approach for a comprehensible structure. Therefore, the methodology of Design Science Research for Information Systems according to Peffers et al. [14] is chosen to align the development and evaluation of technical artifacts for solving relevant business problems. The overall procedure is split into the three following phases:

### 3.1 Problem Identification and Research Objective:

In addition to the conducted literature review, expert workshops and interviews with international auditors, technicians and domain experts were carried out between September of 2024 and May of 2025 to identify the pains and needs considering current process models and corporate audits. For that, the initial workshop served to elicit operational pain points and primary end-user needs. Subsequent sessions facilitated an iterative refinement of the researched model, specifically defining characteristics of a suiting IT architecture. This multi-step process revealed implicit requirements of international auditors, which could be translated into concrete technical features. Further insights within traditional audit processes displayed a fundamental "trust gap", where reliance on manual, retrospective reconciliation and subjective institutional trust creates systemic vulnerabilities. As a consequence, financial workflows are prone to information asymmetry, data manipulation, and long inspection cycles. Additionally, the targeted process of inspecting open items after the predetermined accounting date is heavily impacted by media discontinuity, an increased manual workload and complex communication structures. In alignment with these issues, recent research [9] emphasizes the need for improved invoice verification and auditing processes. This section aims to define these new reference processes as a foundation for later automated verification. Finally, this offers systemic, cross-organizational integrity and trust.

I think a figure could be nice at this point to better understand

### 3.2 Design and Development of the Solution:

To design and develop the solution additional expert workshops were conducted to define the new reference processes and to specify additional requirements due to ISA, General Data Protection Regulation (GDPR) etc. More specifically, a dedicated workshop was conducted to explore technical approaches for optimizing the constructed reference process. Subsequent discussions highlighted the need for a robust IT architecture and encryption that enable practical applicability while providing a sufficient level of security. The basis for the new model is the traditional Open Item audit process which requires reconciliation primarily with the examinee and in some cases additional coordination with the examinee's business partners for Accounts Payable, Accounts Receivable, or both. The design aims to maintain operational media continuity and define the additional steps within the processes already existing in ERP systems, so that the process can be fully automated afterwards. In a second step, the IT support and the potential additional technologies like blockchain and smart contracts were examined in additional expert workshops. Several iterations were done to fulfill all requirements of the ISA leading to the new automated and fully Information and Communications Technology (ICT)-supported process. Further workshops prioritized effective auditability and stakeholder acceptance, which marked key deliverables of the optimized billing process. Both examinees and auditors benefit from a significant reduction in compliance efforts, as open items and their verification can be securely anchored in the blockchain environment. Additionally, to decrease organizational resistance due to technical overhead of maintaining a DLT, the proposed model leverages a BaaS solution, which minimizes resource requirements for corporate organizations.

. moderator of debents in the workshop settings

### 3.3 Demonstration and Evaluation of the model:

Lastly, to demonstrate the technical feasibility and practical applicability of the integrative model, a PoC implementation was conducted utilizing the mentioned BaaS infrastructure as the immutable trust layer, integrated with an SAP ERP system for the generation, storage, and management of financial documents. An automated email listener was employed to capture inbound confirmations from business partners. This configuration simulates a traditional reconciliation mechanism that records and verifies the business partner's acceptance before cryptographically anchoring the information in the blockchain environment. As the final methodological step, the proposed approach was validated within a final expert workshop with international auditors. These experts confirmed that the architecture successfully shifts the reliance from institutional to systemic trust. In addition, the architecture's minimally invasive design enables effective integration into contemporary corporate audit procedures.

→ OK that's the feeling of the expert, but is that true?

## 4 Problem Analysis and Requirements Engineering

The following section synthesizes theoretical insights and expert opinions to establish a solid basis for the latter practice-oriented design. For that, the proposed solution is built upon an optimized reference process developed collaboratively during the

aforementioned expert workshops. The resulting workflow is formally depicted as a flowchart in **Fig. 1**.

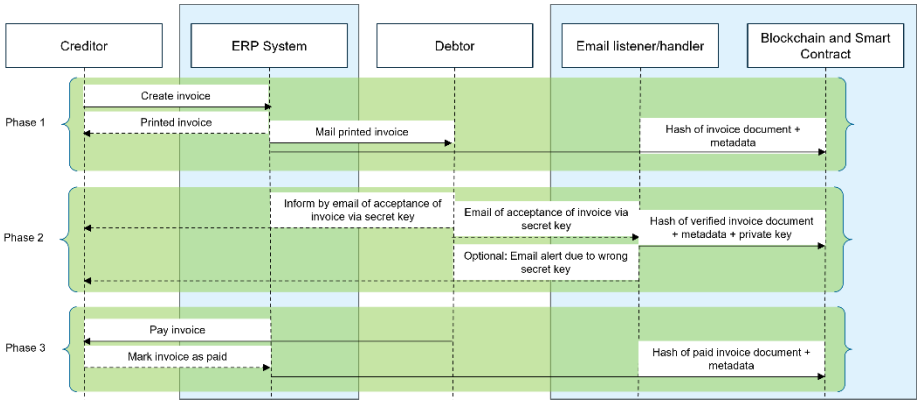


**Fig. 1.** Sequential process flow of the novel, integrated invoice confirmation procedure

The visualized parties are end-users of the creditor and debtor. The supplier (creditor) manages the Order-to-Cash (O2C) process using an ERP system. To reduce complexity, the initial process steps of a completed order, production, and potential delivery were skipped, thus focusing solely on the invoicing process. The creditor starts the function to create an invoice, which is issued by the ERP system and subsequently downloaded and mailed to the debtor. In this step, the hash of financial data, consisting of the billing document and corresponding metadata, is transmitted and stored in the blockchain network, which completes Phase 1. As soon as the debtor formally accepts the received invoice by replying with a previously shared secret key, the email listener forwards the saved hash of the accepted invoice document and metadata to the blockchain environment. Consequently, this marks the creation of the second entry, visible in the blockchain. If the secret key is incorrect, an email is sent to the supplier to inform about potential misuse (Phase 2). Finally, Phase 3 concludes the enhanced payment cycle by recording the incoming payment in the ERP system. Afterwards, the transaction status is automatically synchronized with the blockchain by appending an immutable "paid" tag to a newly created blockchain entry of the affected invoice.

how?

A central design objective was to ensure a non-intrusive integration for end-users while keeping the verification mechanism transparent. In more detail, an ERP system's Application Programming Interface (API) yields only encrypted invoicing data to a middleware service, which prepares, stores, and further calls predefined API interfaces of a BaaS infrastructure. Additionally, expert workshops indicated the necessity of a systemically resilient environment, which implies the incorporation of a simple fault tolerance mechanism for inter-systemic communication failures. Hence, in the event of API timeouts or endpoint unavailability, outbound payloads are asynchronously queued within a dedicated ERP's custom table or staging database. A continuously scheduled background process subsequently polls this queue, which ensures the delivery of

financial information to their target destinations. This includes billing documents, encrypted invoice metadata and documents, and payment updates.

By further synthesizing the identified practical requirements, process automations, and mutually agreed design principles, this research presents a novel, practically acknowledged, and integrated end-to-end process, which is illustrated in **Fig. 2**.

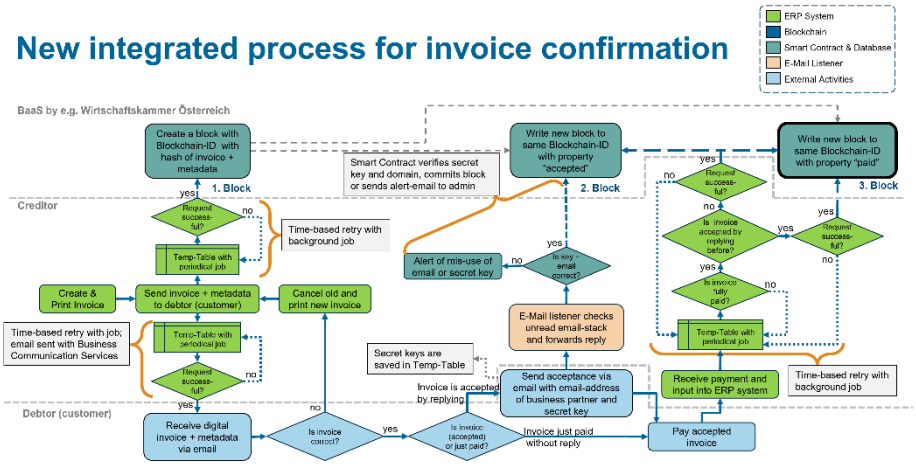


**Fig. 2.** Integrated end-to-end process split according to technical environment and stakeholders

Concluding the requirements engineering phase, this formalized workflow was rigorously validated and endorsed by international auditors to ensure both practical applicability and strict compliance, thereby providing a robust and approved baseline for the subsequent integrative model. fig 2 is too big can not described

## 5 Development of the Lightweight Integrity Data Anchor

Following the methodological framework of DSR, this chapter addresses and concludes the third and fourth phase by Peffers et al. [14]; design, development, and demonstration. The primary objective is to showcase and validate the technical feasibility of the developed artifact and therefore bridge the interoperability gap between legacy ERP systems and DLTs, followed by a qualitative evaluation of the resulting improvements for invoicing processes using enterprise systems.

Firstly, to delineate the technical intricacies of the detailed end-to-end process, this research abstracts the previously defined requirements into a generalized integrative architecture, which is showcased within a four-layer model visualized in **Fig. 3**.

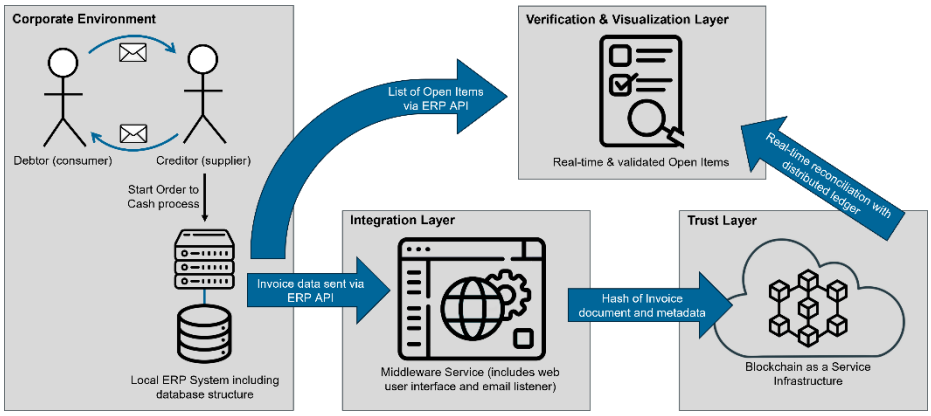


**Fig. 3.** Visualization of the proposed integrative model's four-layer architecture

The model strictly decouples the public verification proof (hash) from the private invoice data while providing near real-time validated open items to ensure that invoice content remains exclusively visible to the intended parties (Corporate Environment Layer). The resulting fundamental design principle considers strict data minimization, ensuring that sensitive billing data remains protected from unauthorized access. Within this step, only cryptographic fingerprints, thus the combined hash of the invoice document and metadata, leave the ERP system's database either to the Integration Layer or Verification and Visualization Layer. The Integration Layer serves as a link between the centralized ERP system and the decentralized BaaS, which transparently logs changes during a corporate's invoicing process. Similar to work by Sarwar et al. [31], the cryptographic hash function follows the standard of the SHA-256, which provides a fixed output of 256 bits. The concept can be simplified into a one-way mathematical function, where the hash is constructed using the original financial data, but the hash itself cannot lead back to the original data. Replicated to this context, financial datasets of varying dimensions are condensed into a fixed length, allowing for a highly efficient data storage footprint on the blockchain, further reducing costs. The strategy directly addresses the scalability and performance bottlenecks of blockchains, frequently emphasized in recent literature [32], [33]. The designated cryptographic fingerprint embodies a unique identifier of the billing data, which is passed through subsequent stages. Consequently, even if the hash is now visible to all blockchain participants no conclusions can be drawn to the original financial data. Finally, the cryptographic digest reaches the Verification and Visualization Layer, in which the hash serves as a unique anchor for automated reconciliation. this is no more than external data storage pattern

The latter audit process offers a dynamic overview by combining data from both, the ERP system's database filtered by unresolved invoices (Open items) and the cryptographic fingerprint including the exact timestamp retrieved from the BaaS. The actual verification process involves recalculating the cryptographic hash value based on the recently transmitted invoice documents and the associated metadata. This newly generated digest is then automatically compared to the blockchain entry. A match on character-level of these two values provides mathematical proof of integrity without the

need of a trusted third-party provider. Applied on a general scale, the results show that all verified open items are validated in near real-time, greatly reducing the effort for manual reconciliation and compliance with stakeholders.

this sound autinomic...

## 6 Conceptual Evaluation of the Implementation

Following the definition of the architecture's structure and design characteristics, this section implements the idea as a functional PoC prototype. As a first step, to facilitate the reproducibility of this experimental implementation, the core technical specifications and architectural configuration of the development environment are summarized in the following list:

- Corporate Environment Layer: SAP S/4HANA On Premise Release 2021 (FPS04) (Stack Release Date: 05/2023)
- Integration Layer: Hybrid-Approach consisting of a Python (3.12.6) backend and Node.js (20) frontend.
- Trust Layer: Consortium Blockchain of the WKÖ; Consensus mechanism: Proof-of-Authority
- Verification & Visualization Layer: Hybrid-Approach consisting of a Python (3.12.6) backend and Node.js (20) frontend.

custom code where's the line?

we have too few detail on this BC

The experimental setup was configured according to the integrated reference process defined in Section 4 . The Corporate Environment was simulated by generating, editing, and ultimately printing the invoice using the SAP transaction "Display Billing Documents" (Code: VF03), which represents the final phase of the internal invoicing workflow. The document can be either sent manually by the creditor to the customer, or it can be automatically sent by a developed custom report. A distinct characteristic of the SAP system is the utilization of a Spool Service for dynamic document generation, which enhances operational performance and storage efficiency. The resulting spool request is adapted by automatically converting the spool document into a Portable Document Format (PDF)-file. Next, the cryptographic digest of the PDF-file, together with the associated billing metadata, are transmitted to the WKÖ blockchain infrastructure via a predefined RESTful POST interface. The specific JSON scheme required for this transaction is defined in **Table 1**.

**Table 1.** Applied Properties of the JSON scheme for WKÖ's blockchain interface

| Field (JSON Key) | Data Type | Example |
|---|---|---|
| blockchainId | UUID | 550e7400-e11b-41d4-a716-446655430000 |
| sha256 | String (Length: 256 bit) | bc204f6a41feb89b……dcb1701b95b959 |
| remarks | Enum-String | "unaccepted", "accepted", or "paid" |

A successful acceptance of the invoice serves as the mandatory trigger for phase 2 (see overview in **Fig. 2**), which is predominately executed via an email reply including a shared secret key between both affected parties. To reduce the technical overhead for

how?

end-users an email listener was implemented on the creditor's side. Consequently, the validity check is automated by forwarding the content to a smart contract, which decides whether the shared secret key is correct. If the secret key provided is wrong the information will be sent to the creditor's email address to inform them about a potential misuse or lack of permission to formally accept the invoice. However, if the invoice is accepted by an authorized person and the secret key is correct, then the smart contract initiates the second entry on the blockchain infrastructure. We don't know the transaction details

During this step, the value of "remarks" is set to "accepted" in a new blockchain entry, which marks an acknowledged open financial position (Open Item), that awaits payment by the debtor.

Phase 3 takes place after the payment by the customer, in which the creditor receives the payment notification and inputs the paid amount into the SAP system using the transaction "Post Incoming Payments" (Code: F-28). Even though partial payments can be inputted into the ERP system, no action will be taken unless the invoice is fully paid. Lastly, the developed report prepares and uploads a third entry marked as "paid" to the WKÖ blockchain environment.

The final component of the implementation concerns the fourth layer, which shows a web-based user interface for financial audits. First, an updated list of open items is retrieved from the SAP system using the transaction "Vendor Line Item Display" (Code: FBL1N). These issued invoice documents and associated metadata are separately hashed and automatically reconciled with existing entries recorded in the mentioned blockchain infrastructure, which can result in six different outcomes categorized into two relevant groups. A successful status response from the WKÖ blockchain environment confirms a cryptographic match between the current invoice and the original entry accepted by the debtor in the distributed ledger. This proves that the document and metadata remain unchanged since the initial upload and were accepted by the debtor, establishing data validity without the need of a trusted party. The second relevant group comprises all outcomes in which the cryptographic hash cannot be found in the blockchain infrastructure or debtor confirmation has not been recorded. These discrepancies signify a potential breach of data integrity of the affected open items, indicating that the invoice data was modified prior to the audit date. Invoices lacking explicit debtor acceptance are visually flagged to indicate potential fraud risk, which requires detailed examination by auditors. This targeted and automated approach yields substantial time savings and significantly enhances the overall efficiency of corporate audits.

since it's a consortium BC that's a bit strong

To further validate the functional improvement and practical benefits of the developed artifact, the proposed extension is qualitatively compared with the traditional audit process, highlighting increased reliability, performance, and reduction of compliance effort in **Table 2**.

so, what if SAP is tampered with (eg metadata changes?) there's no way for the reconciliation

**Table 2.** Summary of the Qualitative Evaluation of the Audit Process Characteristics

| Criteria | Traditional Process | Blockchain Integrated Process |
|---|---|---|
| Data Integrity | Manipulation possible before sending to debtor | Cryptographic data encryption, high robustness (51% attacks) → in a PoA? |
| Completeness | Only when requested (manual effort) | Continuous, full lists of open items |
| Communication Mode | Manual, low security, invoice acceptance not recorded | Automatic integrity (includes invoice acceptance), only hashes are sent to BaaS |
| Speed | Days/weeks [6] | Seconds |
| Storage | Each stakeholder has one invoice copy | Each stakeholder has one invoice copy and two or three blockchain entries per invoice |
| End-user complexity | No additional steps | No additional steps (except secret...) |
| Auditor complexity | Manual collection and data reconciliation | Automatic collection and data reconciliation, blockchain provides an immutable log |

## 7 Discussion and Limitation

The results derived from the experimental implementation of the architecture provide empirical evidence that the SAP on-premise system and blockchain technology as part of the emerging technologies can be connected via a middleware without hard barriers. Work by Rozario and Vasarhelyi [3] also demonstrate the applicability of smart contracts in auditing by proposing an active approach in which the smart contract directly performs the financial audit. The mentioned architecture is affected by a major limitation to fulfill data security and privacy requirements when comparing to zero-knowledge proofs. Comparably, the validation of open items in this paper is achieved without exposing sensitive financial data to third parties or a blockchain infrastructure, because only the cryptographic data fingerprint as proof is utilized for verification. This consideration can have a significant influence on the willingness of companies to employ a blockchain integration, due to prior data privacy concerns [34], [35], [36], especially with unauthorized parties within a shared blockchain network.

Furthermore, recent literature [8], [20], [23] emphasizes that conceptual future integrations and theoretical benefits of using a DLT within supply chains can increase the overall transparency and visibility and provide a more efficient audit process, tackling critical industry challenges. This paper appends the current knowledge level by combining ERP systems, which can be viewed as unconnected data silos, with existing and secure blockchain environments, further reducing the complexity of maintaining blockchain nodes. Significant improvements are also attributed to solving current audit bottlenecks of manual reconciliation and invoice acceptance by debtors [6]. Eventually, the proposed model is not only bound to ERP systems by SAP, but can be applied to any ERP system, which provide sufficient interfaces to connect to an external environment. Among most used technologies to access these interfaces are REST, Hypertext

proofs



Transfer Protocol, Simple Object Access Protocol, Extensible Markup Language, and JavaScript Object Notation. What an odd way of saying this...

The PoC prototype additionally proves the technical possibility of implementing near real-time and continuous auditing and full population testing by automating the generation and latter reconciliation of hashes. Thus, audit risks attributable to human errors and sampling biases can be mitigated. At the same time, the system gives auditors autonomous access to verified financial data, which eliminated the need for manual feedback from audit examinees or in further instances their business partners. In addition, this approach enhances the overall assurance level and promotes greater standardization in practice. Nevertheless, the auditor's role shifts in this regard; correctly labeled open items can be automatically checked by the system. Consequently, the audit methodology shifts from individual record verification to a systemic approach, focusing more on the integrity of the underlying program logic and interfaces, which can be applied to several systems and thus providing a higher level of scalability. Prospectively, this enables audits of entire populations with minimal manual interventions at a fraction of the traditionally required effort. This aspect in particular was requested by international auditors during this research, and the proposed methodology and solution was therefore subsequently validated. At the same time this approach serves as a functional archetype for the next generation of digital auditing.

unsubstanc

yes, but it's not the same job at all.

too few details

Closely related to the implications for auditing are concerns about privacy and GDPR compliance. The lightweight design of the architecture follows a data minimization principle by only transmitting and thus providing the cryptographic fingerprint, which simulates a unique document identifier. Nevertheless, the possibility of a hash collision can be neglected due to statistical improbability [37]. The primary billing records persisted locally on the ERP system's internal database, which are often encapsulated and protected by a firewall to ensure sensitive data is safe from external parties. In contrast to blockchain integrations that store sensitive data directly on-chain [21], [25], which are obliged to delete data under Article 17 of the GDPR [38]. However, the proposed architecture circumvents such regulations, because the original document cannot be reconstructed from the DLT (more information in Section 5). Consequently, the underlying data remains entirely inaccessible also to other blockchain participants. This implies that once the data is deleted from the ERP system, the remaining on-chain hash becomes a unique identifier without an existing referent, fulfilling the intent of data erasure in theory. In contrast, deleting entries is often bound to high workloads due to a blockchain's characteristic. Nevertheless, in financial business contexts true anonymization of sensitive information is hardly possible due to legal retention, audit requirements, and existing copies of invoices [39]. Crucially, storing cryptographic fingerprints directly on-chain should not compromise GDPR compliance, as hashes do not contain or reveal any identifiable information.

this is already well known

odd!

Similar to research by Rozario & Vasarhelyi [3], this work focuses on improvement of reference processes while using ERP systems as the "single source of truth" for many financial reports and regular audits. While the blockchain provides a transparent audit trail for alterations after the initial blockchain entry, it does not solve the "Oracle Problem" and thus cannot determine whether the invoice content is correct. Nevertheless, the system's design minimizes the scope of this problem by setting an integrity anchor

harmonize



at the decisive point of invoice issuance to the debtor. In more detail, changes which occurred after the document was transmitted to the customer are immediately detectable using a mathematical proof verifying the document's existence and proof of its immutability since the initial anchoring in the blockchain. Furthermore, a cost and scalability bottleneck occurs in blockchain environments when issuing high amounts of invoices in a short period of time, comparable to work by [40], [41], [42]. Further limitations consider the technical reliance on custom code development, necessitated by missing integration interfaces within legacy ERP systems used in practice. Finally, while this paper focuses primarily on the technical instantiation and PoC of the technical artifact, a comprehensive legal analysis remains outside its scope and should be examined in future implementations.

that's not a proper threat to validity section

## 8 Conclusion & Future Work

The research investigates the current Sales and Collection Cycle within financial audits, specifically focusing on the reconciliation of unresolved invoices (open items). The current process represents a significant operational bottleneck, as the manual verification by the examinee's business partners consumes a big portion of an audit's resources [6]. Furthermore, qualitative insights from expert workshops identified a critical procedural gap and an inability to systematically verify invoice approvals by debtors during corporate audits. As a response, the proposed solution includes a "Lightweight Integrity Data Anchor" by interposing a BaaS environment as an automated trusted party between all stakeholders of the billing process. On the technical side, only the cryptographic fingerprint (hash) of financial data, which includes the invoice metadata and the invoice document, will be used to prove data integrity and immutability to auditors. This design follows a zero-knowledge proof in which blockchain participants can verify the hash of financial data but cannot reconstruct the underlying invoices including sensitive or critical information. The paper demonstrates the technical feasibility (PoC) of this architecture by implementing the workflow with a legacy SAP on-premise system combined with an existing BaaS environment provided by the WKÖ. The developed prototype provides first technical insights for practical implementation, benefitting especially auditors, optimizing resources for reconciliation of open items from hours to days to mere seconds. By utilizing existing interfaces this solution can be a viable and cost-efficient option for enterprises, optimizing the input-output ratio while enabling a possibility for automated, continuous and near real-time auditing.

keep the conclusion brief &

improper?

Based on successful design and implementation of the technical artifact presented in prior sections, the predefined RQs of this paper can be comprehensively addressed:

*RQ1: To what extent can the current manual process for invoice verification and auditing of Open Items be automated using blockchain and smart contracts?*

ERP systems often provide lists of open items, which can be extracted via dedicated API-interfaces. The automated comparison of open items with the BaaS environment streamlines the reconciliation process by immediately identifying content-related discrepancies. This mechanism transforms the audit from a manual, sample-based task into a semi-automated verifier. Due to greatly increased efficiency, the sample size can

no details/discussion of what SaaS entails or smart contract design...

redundancy

be extended to all available unresolved invoices, allowing a full audit on an enterprise level. Simultaneously, the architectural design should ensure compliance with Article 17 of the GDPR by utilizing the one-way cryptographic hashes that contain no identifiable information. Once the source data is deleted from the ERP system, the on-chain anchor loses its utility. However, critical limitations remain, as the solution does not guarantee contextual accuracy of the data. Ultimately, the "Oracle Problem" and risks associated with manual data entries still pertain, as the blockchain environment cannot prove contextual correctness.

*RQ2: How should a system architecture be designed to ensure data integrity in ERP systems using Distributed Ledger Technologies (DLT) without passing on sensitive data to third parties?*

Related to the previous RQ, this paper proposes a model, which builds upon a literature review and expert workshops. It proposes a minimally obtrusive blockchain integration consisting of four layers; Corporate Environment, Integration, Trust, and Verification & Visualization. Billing data is generated in compliance with the business partner's orders, which are cryptographically encrypted and sent to subsequent layer. The final layer (Verification & Visualization) offers a complete list of all open items, including the information which are verified by the debtors. This can be validated utilizing the Trust layer, which represents a BaaS environment. The system always remains secure by sending only the hash of the financial data. As even blockchain participants, who can track created blockchain entries and inspect the hash-values, cannot reconstruct the actual data. Further utilizing a PoC implementation the architecture's technical feasibility could be proven, creating an automated zero-knowledge validation environment.

This paper contributes to the growing body of theoretical, technical, and managerial knowledge on integrating DLT and ERP systems, often embodying "data silos". The DSR framework was utilized to provide a structured, comprehensive, and replicable artifact, which can be adapted to a generalized model for a wider application area. The proposed design serves as a functional prototype for corporate finance, by specifically addressing today's auditors pain and needs, while streamlining reconciliation procedures, and lastly additionally increasing audit quality through increased transparency and reduction of costs.

Future research should investigate the legal admissibility and potential confirmability of DLT-anchored data compared to standards, such as electronic signatures or traditional manual documentation. The proposed architecture lays the foundation for automated audit procedures, where the system provides reports on open items requiring further inspection. Future work will focus on a detailed performance analysis, specifically developing quantitative and qualitative metrics to measure the effectiveness and overhead of this integration. By adhering to a lightweight design, the approach confirms that ERP systems with DLT can significantly increase audit transparency without sacrificing on overall process performance and potentially aligning with Article 17 of the GDPR.

**Disclosure of Interests.** The authors have no competing interests to declare that are relevant to the content of this article.

## References


[1] I. E. Inghirami, "Accounting Information Systems: The Scope of Blockchain Accounting," *Digit. Bus. Transform. Lect. Notes Inf. Syst. Organ.*, vol. 38, pp. 107–120, 2020, doi: 10.1007/978-3-030-47355-6_8.

[2] P. Petratos and A. Faccia, "Securing Energy Networks: Blockchain and Accounting Systems," *Int. Conf. Electr. Comput. Energy Technol. ICECET 2021*, no. December, pp. 1–5, 2021, doi: 10.1109/ICECET52533.2021.9698728.

[3] A. M. Rozario and M. A. Vasarhelyi, "Auditing with Smart Contracts," *Int. J. Digit. Account. Res.*, vol. 18, no. February, pp. 1–27, 2018, doi: 10.4192/1577-8517-v18.

[4] E. M. Shehab, M. W. Sharp, L. Supramaniam, and T. A. Spedding, "Enterprise resource planning: An integrative review," *Bus. Process Manag. J.*, vol. 10, no. 4, pp. 359–386, 2004, doi: 10.1108/14637150410548056.

[5] X. Chu, T. Jiang, X. Li, and X. Ding, "Bye Audit! A Novel Blockchain-Based Automated Data Processing Scheme for Bank Audit Confirmation," *Commun. Comput. Inf. Sci.*, vol. 1176 CCIS, pp. 68–82, 2020, doi: 10.1007/978-981-15-3278-8_5.

[6] H. Peng, H. Hu, J. Chen, G. Li, X. Xie, and K. Xu, "Innovation in a Real-Time Settlement Model for Aviation Fuel Supply Chain Based on Blockchain Smart Contracts: Construction of a Collaborative Ecosystem Integrating Business, Finance, and Financial Services at China Southern Airlines," *ICNC-FSKD 2025 - 21st Int. Conf. Nat. Comput. Fuzzy Syst. Knowl. Discov.*, pp. 153–159, 2025, doi: 10.1109/ICNC-FSKD67701.2025.11198072.

[7] International Federation of Accountants, "International Standards on Auditing (ISA)." Accessed: Feb. 02, 2026. [Online]. Available: https://www.fsb.org/2024/01/international-standards-on-auditing-isa/

[8] P. Kalaiselvi, C. C. Deboral, R. Somasundaraman, G. S. Anirudh Srinivasan, and A. Surya, "Organizational Finance Tracking System Using Blockchain," *Commun. Comput. Inf. Sci.*, vol. 2608 CCIS, pp. 239–247, 2026, doi: 10.1007/978-3-032-02537-1_22.

[9] N. E. Vincent, A. Skjellum, and S. Medury, "Blockchain architecture: A design that helps CPA firms leverage the technology," *Int. J. Account. Inf. Syst.*, vol. 38, p. 100466, 2020, doi: 10.1016/j.accinf.2020.100466.

[10] J. Krissansen, "Accounts receivable fraud: Types & how to detect them." Accessed: Feb. 03, 2026. [Online]. Available: https://www.bill.com/learning/accounts-receivable-fraud

[11] International Federation of Accountants, *2025 Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements*. 2025.

[12] Subhasis Sahoo, "What is Open Item in Accounting?" Accessed: Feb. 03, 2026. [Online]. Available: https://finfloh.com/blog/open-item

[13] A. Redlein, E. Stopajnik, K. Schaad, S. Hofer, C. Höhenberger, and P. Turnbull, *Modern Facility and Workplace Management*. Springer Nature, 2020. doi: 10.1007/978-3-030-35314-8.

[14] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *J. Manag. Inf. Syst.*, vol. 24,

no. 3, pp. 45–77, 2007, doi: 10.2753/MIS0742-1222240302.

[15] SAP, "Correspondence: Open Item List." Accessed: Feb. 03, 2026. [Online]. Available: https://help.sap.com/docs/SAP_S4HANA_CLOUD/918bca53037f408f91a2295d04ac16bc/fd79eba1ea8b4bbfbbdaf0d2b6e3ee67.html

[16] T. Miller, "How to conduct a thorough ERP audit." Accessed: Feb. 03, 2026. [Online]. Available: https://www.erpfocus.com/how-to-conduct-a-thorough-erp-audit-4146.html

[17] International Federation of Accountants, "ISA 240 (Revised), The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements." Accessed: Feb. 03, 2026. [Online]. Available: https://www.iaasb.org/publications/isa-240-revised-auditor-s-responsibilities-relating-fraud-audit-financial-statements

[18] B. Naghshineh, V. Feijao, B. Sieben, and H. Carvalho, "E-invoicing process reengineering: a case study," *Bus. Process Manag. J.*, 2025, doi: 10.1108/bpmj-06-2025-1025.

[19] D. Fernandez and N. H. Nik Man, "Exploring Organizational Contexts in Blockchain Adoption: A Malaysian Public Sector Case Study," *2024 10th Int. Conf. Comput. Eng. Des. ICCED 2024*, pp. 1–6, 2024, doi: 10.1109/ICCED64257.2024.10983847.

[20] A. T. Agustini and J. H. Mustakini, "A systematic literature review of blockchain technology and accounting issues: Is it a hype or hope?," *South African J. Account. Res.*, vol. 39, no. 1, pp. 73–107, 2024, doi: 10.1080/10291954.2024.2371616.

[21] K. Narayanam, S. Goel, A. Singh, Y. Shrinivasan, and P. Selvam, "Blockchain based accounts payable platform for goods trade," *IEEE Int. Conf. Blockchain Cryptocurrency, ICBC 2021*, pp. 1–5, 2021, doi: 10.1109/ICBC51069.2021.9461053.

[22] R. Tan, Y. Li, J. Zhang, and W. Si, "Application of Blockchain Technology to the Credit Management of Supply Chain," *Commun. Comput. Inf. Sci.*, vol. 1286, pp. 121–132, 2020, doi: 10.1007/978-981-15-9739-8_11.

[23] G. W. Wickramakalutota and C. R. Oruthotaarachchi, "Evaluating Blockchain Integration for Enhanced Security and Transparency in ERP Systems: A Systematic Review Across Manufacturing, Healthcare, and Finance Domains," *2025 5th Int. Conf. Adv. Res. Comput. Converging Horizons Uniting Discip. Comput. Res. through AI Innov. ICARC 2025 - Proc.*, pp. 1–6, 2025, doi: 10.1109/ICARC64760.2025.10962893.

[24] W. Al-Azzawi, J. M. Rajaa, A. Ali Saber Mohammed, M. Z. Nayef Al-Dabagh, and N. H. Hameed, "Transforming Enterprise Financial Management with Blockchain-Driven Computational Innovations," *2025 Int. Conf. Comput. Innov. Eng. Sustain.*, pp. 1–5, 2025, doi: 10.1109/iccies63851.2025.11032212.

[25] A. Ribeiro, L. Santos, A. Furtado, B. Schroder, D. Vidaletti, and M. Vanzin, "A Blockchain-Based Approach for Cross-Ledger Reconciliation," *Blockchain Appl.*, pp. 52–60, 2020, doi: 10.1007/978-3-030-52535-4_6.

[26] W. Zhang *et al.*, "Blockchain-Based Distributed Compliance in Multinational Corporations' Cross-Border Intercompany Transactions," *Adv. Inf. Commun. Networks*, no. April, pp. 304–320, 2019, doi: 10.1007/978-3-030-03405-4_20.

[27] J. Simm, J. Steiner, and A. Truu, "Verifiable Multi-Party Business Process Automation," *Int. Conf. Bus. Process Manag.*, pp. 30–41, 2020, doi: 10.1007/978-3-030-66498-5_3.

[28] H. Li *et al.*, "FISCO-BCOS: An Enterprise-Grade Permissioned Blockchain System with High-Performance," *Int. Conf. High Perform. Comput. Networking, Storage Anal.*

*SC*, no. January, 2023, doi: 10.1145/3581784.3607053.

[29] B. P. Hansen and T. Davis, "A primer on Web3 adoption for enterprise." Accessed: Feb. 03, 2026. [Online]. Available: https://www.deloitte.com/us/en/services/consulting/articles/blockchain-and-web3-adoption-for-enterprises.html

[30] A. Macaulay, "SAP und Blockchain." Accessed: Feb. 03, 2026. [Online]. Available: https://ignitesap.com/de/SAP-und-Blockchain/

[31] M. I. Sarwar *et al.*, "Data Vaults for Blockchain-Empowered Accounting Information Systems," *IEEE Access*, vol. 9, pp. 117306–117324, 2021, doi: 10.1109/ACCESS.2021.3107484.

[32] F. Dietrich, A. Turgut, D. Palm, and L. Louw, "Token-Based Blockchain Solutions for Supply Chain Strategies," *Congr. Ger. Acad. Assoc. Prod. Technol.*, vol. 2, pp. 689–698, 2020, doi: 10.1007/978-3-662-62138-7_69.

[33] V. Malamas, T. K. Dasaklis, T. G. Voutsinas, and P. Kotzanikolaou, "Blockchain Service Layer for ERP data interoperability among multiple supply chain stakeholders," *9th 2023 Int. Conf. Control. Decis. Inf. Technol. CoDIT 2023*, pp. 145–150, 2023, doi: 10.1109/CoDIT58514.2023.10284288.

[34] T. Hristova, G. Mihaylov, P. Hristov, and A. Taneva, "Analysis of Data Sharing Systems in the Context of Industry 4.0 via Blockchain in 5G Mobile Networks," *Eng. Proc.*, vol. 70, no. 1, 2024, doi: 10.3390/engproc2024070002.

[35] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proc. 13th EuroSys Conf. EuroSys 2018*, vol. 2018-Janua, no. February, 2018, doi: 10.1145/3190508.3190538.

[36] K. Seidenfad, T. Hoiss, and U. Lechner, "A Blockchain to Bridge Business Information Systems and Industrial Automation," *Innov. Community Serv.*, pp. 22–40, 2021, doi: 10.1007/978-3-030-75004-6_3.

[37] National Institute of Standards and Technology, "Secure Hash Standard," *FIBS 180-4 Publ.*, vol. 4, no. August, p. 36, 2015, doi: 10.6028/NIST.FIPS.180-4.

[38] European Parliament, "Art. 17 GDPR." Accessed: Feb. 25, 2026. [Online]. Available: https://gdpr-info.eu/art-17-gdpr/

[39] E. Politou, A. Michota, E. Alepis, M. Pocs, and C. Patsakis, "Backups and the right to be forgotten in the GDPR: An uneasy relationship," *Comput. Law Secur. Rev.*, vol. 34, no. 6, pp. 1247–1257, 2018, doi: 10.1016/j.clsr.2018.08.006.

[40] R. Perera, K. R. Nawurunnage, S. Chathuranga, R. Wickramarachchi, and A. Withanaarachchi, "Role of Blockchain Technology in ERP Systems for a Transparent Supply Chain: A Systematic Review of Literature," *ICARC 2023 - 3rd Int. Conf. Adv. Res. Comput. Digit. Transform. Sustain. Dev.*, pp. 232–237, 2023, doi: 10.1109/ICARC57651.2023.10145618.

[41] N. Pytel, C. Ziegler, and A. Winkelmann, "From Dissonance to Dialogue: A Token-Based Approach to Bridge the Gap between Manufacturers and Customers," *ACM Trans. Manag. Inf. Syst.*, vol. 15, no. 1, 2024, doi: 10.1145/3639058.

[42] M. G. Stoica, "Smart Contracts: A Valuable Technology in ERP e-Commerce Systems and for Customer Experience," *Int. Conf. Comput. Commun. Control*, pp. 20–33, 2023, doi: 10.1007/978-3-031-16684-6_2.