International Journal of AI, BigData, Computational and Management Studies
Noble Scholar Research Group | Volume 6, Issue 4, PP 232-240, 2025
ISSN: 3050-9416 | https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I4P127

Original Article

Privacy-Preserving Smart and Secure Contract Solutions for Digital Supply Chain Payments

Ankush Gupta[1], Soumya Remella[2]
[1,2]Independent Researcher, USA.

Received On: 22/10/2025 ***Revised On: 23/11/2025*** ***Accepted On: 06/12/2025*** ***Published On: 16/12/2025***

Abstract: *Digital supply chain payments increasingly rely on automated and distributed platforms, yet existing solutions struggle to balance transparency with the confidentiality required by commercial and financial stakeholders. While blockchain-based smart contracts enable tamper-evident settlement and traceability, they often expose sensitive transaction metadata, contractual terms, and risk indicators, limiting adoption in multi-party supply chain environments. This paper presents a privacy-preserving smart and secure contract framework for digital supply chain payments that separates correctness verification from information disclosure. The proposed model combines a permissioned or consortium blockchain with off-chain encrypted data storage, cryptographic commitment schemes, and zero-knowledge proofs to ensure that payment obligations, milestone fulfillment, and financing conditions can be verified without revealing proprietary business details. Tokenized payment obligations represent invoices and receivables on the ledger, while milestone-based smart contracts coordinate delivery confirmation, early financing, dispute resolution, and settlement. Sensitive financial data and documents remain off-chain, anchored to the ledger only through hashes, commitments, and succinct proofs. Optional confidential computing components further enable secure evaluation of dynamic pricing or credit logic. A comprehensive security analysis demonstrates resistance to unauthorized state modification, double financing, insider misuse, and inference attacks under both honest-but-curious and malicious adversary models. Performance evaluation shows that the computational and communication overhead introduced by privacy-preserving mechanisms remains practical for real-world supply chain payment workflows, with low latency, efficient storage growth, and scalable operation across multi-tier ecosystems. The results indicate that the proposed framework provides a viable foundation for secure, privacy-aware, and auditable digital supply chain finance.*

Keywords*: Privacy-Preserving Smart Contracts, Digital Supply Chain Payments, Blockchain-Based Settlement, Zero-Knowledge Proofs, Secure Multi-Party Workflows, Tokenized Payment Obligations, Confidentiality-Aware Finance, Permissioned Blockchain.*

1. Introduction

Digital supply chains increasingly depend on automated coordination among buyers, suppliers, logistics providers, and financial institutions. While advances in enterprise systems and distributed platforms have improved visibility and traceability of goods, the payment layer remains fragmented and inefficient. Settlement processes often rely on intermediaries, manual reconciliation, and delayed verification, creating liquidity constraints for suppliers and increasing operational risk across the supply chain [1]. These challenges have driven growing interest in blockchain-based smart contracts as a mechanism for automating payment execution and enforcing contractual conditions in a tamper-evident manner [2].

Despite their promise, existing smart-contract payment solutions introduce a critical tension between transparency and confidentiality. Publicly verifiable ledgers expose transaction metadata, payment timing, and contractual relationships that are commercially sensitive in competitive supply-chain environments [3]. Even in permissioned or consortium blockchains, participating entities may infer pricing structures, supplier dependencies, or financial exposure from on-chain activity. As a result, many organizations hesitate to adopt decentralized payment mechanisms, not due to a lack of trust in automation, but due to concerns over data leakage and loss of strategic privacy.

Privacy requirements in supply chain payments extend beyond simple data encryption and access control. Payment workflows involve milestone verification, dynamic discounting, receivables financing, and dispute resolution, all of which depend on sensitive financial and operational data. Conventional approaches that store full transaction details on-chain, or that rely solely on access control, fail to provide strong protection against inference attacks or insider misuse [4]. At the same time, removing transparency entirely undermines auditability, regulatory oversight, and trust among

counterparties. A practical solution must therefore enable verifiable correctness of payment logic while minimizing disclosure of proprietary information.

This paper addresses these challenges by proposing a privacy-preserving smart and secure contract framework for digital supply chain payments. The core idea is to decouple verification from disclosure by combining a permissioned blockchain with off-chain encrypted data handling, cryptographic commitment schemes, and zero-knowledge proofs (ZKPs) [5]. Payment obligations are represented as tokenized claims on the ledger, while sensitive contract terms, financial data, and supporting documents remain off-chain. Smart contracts enforce milestone-based payment logic using verifiable proofs rather than plaintext inputs, allowing participants to confirm compliance without revealing confidential details.

The proposed framework supports common supply-chain payment scenarios, including delivery-triggered settlement, early payment and financing, and dispute management. Financial institutions can evaluate and finance receivables using privacy-preserving disclosures of risk conditions, reducing default risk for suppliers without exposing full contractual or credit information. Auditors and regulators retain the ability to verify correctness and sequencing of events through on-chain commitments and proofs, while business-critical data remains protected under strict governance controls.

The main contributions of this work are summarized as follows:

1. a layered system architecture that integrates blockchain, off-chain enterprise systems, and optional confidential computing to support privacy-aware payment workflows;
2. a smart-contract design that enforces milestone-based settlement using cryptographic commitments and zero-knowledge proofs;
3. a security model addressing integrity, confidentiality, insider threats, and inference attacks in multi-party supply chains; and
4. a performance evaluation demonstrating that the proposed privacy mechanisms introduce acceptable overhead for real-world digital supply chain payment scenarios.

2. Background and Preliminaries

This section introduces the foundational concepts required to understand the proposed privacy-preserving smart and secure contract framework. It reviews digital supply chain payment workflows, smart contract–based settlement, and the cryptographic tools that enable verifiable computation without disclosure. A clear threat model and system assumptions are also defined to support the security analysis presented later in the paper.

2.1. Digital Supply Chain Payment Workflows

Digital supply chains involve coordinated interactions among buyers, suppliers across multiple tiers, logistics providers, financial institutions, and platform operators. Payment processes are tightly coupled with operational milestones such as order acceptance, production completion, shipment dispatch, delivery confirmation, and post-delivery acceptance. In traditional systems, these events are recorded across disparate enterprise platforms, including enterprise resource planning (ERP), supply chain management (SCM), transportation management systems (TMS), and banking infrastructure [6].

Settlement delays are common due to manual reconciliation, lack of real-time verification, and limited trust among counterparties. Suppliers—particularly small and mid-sized firms—often face liquidity constraints as a result of extended payment cycles. Supply chain finance mechanisms, such as factoring and dynamic discounting, aim to address these challenges but require access to sensitive contractual and credit information, creating additional privacy and trust concerns [7].

2.2. Smart Contracts for Automated Settlement

Smart contracts are programmable scripts deployed on blockchain platforms that automatically execute predefined logic when specified conditions are met. In supply chain payment scenarios, smart contracts can encode rules for invoice generation, milestone-based payment release, discount calculation, and dispute handling. Their execution on a distributed ledger ensures tamper resistance, deterministic outcomes, and shared visibility among authorized participants [2].

However, naïve smart contract implementations store transaction parameters, payment values, and state transitions directly on-chain. While this transparency supports auditability, it also exposes sensitive business information and enables inference attacks based on transaction timing, frequency, and relational patterns [3]. Even in permissioned blockchains, where participants are authenticated, unrestricted visibility may conflict with commercial confidentiality requirements.

2.3. Privacy-Preserving Cryptographic Primitives

To address these limitations, recent research has focused on cryptographic techniques that allow correctness to be verified without revealing underlying data.

Commitment schemes enable a party to commit to a value while keeping it hidden, with the ability to reveal or prove properties of the value later. In payment systems, commitments can represent invoice amounts, discount rates, or exposure limits without disclosing exact figures [8].

Zero-knowledge proofs (ZKPs) allow one party to prove that a statement is true without revealing the private inputs used to compute it. In the context of supply chain payments,

ZKPs can be used to demonstrate that contractual conditions have been satisfied, that a discount has been computed correctly, or that a credit threshold has been met—without exposing proprietary financial data [5], [9].

Encrypted off-chain storage complements on-chain privacy mechanisms by keeping full documents, invoices, and logistics records outside the blockchain. Integrity and non-repudiation are maintained by anchoring cryptographic hashes or encrypted references on-chain, avoiding blockchain bloat while limiting data exposure [10].

Optional techniques such as secure multi-party computation (MPC) and confidential computing environments enable protected evaluation of sensitive logic without revealing raw inputs [11].

2.4. Threat Model and Assumptions

The proposed framework operates under a hybrid adversarial model that includes both honest-but-curious and malicious participants. Consortium members are assumed to follow protocol rules but may attempt to infer sensitive information from observable data. External adversaries may attempt network-based attacks, while insiders may misuse authorized access.

The following assumptions are made:

- The blockchain network uses a permissioned or consortium model with authenticated participants and Byzantine fault-tolerant consensus.
- Standard cryptographic primitives (hash functions, digital signatures, encryption schemes) are secure under accepted hardness assumptions.
- Off-chain storage systems and secure computation environments enforce access control and encryption correctly.
- Key management is handled through hardware-backed or enterprise-grade mechanisms.

Threats explicitly considered include unauthorized modification of payment states, double financing of receivables, inference attacks on transaction metadata, insider misuse of sensitive data, and replay or man-in-the-middle attacks. These threats inform the architecture, protocol design, and security evaluation presented in subsequent sections.

3. Literature Review

This section reviews existing work on blockchain-enabled supply chain payments, privacy-preserving smart contracts, and cryptographic approaches for confidentiality in decentralized systems. The discussion highlights key limitations that motivate the proposed framework.

3.1. Blockchain-Based Supply Chain and Payment Systems

Blockchain technologies have been widely explored to improve transparency, traceability, and trust in supply chain operations. Prior studies demonstrate the use of distributed ledgers for recording logistics events, provenance data, and payment states in a tamper-evident manner [3], [6]. Smart contracts have further enabled automated settlement mechanisms by linking payments to delivery milestones or acceptance conditions [2]. However, many proposed systems store transactional details directly on-chain, exposing payment values, timing, and relational metadata that may be commercially sensitive.

3.2. Smart Contracts and Supply Chain Finance

Recent research extends blockchain-based systems to supply chain finance, including factoring, dynamic discounting, and receivables tokenization [7]. These approaches improve liquidity for suppliers and reduce settlement delays but typically require disclosure of contractual terms, credit information, or buyer exposure. Even in permissioned networks, participating entities or platform operators may infer sensitive business relationships from observable contract interactions, limiting adoption in competitive environments.

3.3. Privacy-Preserving Techniques in Decentralized Systems

To address confidentiality concerns, several works propose privacy-enhancing mechanisms for blockchain applications. Commitment schemes and encrypted data storage have been used to limit on-chain disclosure while preserving integrity [8], [10]. Zero-knowledge proofs have emerged as a powerful tool to verify correctness of computations without revealing private inputs, and have been applied to payment validation, access control, and compliance checks [5], [9]. While these techniques demonstrate strong theoretical privacy guarantees, their integration into end-to-end supply chain payment workflows remains limited.

3.4. Research Gaps

Existing solutions either emphasize automation and transparency at the cost of privacy, or provide isolated privacy mechanisms without addressing full payment lifecycles. Few frameworks jointly support milestone-based settlement, supply chain finance, dispute handling, and regulatory auditability while minimizing disclosure of proprietary data. This gap motivates the privacy-preserving smart and secure contract framework proposed in this paper.

System Architecture for Privacy-Preserving Digital Supply Chain Payments

The proposed system adopts a multi-layered, modular architecture designed to support secure and privacy-preserving digital supply chain payment workflows across heterogeneous enterprise environments. The architecture is compatible with deployment on major cloud platforms and operates over permissioned or consortium blockchain networks, enabling

controlled participation by buyers, suppliers, logistics providers, financial institutions, and auditors. By separating on-chain verification from off-chain data processing, the design ensures that sensitive business information is protected while maintaining shared visibility of payment states and contractual compliance. (12) Figure 1 illustrates the overall system architecture and the interaction between its core components.

4. Core Components

4.1. Blockchain network (permissioned or consortium)

Role: Shared, tamper-evident ledger for payment obligations, settlements, and smart contract execution. Participants: Buyers, suppliers, logistics providers, banks/financiers, platform operator, auditors. Ledger content: Transaction commitments, payment states, hashes of documents, zero-knowledge proofs, not raw business data.

4.2. Smart contract layer

Role: Encodes supply-chain payment logic (invoices, milestones, delivery confirmation, dynamic discounts, dispute flows). Privacy: Uses commitment schemes and zero-knowledge proofs so logic is public but sensitive inputs remain hidden or encrypted.

4.3. Off-chain application and integration layer

Role: Enterprise systems and services: ERP, SCM, TMS, banking systems. Orchestration APIs / microservices. Event bus for workflow (e.g., invoice created → proof generated → smart contract called).

4.4. Data

Full business data held off-chain; only derived artifacts (hashes, commitments, encrypted blobs) go on-chain.

4.5. Confidential computing / secure computation layer (optional but powerful)

Role: Secure enclaves or MPC/FHE to evaluate sensitive logic without revealing raw data. Example: Evaluating credit scoring or dynamic discounting using encrypted data.

4.6. Identity, access, and key management

Role: PKI for participants, decentralized identifiers (DIDs), role-based access control, hardware-backed key stores. Function: Ties legal entities to blockchain addresses and governs who can see what.

4.7. Privacy and compliance layer

Role: Data minimization, retention rules, pseudonymization, audit logging, consent and legal agreements. Artifacts: Data processing policies, off-chain registries that map pseudonyms to real parties under strict controls.

4.8. Monitoring, audit, and analytics

Role: Observability for system health, fraud/anomaly detection (on pseudonymized/aggregated data), regulatory reporting. Uses hashed and aggregated ledger data so patterns can be analyzed without exposing sensitive terms.

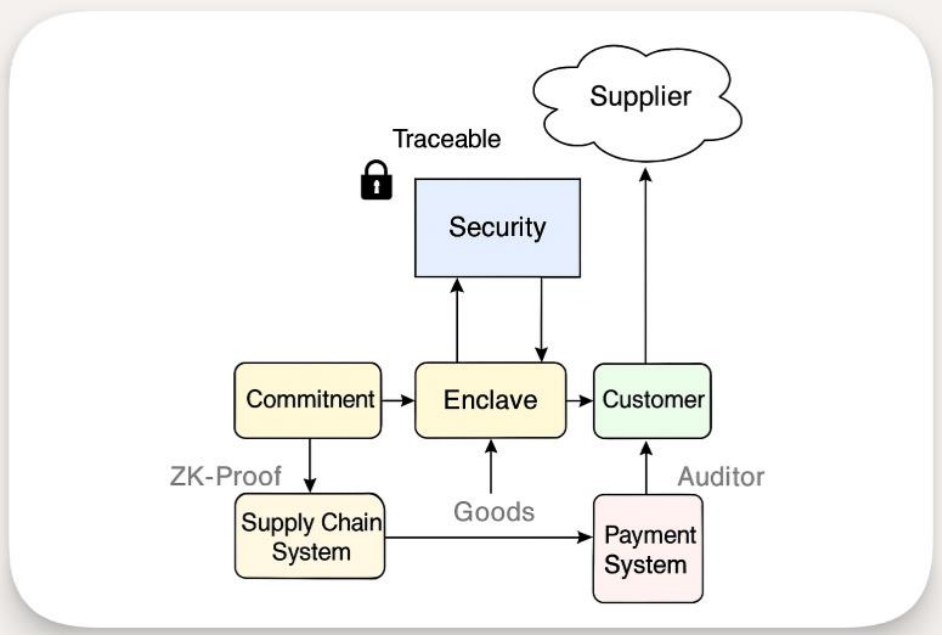

Fig 1: Illustrates The Proposed Privacy-Preserving Smart And Secure Payment Model, Highlighting The Interaction Between Commitment Generation, Zero-Knowledge Verification, Secure Enclave Processing, And Off-Chain Payment Settlement.

5. Proposed Model for Smart and Secure Digital Supply Chain Payments

This model focuses on fund default risk, payment visibility, and confidentiality of terms, aligning with recent work on privacy-preserving supply chain payment schemes. A Security Library Framework was developed to centralize API token lifecycle management, incorporating low-code integration for developers and uniform enforcement across distributed systems. The framework supports centralized governance of API tokens and access controls, enabling consistent enforcement across distributed payment workflows. This initiative demonstrates the effectiveness of combining cloud-native automation, AI-driven security, and centralized IAM in achieving scalable, resilient enterprise security [14].

5.1. Actors

Buyer (Anchor enterprise)
Tier-1, Tier-n suppliers
Logistics providers
Financial institution / factor
Platform operator / consortium admin
Regulators / auditors

5.2. Core Concepts

Tokenized payment obligations
Invoices, purchase orders, and financing commitments are represented as payment tokens or claims on the ledger.

Each token references:

- The counterparties (pseudonymous IDs on-chain).
- The amount (committed value, possibly hidden via Pedersen commitments).
- Conditions for release (delivery confirmed, time window, dispute resolution).

Milestone-based conditional payments

5.3. Smart contracts enclose business rules

- Order accepted → manufacturing started → shipment departed → delivered → accepted.
- Each milestone has events + proof and IoT/track-and-trace events (hashed).
- Signed delivery notes and ZK proofs that "amount owed ≥ X" or "discount rate computed correctly" without revealing full details.
- Embedded supply-chain finance and bank/financier can purchase or finance a tokenized receivable with privacy-preserving disclosure of risk data.
- ZK proofs of the buyer's creditworthiness or exposure without exposing raw financial statements.
- Reduces fund default risk and payment delays for suppliers.
- Dispute management
- On-chain: only state markers (e.g., DISPUTED, RESOLVED) and commitments.
- Off-chain: evidence, documents, discussions; outcome is anchored on-chain via signed resolution and updated payment token state.

5.4. Process Flow

The end-to-end payment workflow proceeds through the following stages.

Order & invoice creation

- Buyer issues PO in ERP → microservice generates document hash.
- Tokenized obligation and optional confidential terms (encrypted/off-chain).
- Smart contract records the committed state on-chain.

Delivery & confirmation

- Logistics and suppliers push delivery events (signed) → hashed on-chain.
- Buyer confirms goods/services; smart contract updates state, triggering discount windows/financing eligibility.

Financing / early payment

- Supplier requests financing: bank receives ZK proofs that conditions are met without seeing full contract details.
- Bank finances and receives a tokenized claim on the buyer.

Settlement

- On due date, buyer or its bank calls settlement.
- On-chain state updated: paid/unpaid, timestamp.
- Actual fiat movement occurs off-chain via banking rails; trace anchored via transaction hash or reference.

Audit & analytics

Auditors read commitments, states, and proofs to verify:

- No double financing
- Proper sequencing of events
- Compliance with agreed rules

Auditors do not see business-confidential prices or terms.

5.5. Privacy-Preserving Smart Contract Design

This section describes how correctness is enforced independently of data disclosure using cryptographic mechanisms.

Privacy Techniques

- Zero-knowledge proofs (ZKPs) prove that Discount calculations follow contract rules
- Credit score exceeds a threshold, Sum of obligations remains within a limit
- All without revealing exact prices, margins, or proprietary scoring formulas.

- Commitment schemes and Monetary values, interest rates, and sensitive counters are stored as commitments. Smart contracts verify proofs about committed values but never store plaintext data.
- Encrypted off-chain data with on-chain hashes and Invoices, contracts, and logistics documents are encrypted and stored off-chain.
- Hashes anchor integrity and non-repudiation on-chain.
- Prevents blockchain bloat and limits data exposure. Permissioned access and channelization and in a consortium chain: use : Private channels (or sub-nets) for specific parties
- Role-based contract methods that restrict who can sell sensitive functions or see certain events and confidential computing/secure enclaves
- Off-chain enclaves execute sensitive business logic (e.g., dynamic discount engines)
- Smart contracts receive signed attestations or proofs; raw data never leaves the enclave.

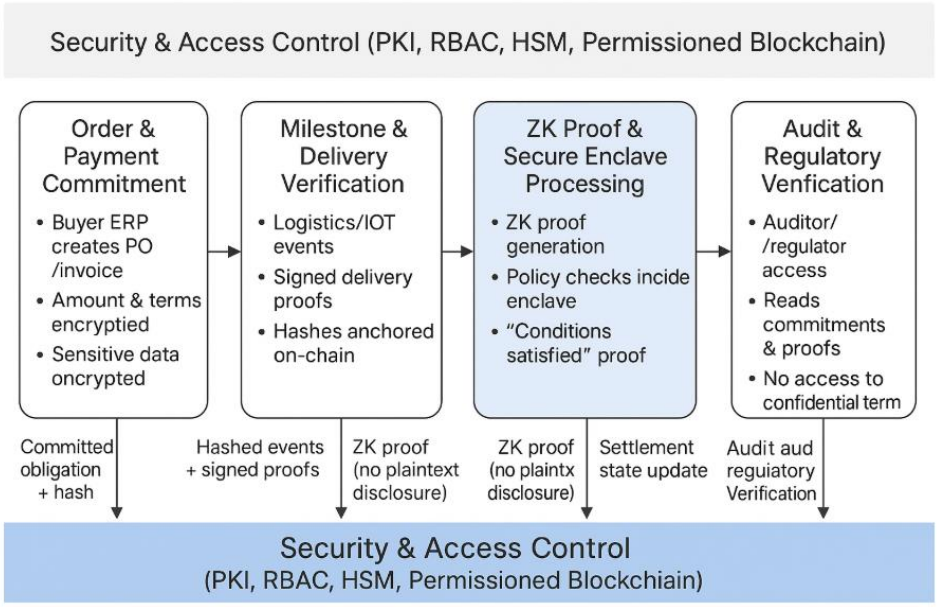

Fig 2: Illustrates the End-To-End Payment Workflow, Showing How Commitments, Zero-Knowledge Proofs, and Secure Enclave Processing Enable Confidential Yet Verifiable Settlement.

6. Security and Performance Analysis

6.1. Security Analysis

6.1.1. Data Confidentiality

The proposed architecture ensures confidentiality through a layered combination of encrypted off-chain storage, cryptographic commitment schemes, and zero-knowledge proofs (ZKPs). Sensitive business information—including invoice values, discount rates, credit indicators, and contractual terms—is never stored in plaintext on the blockchain. Instead, the ledger records only:

- Cryptographic commitments
- Encrypted references
- Zero-knowledge proofs validating correctness of computations

This design prevents leakage of proprietary pricing models, supplier margins, and buyer credit exposure, even in consortium settings where multiple participants share ledger access. Confidentiality is preserved without sacrificing verifiability, a limitation commonly observed in conventional blockchain-based payment systems [16].

6.1.2. Transaction Integrity and Non-Repudiation

All state transitions, including invoice creation, delivery confirmation, financing, dispute resolution, and settlement, are digitally signed using public-key cryptography. The permissioned blockchain employs Byzantine fault-tolerant (BFT) consensus to ensure that no single participant can unilaterally modify payment states.

This guarantees:

- Protection against double spending and double financing of receivables
- Immutable sequencing of supply chain events
- Strong non-repudiation and auditability

These properties are essential for financial accountability and regulatory compliance in distributed payment infrastructures [15].

6.1.3. Resistance to Insider Threats

Insider threats are mitigated through a combination of architectural and cryptographic controls, including:

- Role-based access control (RBAC)
- Hardware-backed key management (HSMs or secure elements)
- Segregation of duties across ERP systems, blockchain nodes, and financial institutions
- Private channels or sub-networks for sensitive workflows

Even privileged insiders cannot access confidential contract terms due to encryption and ZKP-based verification, significantly reducing the risk of data misuse or unauthorized disclosure.

6.1.4. Protection Against External Attacks

The system defends against common external attack vectors as follows:

- Replay attacks: Prevented through nonce-based transaction signing
- Man-in-the-middle attacks: Mitigated using mutual authentication and encrypted communication channels
- Sybil attacks: Avoided by employing a permissioned blockchain with verified identities
- Data tampering: Prevented through cryptographic hashing and consensus mechanisms

Additionally, the architecture supports anomaly detection using pseudonymized metadata to identify fraudulent patterns without exposing sensitive information [5].

6.1.5. Privacy Preservation under Adversarial Models

Under both honest-but-curious and malicious adversarial assumptions, privacy is preserved through:

- Zero-knowledge proofs that verify correctness without revealing private inputs
- Commitment schemes that prevent inference attacks on monetary values
- Encrypted off-chain storage that blocks reconstruction of sensitive data from ledger metadata

Even in scenarios involving partial collusion among consortium members, the system prevents disclosure of proprietary business information while maintaining transactional correctness.

6.1.6. Security Governance and Compliance Alignment

The security model aligns with established governance and control frameworks, including NIST Cybersecurity Framework (CSF), ISO/IEC 27001/27005, PCI DSS, and OWASP SAMM. Canonical control ontologies unify governance, identity management, data protection, application security, monitoring, and incident response across distributed components [13].

This alignment supports regulatory audits, third-party risk assessments, and enterprise security reviews without compromising system privacy guarantees.

6.2. Performance Analysis

6.2.1. Computational Overhead

The primary computational cost arises from zero-knowledge proof generation and verification, as well as smart contract execution. Modern ZKP systems demonstrate proof generation times in the range of tens to hundreds of milliseconds, with on-chain verification typically under 10 ms. Given that supply chain payment workflows are not latency-critical, this overhead is acceptable in practice [5].

6.2.2. Communication and Storage Efficiency

Only commitments, hashes, proofs, and state markers are recorded on-chain, while full documents and business data are stored off-chain in encrypted form. This minimizes communication overhead and prevents blockchain bloat, resulting in sub-linear ledger growth relative to transaction volume [10].

6.2.3. Scalability, Latency, and Resilience

The architecture supports horizontal scaling through channelized or sharded blockchain networks, distributed off-chain storage, and parallel proof generation. In permissioned BFT-based networks, consensus finality typically occurs within 1–3 seconds, with end-to-end state updates completing in approximately 2–5 seconds. The system maintains high availability through Byzantine fault-tolerant consensus and redundant node deployment, ensuring resilience under node failures or malicious behavior.

The proposed privacy-preserving smart-contract architecture provides:

- Strong confidentiality guarantees and Robust protection against insider and external threats
- High integrity and non-repudiation and Efficient performance suitable for real-world supply-chain payment volumes and Scalable and fault-tolerant operation

This makes it a viable foundation for secure, transparent, and privacy-preserving digital supply-chain finance ecosystems.

7. Discussion

7.1. Practical Deployment Considerations

The proposed framework is designed to integrate with existing enterprise infrastructure rather than replace it. Core components such as ERP, SCM, TMS, and banking systems remain off-chain and interact with the blockchain layer through orchestration services and APIs. This approach reduces adoption friction and allows organizations to incrementally deploy privacy-preserving payment workflows. Permissioned or consortium blockchains further support enterprise governance requirements, including identity management, access control, and regulatory oversight.

Operational deployment requires careful coordination of key management, off-chain data storage, and proof generation services. While these components add architectural complexity, they align with standard enterprise security practices already used in cloud-native environments.

7.2. Limitations

Despite its advantages, the framework has limitations. Privacy-preserving mechanisms such as zero-knowledge proofs introduce computational overhead and require specialized expertise for implementation and maintenance. Off-chain components, including encrypted storage and secure computation services, introduce additional trust and availability assumptions. Furthermore, interoperability with heterogeneous enterprise systems may require customization depending on industry and organizational constraints.

7.3. Integration into Real-World Supply Chain Platforms

The architecture is compatible with existing digital supply chain platforms and supply chain finance solutions. Tokenized payment obligations and milestone-based settlement can coexist with traditional banking rails, allowing fiat settlement to occur off-chain while maintaining verifiable on-chain state. Financial institutions, auditors, and regulators can participate with controlled visibility, supporting compliance without exposing proprietary business information.

7.4. Evolution of Privacy Layers

Privacy layers in the proposed framework can evolve alongside advances in blockchain technology. Layer-2 solutions, private rollups, and improved proof systems may further reduce latency and cost while enhancing confidentiality. As privacy-preserving infrastructure matures, these techniques can be integrated without fundamental changes to the overall architecture.

8. Conclusion and Future Work

This paper presented a privacy-preserving smart and secure contract framework for digital supply chain payments that balances automation, auditability, and confidentiality. By separating verification from disclosure through cryptographic commitments, zero-knowledge proofs, and off-chain encrypted data handling, the proposed approach addresses key barriers to the adoption of blockchain-based payment systems in multi-party supply chains. The framework supports milestone-based settlement, supply chain finance, dispute management, and regulatory auditability while maintaining strong security and practical performance.

The analysis demonstrates that privacy-enhancing mechanisms can be deployed without sacrificing scalability or operational efficiency. Future work includes exploring more efficient cryptographic constructions, supporting cross-chain settlement across heterogeneous blockchain networks, and integrating trusted IoT data sources to strengthen event verification. These directions can further enhance the applicability of privacy-preserving smart contracts in real-world digital supply chain ecosystems.

References

1. M. Hofmann and M. Rüsch, *"Industry 4.0 and the current status as well as future prospects on logistics,"* Computers in Industry, vol. 89, pp. 23–34, 2017.
2. G. Wood, *"Ethereum: A secure decentralised generalised transaction ledger,"* Ethereum Foundation, Tech. Rep., 2014.
3. K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, *"Blockchain-based supply chain traceability: Token recipes model manufacturing processes,"* Applied Sciences, vol. 9, no. 5, 2019.
4. A. Zyskind, O. Nathan, and A. Pentland, *"Decentralizing privacy: Using blockchain to protect personal data,"* in Proc. IEEE Security and Privacy Workshops, 2015, pp. 180–184.
5. E. Ben-Sasson *et al.*, *"Succinct non-interactive zero knowledge for a von Neumann architecture,"* in Proc. USENIX Security Symposium, 2014, pp. 781–796.
6. S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, *"Blockchain technology and its relationships to sustainable supply chain management,"* Int. J. Production Research, vol. 57, no. 7, pp. 2117–2135, 2019.
7. R. Gelsomino, A. Mangiaracina, A. Perego, and A. Tumino, *"Supply chain finance: A literature review,"* Int. J. Physical Distribution & Logistics Management, vol. 46, no. 4, pp. 348–366, 2016.
8. P. Pedersen, *"Non-interactive and information-theoretic secure verifiable secret sharing,"* in Proc. CRYPTO, 1991, pp. 129–140.
9. A. Chiesa *et al.*, *"On the complexity of succinct zero knowledge proofs,"* in Proc. EUROCRYPT, 2014, pp. 327–346.
10. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, *"Blockchain technology: Beyond bitcoin,"* Applied Innovation Review, no. 2, pp. 6–19, 2016.
11. F. Bourse, M. Minelli, M. Minihold, and P. Paillier, *"Fast homomorphic evaluation of deep discretized neural networks,"* in Proc. CRYPTO, 2018, pp. 483–512.
12. A. Gross, J. Notowidigdo, and J. Wang, *"Crisis-aware collections and household credit: Empirical evidence from federally declared disasters,"* Harvard Growth Lab Research Brief, 2023, doi: 10.70924/f83n6wqz/zkok8st3.
13. S. Remella, *"A unified security governance framework mapped to NIST CSF, ISO/IEC 27001, PCI DSS, and OWASP SAMM,"* International Journal of Artificial Intelligence, Big Data and Cloud Management Systems (IJAIBDCMS), vol. 3, no. 1, 2023, doi: 10.63282/3050-9416.IJAIBDCMS-V3I1P110.
14. A. Gupta, *"A centralized authentication and authorization framework for enterprise security modernization,"* International Journal of Science and Advanced Technology (IJSAT), vol. 16, no. 3, 2025, doi: 10.71097/IJSAT.v16.i3.8034.

15. ——, *"Beyond delinquency: The dual economic impacts of behavioral scoring in telecommunications,"* Global Business and Economics Review, 2023, doi: 10.70924/f83n6wqz/0i7t60r2.

16. D. Dhamodaran, *"Performance analysis of network security management models in high-speed networks,"* in Proc. Int. Conf. on Intelligent and Open Computing (INOCON), 2023, doi: 10.1109/INOCON57975.2023.10101329.