telecom

MDPI

Article

Interside: Blockchain Interoperability Architecture for Supply Chain Tracking

Suha Bayraktar [1,*] and Sezer Gören [2]

[1] Computer Engineering, Yeditepe University, Istanbul 34755, Türkiye
[2] Electrical and Computer Engineering, University of Massachusetts Dartmouth, North Dartmouth, MA 02747, USA; sgoren@umassd.edu
* Correspondence: sbayraktar@cse.yeditepe.edu.tr

Abstract

Modern supply chains rely on permissioned blockchain networks that frequently operate as isolated entities, resulting in fragmented data, limited visibility, and inconsistent governance. This research addresses these challenges by proposing "Interside," an interoperability framework designed explicitly for multi-network supply chain ecosystems. Using a design science research methodology, the study includes requirement analysis, framework development, prototype implementation, and a preliminary evaluation. The architecture features a main-chain/side-chain model that preserves network autonomy while enabling secure, auditable cross-chain communication and selective data sharing via a dedicated side-chain tracking ledger. A prototype was built with Hyperledger Fabric and Weaver components, and the framework was evaluated through a conceptual comparison with direct and hub-based approaches. Results show that Interside improves decentralization, governance autonomy, and auditability compared with existing models, with minor trade-offs in prototype performance. This work introduces a novel architectural blueprint for permissioned blockchain interoperability in supply chain environments and outlines practical directions for future large-scale performance benchmarking.

Keywords: blockchain; Hyperledger; interoperability; permissioned; side-by-side; supply-chain

1. Introduction

Global supply chains are becoming increasingly complex, spanning diverse regions and shaped by new regulations and digital infrastructure. This diversity leads to fragmented digital platforms and significant inefficiencies in tracking, verifying, and ensuring the integrity of goods and transactions. Diversified sectors, including telecoms, manufacturing, trade, health, and agriculture, have strong potential to improve existing processes by applying Blockchain technologies to critical use cases that require extensive tracking. Blockchain solutions in these sectors have emerged, offering traceability, transparency, immutability, and decentralized trust. Numerous pilot projects, such as [1], show governments aiming to digitize existing processes, including trade, to enhance traceability, improve security and trust, and reduce end-to-end execution times. In [2], Grossman argues that blockchain technology offers an opportunity to strengthen economic collaboration and stimulate economic growth in the Middle East and North Africa (MENA) region. Grossman also critiques the strategic frameworks various nations use to deploy blockchain solutions and transition toward digitalized economies. According to Grossmann, current implementations predominantly operate as isolated entities, lacking standardized mechanisms to facilitate

Check for updates

Academic Editor: Fabio D'Andreagiovanni

Received: 24 September 2026
Revised: 20 October 2026
Accepted: 26 October 2026
Published: 29 October 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

secure data exchange across organizations and ecosystems. Deploying these projects using single blockchain systems without interoperability hampers the realization of blockchain's potential in critical sectors, such as end-to-end supply chain management and tracking across different sectoral use cases, thereby perpetuating inefficiencies that blockchain was initially intended to resolve. As supply-chain tracking is critical for many of the sectors mentioned earlier, efforts to design and implement interoperability solutions that connect multiple blockchains have become a vital research area.

This study aims to design and validate a decentralized interoperability architecture that enables secure, auditable, and privacy-preserving data exchange across independently governed permissioned blockchains in supply-chain ecosystems. The specific objectives are:

(i) Identify the architectural limitations of existing interoperability models;
(ii) Propose a side-by-side main-chain/side-chain interoperability framework;
(iii) Implement a prototype using Hyperledger Fabric;
(iv) Evaluate the framework conceptually and experimentally against direct and hub-based approaches.

For effective, seamless, and secure supply chain tracking in these sectors, interoperability solutions among independent parties are a critical requirement for blockchain adoption. However, existing approaches, such as the direct integration of two blockchains, have significant shortcomings. Direct connections between blockchains introduce governance complexity and scalability limits, while another option, called centralized hub-based models, compromises decentralization and trust. These limitations prevent supply-chain networks from achieving the desired levels of visibility, accountability, and efficiency.

To address this gap, this paper introduces Interside, a decentralized side-by-side interoperability framework designed explicitly for permissioned blockchains, such as Hyperledger Fabric [3]. Unlike hub-based or direct-connection solutions, Interside preserves the autonomy of individual networks while enabling secure, verifiable, and auditable cross-chain interactions. The framework is designed to strike a balance between architectural soundness, strong security guarantees, and acceptable performance, offering a scalable pathway for global blockchain-enabled supply chains.

1.1. Problem Statement and Motivation

Permissioned blockchains [4] provide robust security and trust mechanisms for registered users. Blockchains generally offer transparency, immutability, and decentralized trust within isolated networks. However, these capabilities do not necessarily enable the interoperability required among permissioned blockchain networks in global supply chains spanning multiple sectors. Without the right interoperability solution, permissioned blockchains still lack support for secure, standardized data exchange across diverse organizational ecosystems that use their own blockchain solutions. This shortcoming hampers end-to-end visibility and accountability, thereby necessitating that organizations operate in silos despite adopting blockchain technologies. Consequently, blockchain networks underpinning globally distributed processes face inefficiencies, redundant verification procedures, and increased vulnerabilities in cross-border transactions. This project is motivated by the need for a decentralized interoperability framework that overcomes these limitations. The proposed approach must preserve the autonomy and governance of individual blockchain networks while enabling secure, scalable, and auditable cross-chain interactions. By addressing this gap, the research aims to unlock the full potential of blockchain in global supply chain use cases, delivering visibility, accountability, and efficiency across complex supply chain ecosystems.

1.2. Research Questions & Hypotheses

Building on the motivation to search for an ideal interoperability solution for permissioned blockchains, our study is guided by three core research questions:

- RQ1 (Architectural Design): How can a standardized interoperability architecture for permissioned blockchains be designed to overcome the limitations of isolated supply chain systems, while preserving decentralization and governance autonomy of each network?
- RQ2 (Security): How can the proposed architecture mitigate the security risks associated with direct interoperability, such as reliance on multiple SDKs, exposure of consensus proofs, and multi-ledger identity management, while ensuring trustworthy cross-chain data exchange?
- RQ3 (Performance): To what extent can the proposed architecture achieve comparable performance to direct interoperability approaches, while avoiding the bottlenecks of centralized hub-based and direct integrated solutions?

From these research questions, we derive the following hypotheses:

H1 (Architecture). *A standardized interoperability architecture for permissioned blockchains can be designed to connect multiple independent supply chain networks while preserving decentralization, governance autonomy, and privacy of each participant, unlike direct or hub-based approaches.*

H2 (Security). *By isolating interoperability into a dedicated architectural layer and relying on cryptographic anchors, the proposed architecture reduces the attack surface and mitigates security risks, including identity compromise, replay attacks, and failures of central hubs.*

H3 (Performance). *The proposed architecture can achieve comparable transaction performance to direct interoperability while avoiding the limitations of centralized hub models, maintaining acceptable efficiency as the number of participants increases.*

1.3. Scope of the Research Project and Intended Contribution

This study presents Interside as an architectural proof-of-concept rather than a fully developed interoperability system suitable for pre-production. The main goal is to articulate, model, and validate a side-by-side interoperability architecture for permissioned blockchains, without providing an extensively optimized, industry-scale implementation. Comprehensive distributed benchmarking, multi-server deployment, and performance stress testing require significant engineering resources and multi-node infrastructure, which are beyond the scope of this initial design-science phase. These activities are planned for the next project phase in 2027. Therefore, the current evaluation focuses on architectural correctness, feasibility, and initial performance observations in a controlled environment, which is appropriate for this stage of research.

1.4. Structure of the Manuscript

The remainder of this manuscript is organized as follows. Section 2 (Background and Related Works) introduces the fundamentals of permissionless and permissioned blockchains and outlines interoperability requirements and use cases in global supply chains. Related Works reviews prior research on blockchain interoperability, including the dimensions of interoperability, architectural approaches to cross-chain communication, and sector-specific frameworks, and identifies key research gaps that motivate the Interside framework. Section 3 (Methodology) details the research design, provides an overview of the proposed architecture, and explains the evaluation approach, data models, smart contract roles, and transaction flows that underpin Interside. Section 4 (Results and

Discussion) presents the comparative evaluation results, validates the framework against the stated hypotheses, and discusses implications for supply chain adoption, study limitations, and directions for future research. Finally, Section 5 (Conclusions) summarizes the study's contributions and highlights opportunities to advance blockchain interoperability in permissioned ecosystems.

2. Background and Related Works

When selecting an interoperability solution for supply chain management and end-to-end tracking, it is imperative to first understand the types of blockchain technologies involved and their compatibility with the chosen interoperability framework. In general, there are two types of blockchains:

- Permissionless;
- Permissioned.

Permissionless blockchains are primarily used in cryptocurrency applications and do not require stringent privacy or trust requirements [5], enabling widespread user participation and immediate access to services. Conversely, permissioned blockchains require stronger security, privacy, and trust mechanisms, as access is restricted to users who join by invitation and under predefined conditions. These permissioned blockchains are often regarded as private networks, predominantly employed across various industry sectors where privacy and rigorous access controls are required. Before delving into interoperability requirements, it is essential to understand the compliance and technical coverage needs of existing blockchain types to ensure proper use in the target interoperability solution. This approach will enable the selection of the appropriate blockchain type that aligns with the target interoperability architecture for supply chain use cases.

2.1. Interoperability Requirements in Supply Chain

Global supply chains involve multiple stakeholders, including suppliers, manufacturers, logistics providers, financial institutions, and regulators, each using different digital platforms, standards, and governance rules. This diversity requires careful consideration of permissioned blockchains that enable multi-party, multi-user transactions with private handling. This diversity creates significant challenges in achieving transparency, traceability, and trust throughout the entire supply chain. While blockchain technologies offer immutability and decentralized trust within individual networks, a lack of interoperability between blockchains prevents smooth, verified data exchange among stakeholders.

According to Kshetri [6], successful adoption of blockchain in supply chains depends on developing interoperability standards that enable networks to exchange data without compromising autonomy or security. Reference [7] emphasizes that interoperability must address not only the technical aspects of cross-chain communication but also governance, scalability, and trust management. Belchior et al. [8] further highlight that without common standards, organizations risk replicating silos on a distributed ledger, undermining the efficiency gains blockchain was meant to deliver. Moreover, achieving blockchain interoperability in supply chains requires addressing key issues, such as data fragmentation, regulatory compliance (e.g., customs regulations or trade laws), and reliable provenance across multiple participants and jurisdictions. Identifying the supply-chain use cases that most require blockchain interoperability is therefore essential to designing suitable solutions.

2.2. Blockchain Interoperability Use Cases in Supply Chain

Supply chains, like telecommunications, are heavily regulated, especially in customs clearance and financial transactions, which require stringent security, scalability, and trust.

Interoperability enables decentralized decision-making among multiple actors, improving efficiency and reducing disputes. Below are the predominant supply-chain applications where blockchain interoperability is essential.

2.2.1. Provenance and Traceability

A key challenge in global supply chains is ensuring product authenticity, accurately tracing origins, and validating certifications across diverse jurisdictions. For instance, sectors such as food safety, pharmaceuticals, and luxury goods require verifiable evidence of provenance (Kshetri [6]). Blockchain interoperability enables secure data exchange among independent networks, including raw material suppliers, manufacturers, and logistics providers, regarding certifications, inspections, and handling conditions. Without interoperability, stakeholders must duplicate verification efforts, reducing efficiency and increasing the risk of fraud. A decentralized interoperability framework enables different blockchain networks to share validated provenance data while maintaining their autonomy, thereby ensuring comprehensive end-to-end traceability (Belchior et al. [8]). Provenance and traceability for parts and goods can be applied across sectors such as telecommunications, manufacturing, and energy.

2.2.2. Trade Finance and Customs Clearance

Another critical aspect of blockchain interoperability is integrating financial services, including banks, insurers, and fintech providers, with logistics and customs networks. Traditional trade finance processes are often slow, labor-intensive, and prone to disputes. Implementing interoperable blockchain systems can streamline these processes by enabling financial institutions to access verified order and shipment data directly from supply chain networks (Hardjono, [7]). Likewise, customs authorities can authenticate documentation, including invoices and certificates of origin, and verify cross-border compliance without relying on manual reconciliation. Such interoperability can significantly reduce delays, diminish fraud, and improve adherence to international trade regulations (Belchior et al., [8]).

2.2.3. Logistics and Delivery Coordination

Efficient logistics management requires real-time coordination among producers, freight carriers, port operators, and last-mile delivery providers. Today, this coordination is hindered by fragmented IT systems and limited data visibility. By leveraging interoperable blockchain frameworks, logistics actors can exchange verified delivery records, shipment statuses, and route optimizations without relying on centralized intermediaries. This enables faster decision-making, reduces disputes over liability, and improves overall efficiency in global trade flows (Kshetri [6]; Belchior et al. [8]).

2.3. Supply Chain in Telecommunication

Blockchain interoperability also presents significant opportunities in the telecom supply chain by addressing challenges in provenance, logistics, and cross-operator coordination. Interoperable blockchains can secure the provenance of devices and components by linking records from manufacturers, logistics providers, and operators, thereby reducing the risk of counterfeits in network infrastructure. In multi-operator environments, particularly those with shared 5G infrastructure, interoperability enables transparent reconciliation of usage data and cost-sharing, eliminating the need for centralized brokers. Roaming and settlement processes also benefit from this, as interoperable permissioned blockchains between international operators support the real-time exchange of authenticated records, reducing settlement delays and fraud. In [9,10], various use cases are discussed for enhancing supply chain functions through blockchain interoperability required for telecoms. In logistics, in-

teroperability provides end-to-end visibility by connecting customs authorities, equipment manufacturers, and telecom operators, ensuring auditable supply chains for towers, fiber cables, and antennas. Service-level agreements (SLAs) in Network-as-a-Service models are further strengthened when monitoring data across different actors' blockchains can be cross-verified, thereby minimizing disputes. Finally, in the broader context of smart cities and IoT (Internet of Things) ecosystems, telecom blockchains can interoperate with those in adjacent sectors to enable the secure and trusted exchange of sensor and service data. Collectively, these use cases underscore the importance of interoperability as a crucial enabler of efficiency, transparency, and trust in modern telecom supply chains.

2.4. Related Works

Research on blockchain interoperability has grown significantly in recent years, leading to the development of various frameworks, taxonomies, and experimental implementations. A comprehensive review of these contributions is essential to contextualize this research within the broader academic discourse and to identify the existing gaps that underpin the proposed framework.

This section, beginning with an examination of current research on interoperability in supply chain applications, emphasizes practical integration considerations, such as blockchain-to-enterprise system connections and intra-chain decentralized application (dApp) interoperability [11]. It then analyzes how architectural trade-offs inherent in different blockchain designs, including permissionless and permissioned systems, affect interoperability requirements. Building on this foundation, the section reviews definitions and dimensions of interoperability, technical architectures that enable cross-chain communication, and challenges specific to permissioned blockchain environments.

Finally, the section discusses sector-specific use cases, security and governance trade-offs, and comparative evaluations of existing frameworks. These related works collectively underscore the limitations of current approaches and provide the rationale for the design of the Interside interoperability framework proposed in this paper.

2.4.1. Practical Interoperability Dimensions in Supply Chains

Most research on blockchain use cases in supply chains has focused on deploying a single blockchain network and enabling interoperability with internal enterprise applications through dApps. Ren et al. [12] describe three main approaches to blockchain interoperability: interoperability between a blockchain and external systems, interoperability between dApps operating on the same blockchain, and interoperability between independent blockchains. The first two approaches have dominated supply-chain projects to date. For example, many studies examine integrating blockchain with enterprise resource planning (ERP) systems or IoT platforms to enhance traceability and data sharing. In contrast, others demonstrate intra-chain dApp interoperability for provenance and auditing. Akyuz et al. [13] discuss integration strategies for ERP and blockchain to manage supply networks. They note that supply chain networks are increasingly referred to as supply networks, which could offer benefits for multi-party collaboration when blockchain and smart contracts are deployed. Mabrook et al. [14] extend this perspective by surveying blockchain interoperability specifically in supply chains, classifying seven distinct approaches: isolated, network, structural, semantic, specification, platform, and organizational interoperability. Their findings indicate that structural and semantic interoperability are relatively well covered in ERP/IoT integration and provenance applications. In contrast, platform- and organizational-level interoperability, especially across independent blockchains, remain underexplored.

2.4.2. System Design Considerations and Trade-Offs for Interoperability

Ref. [15] provides a comprehensive survey comparing permissionless and permissioned networks through the lens of the CAP (Consistency, Availability, Partition Tolerance) theorem. According to their findings, permissionless networks prioritize availability and partition tolerance. Bitcoin [16], recognized as the first permissionless cryptocurrency network, operates as a distributed consensus platform that uses the proof-of-work (PoW) [17] consensus protocol to validate transactions. In this framework, Bitcoin initiates transactions and adds them to blocks without complex logic. Consequently, Bitcoin is a non-Turing-complete [18] solution due to the absence of a loop mechanism [19]. In contrast, permissioned blockchain networks like Hyperledger leverage Smart Contracts to execute custom processes on a distributed ledger (DLT) and ensure transaction finalization, thus achieving Turing completeness. These networks can implement a more sophisticated consensus mechanism involving multiple steps, with various modules working together to reach final consensus. Therefore, permissioned networks tend to prioritize consistency over availability, a characteristic absent in permissionless networks. Ref. [15] even proposes a new architectural framework to redefine CAP for blockchain as Consensus achievement (C), Autonomy (A), and entropic Performance (P). The proposed framework in [20] concentrates on a single blockchain with distributed nodes. This shows that a blockchain solution chosen by a supply chain must not only meet the Turing-completeness requirement but also fulfill the new approach to the CAP theorem offered by blockchain. A candidate interoperability solution that connects two or more blockchains shall not compromise these basic requirements for achieving consensus, autonomy, and entropic performance, thereby providing a Turing-complete process. A single blockchain for a trade network [21] built using Hyperledger Fabric is illustrated in Figure 1. This approach integrates all access rights, trust anchors, and Turing-complete smart contract processes into a single platform. This single-blockchain architecture compromises the autonomy of each involved party (producer, customer, logistics, customs, etc.) and grants a super-administrator the authority to overrule the entire network. Therefore, each party must comply with the specifications deployed and applied by the ruling authority. This approach clearly contradicts the decentralized feature of blockchain.

2.4.3. Definitions and Dimensions of Blockchain Interoperability

Because deploying a single blockchain introduces significant disadvantages, the issue of interoperability warrants further discussion. For this study, the platform and organizational dimensions highlighted by Mabrook et al. are particularly relevant. Platform-level interoperability refers to the ability of heterogeneous blockchains (e.g., Hyperledger Fabric, Ethereum [22], Corda [23]) to exchange data without requiring a shared consensus mechanism. In contrast, organizational interoperability enables independent networks to collaborate without compromising governance autonomy. In this sense, using a single blockchain to deploy such a supply chain network is not a viable option. For deploying a final interoperability architecture, the platform and organizational dimensions covered by Mabrook et al. are critical for supply-chain ecosystems where suppliers, producers, logistics providers, customs authorities, and financial institutions must remain self-governed yet interlinked.

2.4.4. Technical Architectures for Cross-Chain Communication

The technical architecture of blockchain interoperability defines how independent blockchain systems interact to share data, verify events, or execute cross-chain transactions. Various models have been proposed in the literature and in industry implementations, each differing in decentralization, scalability, trust assumptions, and coupling among partici-

pating networks. The three predominant architectures for cross-chain communication are: direct (point-to-point), hub-based (also called intermediary), and middleware-based.

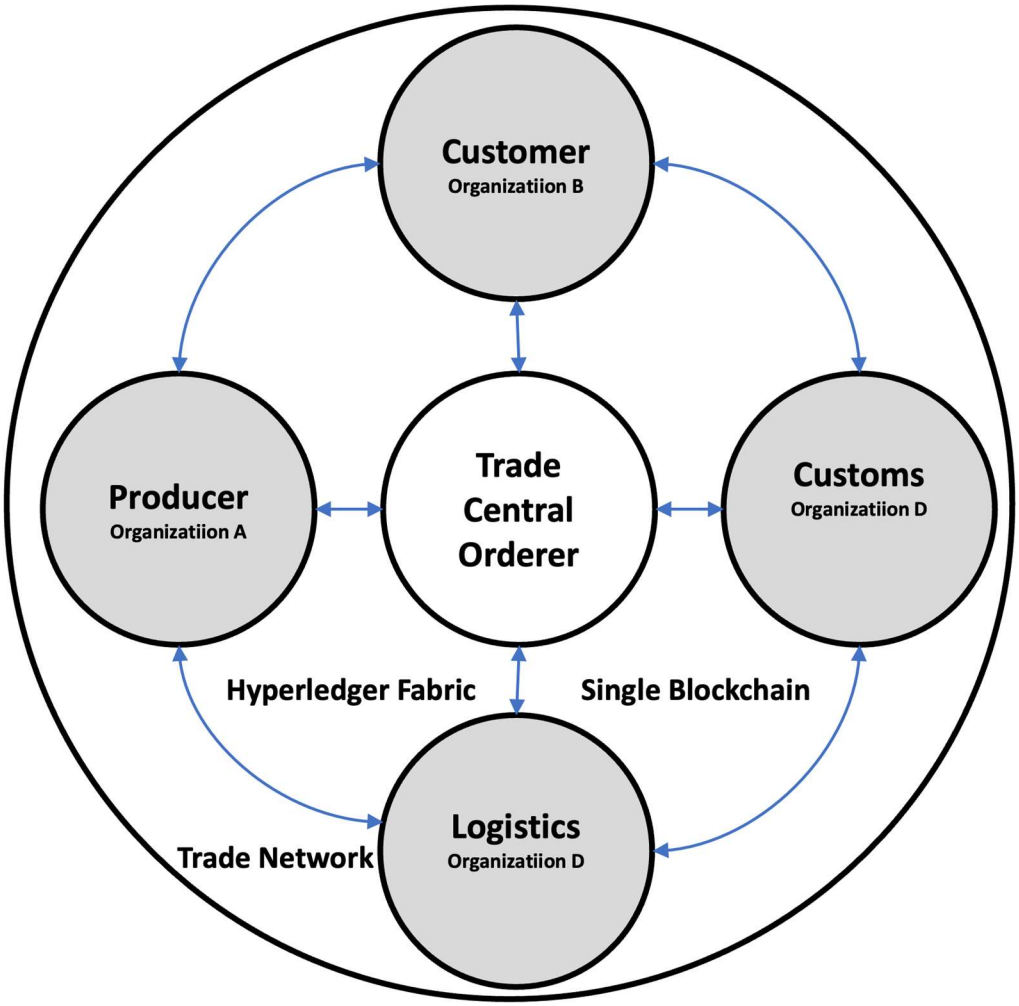


Figure 1. Trade network using a single blockchain [21].

2.4.5. Direct Integration (Point-to-Point Bridges)

Direct integration involves creating custom connections between two blockchain networks using bridge contracts, relays, oracles [24], or APIs. Each bridge handles data formatting, event detection, and message relaying in a bespoke manner. While direct connections offer high performance for transactions between two integrated chains and are tailored to specific use cases, they are inherently non-scalable; adding a new blockchain requires $n(n-1)/2$ connections to achieve full interoperability.

These architectures also pose security risks, including replay attacks [25], consensus manipulation [26], and double spending [27,28], particularly when cross-chain validation depends on off-chain relays. Governance becomes complex because both chains must agree on shared protocols, identity mapping, and data validation rules, often requiring participants to establish trust manually. Direct bridges create a complex interoperability landscape when more than two blockchains are integrated. In a fully connected point-to-point architecture with direct bridges, n blockchain networks require $O(n^2)$ distinct bidirectional connections.

2.4.6. Hub-And-Spoke Models/Intermediaries

Hub-based models centralize interoperability through a single coordination layer, often called an interoperability hub, router, or backbone. All participating blockchains connect to this hub, which mediates message passing, state synchronization, and data translation. This design significantly simplifies adding new blockchains and reduces redundant connections, enabling high connectivity with minimal configuration overhead.

Notable examples include Cosmos IBC [29–31], Polkadot's Relay Chain [32], and Hyperledger Cactus's pluggable interfaces [33]. However, these models often re-centralize trust and introduce a single point of failure (SPOF), potentially violating blockchain's decentralized ethos. Additionally, they may struggle with heterogeneous permission models, especially when permissioned and permissionless blockchains coexist within the same ecosystem.

2.4.7. Middleware and Protocol-Based Interoperability

Middleware-based solutions abstract cross-chain logic into dedicated interoperability layers that sit above existing blockchains. These platforms provide standard APIs, protocol adapters, and governance isolation mechanisms to enable message passing without exposing internal consensus or identity structures. Middleware can also handle asynchronous communication, version control, and policy enforcement across chains.

Examples include Hyperledger Cactus, Quant's Overledger [34], and LayerZero [35]. These solutions excel at protocol modularity and governance decoupling; however, they often add latency, resource overhead, and deployment complexity, particularly in high-throughput environments such as supply chains.

In summary, existing cross-chain architectures present a spectrum of trade-offs. Direct bridges deliver performance at the expense of scalability and security. Hub-based systems simplify integration but reduce decentralization. Middleware strikes a balance but introduces technical complexity and potential bottlenecks. These limitations underscore the need for a decentralized, policy-aware, and auditable solution like Interside, which isolates interoperability in a secure, side-by-side layer without compromising governance or scalability.

2.4.8. Supply Chain-Specific Interoperability Frameworks

Blockchain's application in supply chains has evolved from proof-of-concept pilots to production-grade systems across logistics, trade finance, and regulatory compliance. Yet many implementations remain fragmented, relying on isolated blockchains or siloed applications that cannot interoperate with other networks. As a result, platform- and organizational-level interoperability challenges persist, particularly in environments where multiple independent stakeholders (e.g., manufacturers, customs agencies, financial institutions) must collaborate without ceding governance control. Early efforts in blockchain-enabled supply chains typically integrated a single permissioned blockchain platform (e.g., Hyperledger Fabric) with internal enterprise systems, such as ERP or IoT platforms. These efforts focused primarily on semantic and structural interoperability, ensuring that data formats and process flows were compatible. However, platform-level interoperability, in which entirely different blockchain infrastructures must exchange data securely, remains underdeveloped. Several studies [6,8] highlight that organizational interoperability, the ability of independently governed networks to collaborate without pre-shared consensus or identity management, is a fundamental requirement in supply chains. For example:

- In trade finance, banks and customs agencies need access to validated shipment records without being on the same blockchain network.

- In provenance tracking, logistics firms, producers, and inspectors may each maintain separate blockchain systems, but must ensure end-to-end data continuity.
- During regulatory audits, agencies require verifiable, immutable access to transaction histories, even when the networks involved do not expose their internal consensus protocols.

Frameworks such as TradeLens [36,37] and We.Trade [38] attempted to address these issues through semi-centralized architectures but have faced criticism for relying too heavily on trusted intermediaries or shared consortium governance, limiting scalability and generalizability.

In [39], the authors explore blockchain interoperability frameworks and use cases, including a supply chain use case that uses Polkadot to connect parachains. Parachains, as independent blockchains, connect via the relay chain in the Polkadot network. However, this approach introduces a single point of failure and a potential bottleneck for performance and security.

This analysis highlights an ongoing gap between current frameworks and the complex, multi-actor landscape of global trade. It underscores that no single platform or entity has the authority to unilaterally dictate integration terms. These findings emphasize the critical need for genuinely decentralized interoperability solutions, specifically designed to accommodate the permissioned and multi-jurisdictional characteristics of supply chains.

2.4.9. Security, Governance, and Performance Trade-Offs

The design of any blockchain interoperability framework requires careful balancing of security, governance, and performance. These three dimensions often conflict, and optimizing for one may compromise the others.

2.4.10. Security

Security concerns in blockchain interoperability primarily stem from:

- Cross-chain replay attacks;
- Message spoofing;
- State inconsistency between ledgers;
- Identity compromise across ledgers.

Direct bridges between chains are especially vulnerable because they may require exposing consensus proofs, managing multiple SDKs, and sharing sensitive identity attributes across networks. In permissioned environments with strict access controls, such exposure is often unacceptable. Moreover, the absence of a standardized cryptographic anchoring mechanism introduces ambiguity about transaction finality across chains. Direct integration often exposes the access policies, trust anchors, and cryptographic proofs of both integrated networks to each other during smart contract execution.

2.4.11. Governance

Centralized or consortium-based hub models streamline interoperability by implementing a standardized governance framework. Nonetheless, these models often contravene fundamental blockchain principles, such as decentralization and autonomy. In the context of supply chains, it is imperative that stakeholders, including governmental agencies, logistics companies, and financial institutions, maintain full authority over their ledger governance, particularly regarding legal and compliance considerations. Consequently, interoperability architectures must be designed to avoid compromising local policies, membership criteria, or consensus mechanisms. Conversely, in direct models, while both networks typically

preserve their autonomy, the vulnerability introduced by exposing security components, as discussed in Section 2.4.10, undermines this autonomy.

2.4.12. Performance

Performance trade-offs include:

- Transaction throughput;
- Latency in data synchronization;
- Scalability with an increasing number of networks.

While direct bridges offer low latency for specific use cases, they scale poorly as more networks are added. By contrast, middleware solutions that abstract interoperability often introduce additional overhead. A poorly designed interoperability layer can become a bottleneck, especially when cross-chain validation is computationally intensive. Recent studies, such as [7,40], emphasize the need for architectures that modularize cross-chain interactions, isolate security domains, and support asynchronous communication to preserve both performance and resilience. Performance has been a known issue for blockchain networks since Bitcoin's launch. Ethereum was introduced to address Bitcoin's limitations, including performance and Turing completeness. Solana [41] was introduced to provide significant performance improvements for permissionless networks, as Ethereum's performance improvements were limited. In this respect, performance remains an important topic and must be addressed in a candidate's interoperability by considering integrated blockchain networks. Hyperledger Fabric has demonstrated performance results reported in [42,43]. This led this study to choose Hyperledger Fabric as a strong candidate.

All these constraints inform the design goals of the proposed Interside framework, which aims to achieve:

- Security through cryptographic anchoring and verification;
- Governance autonomy via side-by-side integration without shared consensus;
- Performance efficiency through minimal coupling and asynchronous communication.

2.4.13. Gaps in Current Research and Motivation for Interside

Despite significant progress in designing and evaluating blockchain interoperability frameworks, existing solutions remain largely inadequate for the needs of permissioned blockchain ecosystems in global supply chains. In [44], the authors propose an enterprise framework for blockchain interoperability that addresses several gaps identified in this paper. Although this approach provides useful guidance for identifying candidate interoperability solutions, it is not yet mature enough to support the development of a final solution. In [45], the authors analyze the features of well-known blockchains and propose a workflow for selecting the right interoperability solution. However, this paper does not clearly indicate the right interoperability solution, especially when critical requirements are taken into account. Numerous additional research papers and articles propose interoperability solutions that ultimately yield inadequate requirements. Most prior research has focused on direct bridges or centralized hubs that facilitate cross-chain communication but fail to fully address the unique challenges posed by regulated, multi-organizational environments.

First, direct point-to-point integrations often assume a homogeneous governance environment and require tight coupling between blockchains, which introduces severe scalability and governance overhead. These models also increase the attack surface because each new connection requires custom SDKs, message handlers, and cross-ledger validations that must be securely maintained.

Second, hub-and-spoke models, while reducing implementation complexity, often re-centralize trust, undermining the decentralization principles blockchain technology aims to uphold. By introducing a central coordination entity, these solutions undermine the need

for network autonomy, especially in supply chains where each participant (e.g., customs authorities, logistics firms, banks) must maintain complete control over their data and governance processes.

Third, middleware-based interoperability solutions are often designed for public blockchains and lack the essential access control and identity management features required by permissioned networks. Additionally, most academic and commercial implementations overlook diverse consensus mechanisms, non-standard transaction models, and jurisdictional privacy requirements common in cross-border trade environments. These gaps highlight the need for a new class of interoperability framework that:

- Preserves the autonomy and governance independence of each network.
- Ensures cryptographic verifiability and auditable communication.
- Scales horizontally without requiring centralized intermediaries.
- Aligns with blockchain-specific system constraints such as Turing completeness, CAP trade-offs, and regulated permissioning.

To meet these requirements, this study introduces Interside, a new side-by-side interoperability framework designed specifically for permissioned blockchain systems. Interside enables secure, decentralized cross-chain interactions without relying on centralized trust anchors or shared consensus mechanisms. We chose the side-by-side architecture based on the comparison approach in [9], which we consider a preliminary study. The approach in [9] evaluates blockchain interoperability solutions for telecom interoperability and concludes that the side-by-side architecture has the greatest potential. By abstracting interoperability into a dedicated architectural layer, the framework provides a flexible, performance-conscious, and auditable pathway for interconnecting heterogeneous supply chain networks. The design of Interside directly addresses the limitations identified in the current literature. It aims to bridge the gap between academic models and the real-world, production-grade interoperability demands of regulated industries. The following methodology section elaborates on the design and implementation of this approach.

3. Methodology

The work follows a design-science methodology to propose and validate an architecture. Accordingly, the contribution lies in the conceptual framework, reference models, data structures, and interoperability logic rather than in extensive performance benchmarking under distributed, production-grade conditions. The prototype implementation demonstrates feasibility and validates architectural decisions, not claiming full maturity or complete operational performance. The main scope is to develop and evaluate Interside, a side-by-side interoperability framework for supply chains. The methodology follows a three-phase process:

(i) Problem identification and requirement analysis.
(ii) Framework design and implementation.
(iii) Evaluation through architectural validation and performance assessment. This structured approach ensures that the framework is both theoretically grounded and practically applicable across homogeneous and heterogeneous supply-chain environments.

3.1. Research Design

The research design is guided by insights from the related works subsection, which highlight the scarcity of interoperability solutions at the platform and organizational levels. These gaps informed the central research questions (RQ1–RQ3) and hypotheses (H1–H3) introduced in Section 1.2. Specifically, the literature emphasized the need for architectures that

preserve governance autonomy (H1), mitigate security risks in cross-chain communication (H2), and maintain comparable performance without centralization bottlenecks (H3).

To address these objectives, this study employs a design science research methodology, structured into three phases:

- Problem identification and requirement analysis, in which interoperability challenges from the literature are translated into architectural requirements.
- Framework design and implementation, including conceptual modeling and prototype development on Hyperledger Fabric, using the Weaver [46] architecture to operationalize the Interside architecture.
- Evaluation through architectural validation and performance testing, benchmarking the proposed solution against direct and hub-based models using qualitative and quantitative methods.

This structured approach ensures that the Interside framework is both theoretically grounded in prior research and empirically validated for practical deployment across heterogeneous, multi-stakeholder supply chain ecosystems.

3.2. Architecture Overview

The Interside framework uses the Weaver architecture to establish a decentralized, side-by-side interoperability framework that integrates multiple permissioned blockchains without relying on centralized hubs. The proposed architecture and proof of concept support deploying three or more blockchains, though the original Weaver design demonstrates two. Its design incorporates interoperability chaincode modules, cryptographic anchors, and relay components to enable secure data exchange. In the Weaver-based architectures, relays route cross-chain messages, eliminating the need for a dedicated direct bridge between every pair of blockchains. If each blockchain maintains a single logical connection to the relay infrastructure, the number of blockchain-to-relay connections is O(n). Each participating network maintains its own consensus mechanisms, membership service provider (MSP), and governance structures, thereby ensuring operational autonomy. The interoperability layer orchestrates cross-chain requests and responses, enforces access controls, and ensures auditability through signed proofs and transaction logs. Figure 2 illustrates the proposed interoperability architecture. The interoperation code is triggered by events from the main chaincode (executed by producers, logistics, etc.), which converts data from the distributed ledger technology (DLT) into a simplified format. At this level, the autonomous network is isolated. The interoperation mechanism is only an event listener. This interoperability mechanism transmits the data to the relay component, which subsequently communicates with the relay component of the target blockchain (BC) network. Both the relay and interoperation components are part of the Weaver solution. The main chaincode of each network is adapted to support both interoperability functions and auxiliary BC layers. The side BCs enable end-to-end traceability throughout the supply chain. When the main chaincode in the primary BC executes a data transfer between independent blockchains, the same chaincode starts another process in the relay integrated with the side blockchain. This process transfers either all or a portion of the data to the side chain, facilitating access to tracking information. This approach ensures that the main chain remains autonomous, with tracking data accessible solely to end users with permissioned access rights via the side chain.

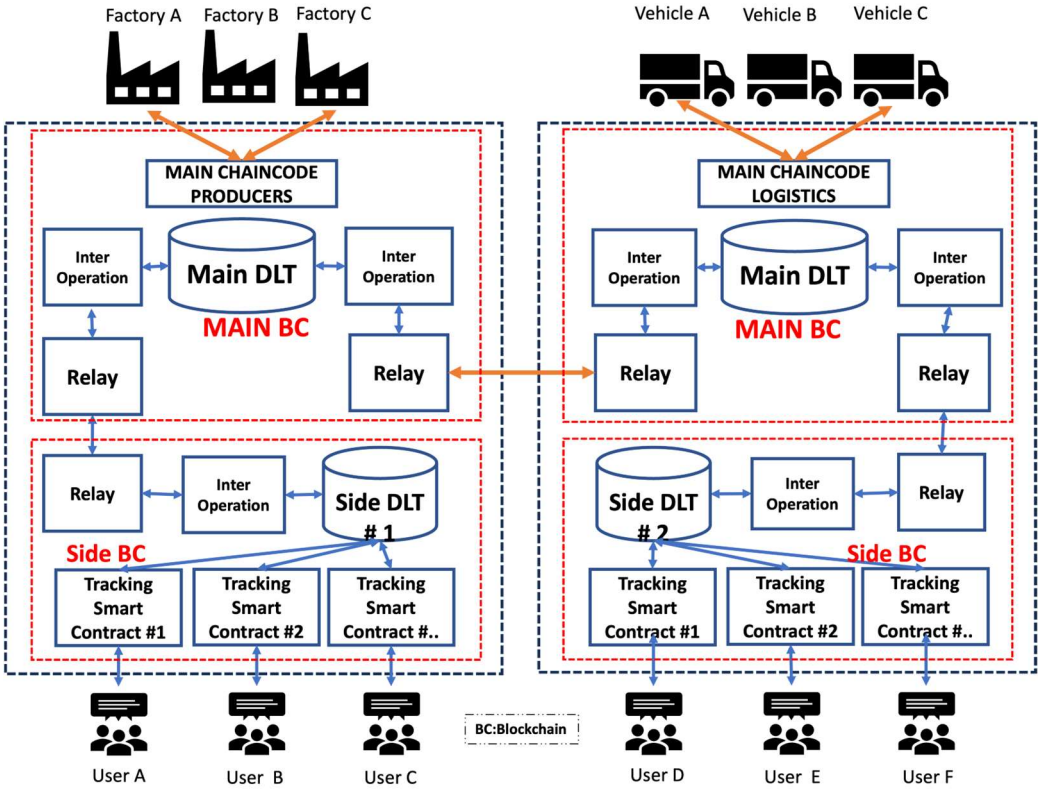


Figure 2. Multi-Domain Blockchain Interoperability Architecture Framework.

In contrast to existing interoperability frameworks such as Hyperledger Weaver and Hyperledger Cactus, the proposed Interside architecture introduces a dual-layer, parallel model that integrates both main chains and dedicated side chains. Within this framework, the side chain serves as an autonomous, permissioned ledger that records cross-chain transactions replicated from the main chains. This layer provides a secure interface for status queries by third-party stakeholders who are not authorized to access the main chains, enabling selective transparency without compromising governance.

Additionally, while previous models typically address interoperability between two blockchains, Interside is explicitly designed to support multi-chain environments composed of several autonomous permissioned networks operating concurrently. This approach extends beyond the pairwise or hub-based communication patterns observed in Weaver and Cactus. Neither Weaver nor Cactus implements a standalone, side-by-side main and side-chain architecture with a dedicated tracking ledger for selective disclosure and multi-network visibility. Consequently, the Interside framework introduces a novel architectural paradigm absent from existing interoperability solutions.

3.3. Evaluation Approach

To evaluate the framework, the study uses both qualitative and quantitative methods. Qualitatively, the architecture is benchmarked against design requirements derived from the literature (security, scalability, governance autonomy). Quantitatively, the study conducts a preliminary performance test in a simulated multi-network supply chain environment, measuring transaction throughput against direct interoperability and Interside. These results indicate that the proposed framework achieves comparable efficiency while offering stronger decentralization and security guarantees.

3.4. Data Models

Each supply-chain entity, such as raw material suppliers, producers, logistics providers, financial institutions, and customs authorities, maintains its own blockchain network with dedicated data models. Core records include orders, products, shipments, and certifications, each enriched with metadata such as Order ID, Product ID, Delivery ID, Customs ID, Quantity, Timestamp, and provenance information. Interoperability transactions are represented as signed claims that encapsulate proofs of authenticity and origin before being shared across networks. By standardizing data structures in this way, the framework ensures that cross-chain communication remains semantically consistent while allowing each network to retain local schema extensions. Figure 3 illustrates the overall data model that can be deployed in a traditional supply chain process for international trade. This data model can be adapted to other supply chain models in different sectors. The process is presented as a pre-proposed model and can be adapted to different use cases by using a unique ID concept based on the transaction flow.

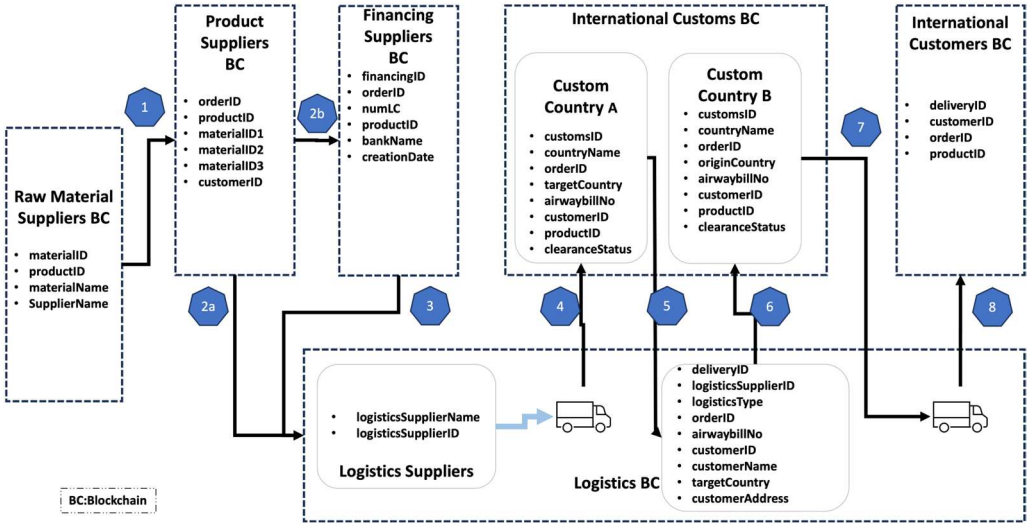


Figure 3. End-to-end supply chain data model.

Each network has a unique ID, such as orderID or deliveryID, that is passed as simple data between networks. Once these unique IDs are created, they can be tracked through side BCs.

3.5. Smart Contract Roles

The interoperability layer relies on two categories of smart contracts deployed across the networks:

- Main Blockchain Contracts
  - Smart Contracts (main chain code) for each main chain that perform cross-chain data transfers.
- Side Blockchain Contracts:
  - Service Publisher Contracts register available services (e.g., request status, delivery confirmation) that external networks can consume.
  - Service Subscriber Contracts enable networks to query or request services offered by others.
  - Transaction Retriever Contracts handle incoming cross-chain data, verify cryptographic proofs, and store validated information in local ledgers.

- Transaction Viewer Contracts provide user-facing access to verified cross-chain data, ensuring transparency and auditability for supply-chain participants.

Together, these smart contracts enforce decentralized access control, validate provenance, and enforce selective disclosure policies, ensuring that only authorized data is exchanged while maintaining privacy and compliance.

3.6. Cross-Chain Transaction Flow

The end-to-end interoperability process follows a structured transaction flow. A request is initiated in one network (e.g., a producer requests the delivery status of raw materials) via a sidechain using available sidechain smart contracts. Finally, the Transaction Viewer Contract enables stakeholders, such as banks or regulators, to inspect the verified data. This workflow ensures one-directional yet auditable information exchange, reflecting the operational needs of supply-chain ecosystems while preserving network autonomy. Having described the data structures, smart contract roles, and transaction workflows that underpin the Interside framework, it is now necessary to position the solution against existing interoperability approaches. While direct bridges, hub-based systems, and middleware frameworks such as Hyperledger Cactus each address interoperability to some extent, they exhibit different limitations in scalability, governance autonomy, and security. The following section compares these architectures, highlighting how Interside advances beyond prior models in meeting the requirements identified in this research.

3.7. Comparative Evaluation of Interoperability Architectures

To benchmark the proposed Interside framework against existing interoperability solutions, a structured evaluation framework was defined. This framework identifies twelve criteria particularly relevant to permissioned blockchain ecosystems and supply chain interoperability: decentralized architecture, interoperability mechanism, network decoupling, trust assumptions, cross-chain integration, smart contract roles, security and identity separation, advanced security, advanced policy management, auditability, production readiness, and performance. Two representative approaches were selected for comparison: direct interoperability models (e.g., point-to-point bridges) and Hyperledger Cactus, a pluggable middleware framework. Section 4 presents the results of this comparative analysis, highlighting how Interside addresses limitations identified in prior work while balancing decentralization, security, and efficiency.

3.7.1. Decentralization Architecture

Decentralization is a crucial approach for many sectors where autonomy and sovereignty are essential. In industries such as healthcare [47], the sovereignty of critical data is vital. The planned interoperability solution aims to preserve the integrity of the decentralized blockchain architecture while avoiding the introduction of any centralized components. Adding intermediary or broker modules would shift the system toward centralization, creating a single point of failure if an intermediary is inaccessible.

3.7.2. Interoperation Mechanism

The interoperability mechanism encompasses the foundational architecture and methodologies that enable communication across blockchain networks. This mechanism includes whether it operates synchronously or asynchronously, on-chain or off-chain, and whether it is event-driven or manually triggered. Direct Fabric SDK-based [48] integration via a dApp requires an application to manually read from and write to two distinct networks. Hyperledger Weaver implements an intent-based model, complemented by cryptographic proofs and relay services. In contrast, Hyperledger Cactus offers pluggable

connectors and APIs that facilitate broader compatibility with diverse Distributed Ledger Technologies (DLTs). The degree of standardization and modularity of the interoperability mechanism significantly influence its scalability and adaptability. As stated in [49], various interoperability techniques provide different mechanisms that must be aligned with and validated against the expected requirements. Reference [49] discusses three interoperability techniques: chain-based, dApp-based, and bridge-based. The interoperation mechanism for each of these options needs to be carefully considered and confirmed against the final requirements.

3.7.3. Network Decoupling

This illustrates the degree of interconnection between two or more blockchain networks during interoperation. In tightly coupled systems, networks know each other's schemas, identities, and runtime states, which limits flexibility. Conversely, loosely coupled networks, as exemplified by Weaver or Cactus, abstract these interactions through protocols or plugins. This abstraction reduces the integration burden and enables independent operation.

3.7.4. Trust Assumptions

Trust is vital for sectors such as finance, healthcare, and government, which rely on operational processes and applications that handle sensitive and private data. In decentralized finance (DeFi) [50], this becomes even more critical when blockchain solutions are deployed. If the underlying solutions rely on flawed or weak trust assumptions, security and privacy risks may arise. Any process or application designed for critical tasks must implement strong trust mechanisms. This concept concerns the implicit expectations each network has of the other during their interaction. Direct approaches often assume complete trust in the accuracy of the other party's information, while systems like Weaver and Cactus actively verify cross-network data using cryptographic assertions or validator attestations. Generally, systems that operate under minimal trust assumptions exhibit greater security.

3.7.5. Cross-Chain Integration

Cross-chain integration defines a dedicated service that facilitates message transmission across networks. Interside incorporates a relay that monitors events and submits verification proofs to designated target networks. Similarly, Cactus employs connectors or registries that serve as relays. In direct integration, the relay function is often absent, imposing greater obligations on the application layer. Implementing relays improves component decoupling and supports reactive interoperability.

3.7.6. Smart Contract Roles

Regulations governing smart contracts, commonly referred to as chaincode, clarify their role in interoperability contexts. In scenarios involving direct integration, these contracts often lack awareness of cross-chain logic. Smart contracts are crucial for Turing-complete processes; however, they should not be used directly as the final interoperability layer that interfaces with target blockchains. Solutions such as [51] use smart contracts as the primary mechanism for achieving interoperability. Such direct smart contract-based integrations carry potential risks. The Interside framework requires that chaincode be used to validate proofs, manage state transitions, and enforce access controls. Conversely, Cactus may depend less on smart contracts, delegating logic to plugin connectors, though integrating smart contracts can enhance the overall trust framework. Increased on-chain engagement significantly improves auditability and transparency.

3.7.7. Security Identity Separation

This separation distinguishes identities used for interoperability, such as relays, validators, or service agents, from application-level user identities, both logically and cryptographically. Separating identities is essential for maintaining minimal privileges and clearly delineating operational and user contexts, thereby mitigating risks in complex environments.

3.7.8. Advanced Security

Transport Layer Security (TLS) [52] provides encrypted communication, whereas Certificate Authorities (CAs) authenticate entities' identities. In the context of interoperability, both TLS and CA mechanisms must be upheld across blockchain boundaries rather than confined to a single network. Systems such as Weaver and Cactus integrate these protocols at both the interoperability and network levels, thereby supporting mutual TLS and the use of trusted root certificates.

3.7.9. Advanced Policy Management

Many sectors, such as healthcare [53], require enhanced policy management because of the criticality of the data processed in blockchain network-based solutions. An advanced interoperability system must adequately support the lifecycle management of keys and certificates, including revocation upon key compromise and rotation for regular maintenance and security hygiene. This can be viewed as advanced policy enforcement and automation of the interoperability transaction execution process. Traditional Fabric SDK methods often fall short of automating these processes. In contrast, Interside uses Management Service Provider (MSP) revocation lists, while Cactus incorporates modular security components that can enforce key-rotation policies.

3.7.10. Auditability

Many blockchain solutions are designed to be auditable [54,55]. Auditability is also a critical requirement for blockchain interoperability. It refers to the extent to which actions during interoperability can be traced, verified, and replayed. This includes signed messages, logs, state changes invoked by chaincode, and events related to proof verification. Solutions such as Weaver, which uses signed view proofs, and Cactus, which uses validator attestations, provide inherent audit trails. Conversely, manual methods seldom offer such capabilities.

3.7.11. Production Readiness

This option evaluates whether a system is mature enough for real-world deployment. Indicators include test coverage, version stability, production use cases, documentation quality, and active maintenance. Direct SDKs are stable but limited in functionality. Weaver is research-grade but progressing. Cactus is modular, actively developed, and already deployed in some enterprise trials.

3.7.12. Performance

This option evaluates the latency, throughput, and overhead of interoperation logic. Systems that use cryptographic proofs or multi-step verification may trade speed for enhanced security. Furthermore, performance depends on factors such as orchestration design, message queuing, and relay throughput. Direct SDK integrations provide expedited pathways; however, they may compromise safety. Interside and Cactus enhance event-driven, secure interoperability within reasonable parameters. The existing literature, such as [56], shows degraded performance when complex Hyperledger architectures with multiple organizations and peers are deployed.

The comparative analysis of existing interoperability approaches highlights a persistent gap: no current solution simultaneously achieves scalability, governance autonomy, strong security guarantees, and production readiness for permissioned blockchain networks in global supply chains. While direct and hub-based models offer specific performance or integration benefits, they introduce unacceptable trade-offs in decentralization and trust. Middleware approaches, though flexible, often struggle with latency and governance heterogeneity. These findings reinforce the need for a decentralized, side-by-side interoperability framework. Building on this gap, this section presents the Interside architectural framework, which provides a strong foundation for an ideal supply chain interoperability solution. Section 4 presents the comparative results, and the discussion demonstrates the viability of the proposed architecture.

3.8. Comparison with Layer-0 Interoperability Models

While Interside is tailored for permissioned supply-chain blockchains, Layer-0 architectures such as Polkadot XCMP and Cosmos IBC enable interoperability among public or semi-public heterogeneous chains. These models rely on shared security mechanisms, relay chains, or interchain message passing, requiring participating networks to operate within the same underlying ecosystem. Conversely, Interside supports fully autonomous, privately governed Fabric networks, eliminating the need for shared validators, consensus mechanisms, or security assumptions. This places Interside in a distinct architectural domain where private governance autonomy is paramount.

4. Results and Discussion

This section presents the evaluation results for the proposed Interside framework, including its performance relative to existing interoperability approaches. This section presents the evaluation results for the proposed Interside framework, including performance results relative to existing interoperability approaches. The discussion follows the evaluation framework introduced in Section 3.7, which treats decentralization, security, governance autonomy, and performance trade-offs as key criteria. Results are first reported through a comparative analysis of the Interside, Direct interoperability, and Hyperledger Cactus models. The section then examines how Interside addresses the identified research hypotheses (H1–H3), followed by a discussion of implications for supply-chain adoption, limitations of the current study, and directions for future research.

4.1. Rating Scale Definitions for the Evaluation

The evaluation scores for the compared solutions are ranked on a 100% scale and a numeric median scale. This scale is divided into five categories: very low (0–20%) or 10, low (21–40%) or 30, medium (41–60%) or 50, high (61–80%) or 70, and very high (81–100%) or 90. The following provides a detailed explanation of each category.

- Very High: The solution fully meets or exceeds the evaluation criteria without significant compromises. The design is top-tier, closely aligned with theoretical and practical needs, and demonstrates outstanding robustness, scalability, and adaptability. Any potential weaknesses are minor and do not significantly affect functional completeness or reliability.
- High: The solution demonstrates strong alignment with the evaluation criterion, with only minor trade-offs that have limited operational impact. It performs reliably under realistic conditions and offers high compatibility with relevant standards, though it may lack some advanced optimizations found in Very High-rated solutions.
- Medium: The solution shows balanced functional completeness. It meets the criterion at a basic or acceptable level, but has noticeable limitations or conditions that may

degrade functionality. The approach works and can be used, but it might require significant customization, additional safeguards, or operational changes to match higher-rated options.

- Low: The solution only partially meets the evaluation criterion and has significant limitations. Core requirements may be met under limited conditions, but the design introduces risks, inefficiencies, or dependencies that reduce its suitability for demanding or large-scale deployments.
- Very Low: The solution demonstrates poor alignment with the evaluation criterion. The solution largely fails to meet key requirements, exhibits critical vulnerabilities (such as single points of failure and security weaknesses), or imposes significant operational limitations. A major redesign or architectural overhaul would be required to improve functional coverage in this category.

The numeric equivalence of each category serves as the median value within its comparison range. An average score is then calculated for each solution being compared. The numeric results are qualitative and not a direct claim.

4.2. Comparative Results

Table 1 presents the comparison and evaluation results for interoperability solutions. Based on the requirements and essential feature set, researchers can identify the most suitable solution for specific use cases in their respective sectors.

Table 1. Comparative Results of Selected Interoperability Solutions.

Evaluation Topic	Interside		Direct		Cactus	
Decentralization Architecture	Very High	90	Low	30	Very Low	10
Interoperation Mechanism	Very High	90	Medium	50	High	70
Network Decoupling	Very High	90	Low	30	High	70
Trust Assumptions	Very High	90	Medium	50	High	70
Cross-chain Integration	Medium	50	Very Low	10	High	70
Smart Contract Roles	Very High	90	Low	30	High	70
Security Identity Separation	Very High	90	Medium	50	High	70
Advanced Security	Very High	90	Medium	50	Very High	90
Advanced Policy Management	Very High	90	Low	30	Very High	90
Auditability	Very High	90	Medium	50	High	70
Production Readiness	Medium	50	Low	30	High	70
Performance	Very Low	10	Very High	90	High	70
Average Scores		77		42		68

The results demonstrate the architectural advantages of Interside across nearly all critical dimensions:

- Decentralization & Trust Assumptions: Interside enforces side-by-side execution, eliminating centralized coordination and preserving full network autonomy, whereas Cactus and direct bridges rely on centralized hubs or trusted middleware layers that provide limited coverage of decentralization and trust.
- Security Features: Interside provides strong identity separation, advanced policy enforcement, and cryptographic auditing, all of which are vital in multi-jurisdictional

supply chain contexts where compliance and access control are mandatory. Built on Hyperledger and Weaver components, Weaver has a strong security platform [46] with multi-layered security components.

- Network Decoupling: Interside received a very high score as it enables interoperability between independently governed permissioned networks without forcing consensus homogenization or identity sharing. In a direct approach, tight identity integration endangers existing identities on both integrated blockchains which is a low coverage.
- Smart Contract Integration: Interside allows each blockchain to retain its own smart contract logic, enabling localized decision-making while still participating in cross-chain transactions. Direct approaches share smart contracts, which introduce security concerns through shared identities, although Cactus resolves this with an intermediary layer that provides better smart contract integration.
- Performance: The only trade-off is throughput, where direct bridges are faster in isolated use cases. However, this comes at the cost of security, auditability, and scalability, which are non-negotiable in regulated supply chain environments. Interside, built on Hyperledger Fabric, provides additional scalability through customer designs, such as [57], when required. However, the additional security layers needed to achieve strong identity isolation between integrated blockchains are likely to reduce performance.

4.3. Preliminary Performance Results

The preliminary performance evaluations were conducted on a single macOS computer with minimal network latency. The measurements are based on end-to-end time measurements and not on each detailed layer, especially in Interside. Because both direct and Interside are built on Hyperledger Fabric, while Weaver adds additional layers on top, we hypothesize that Interside's additional interaction layers are the primary source of the observed latency overhead, increasing the total processing time for read operations. Conversely, update/insert latency is about 10–20% higher than with the direct method, which requires multiple access policy checks with deployed network artifacts. Read latency is about four hundred times higher, a significant performance issue. The side-by-side architecture includes two additional components, interoperation and relay, that add processing delays to transactions. Neither component interacts with the distributed ledger and serves only a functional role. Therefore, their impact is recognized, but they do not introduce significant delays. Direct integration delivers significantly better performance than a side-by-side architecture. The increased number of layers in the side-by-side approach, especially within Hyperledger Fabric, requires an approval process to ensure secure transaction processing. Notably, for read operations, we observed a performance gap of over four hundred times between direct integration and the side-by-side architecture. The extra layers introduced by side-by-side are the main reason for these substantial differences. Because this performance comparison is a proof of concept, deeper tests on a distributed, complex architecture with multiple servers and nodes are needed to draw stronger conclusions.

It is important to emphasize that these performance results reflect the limitations of the prototype environment rather than the architecture's inherent scalability constraints. The implementation ran on a single-machine setup without distributed peers, optimized relay services, or parallel event processing. As a result, the observed latency is primarily driven by prototype-level overhead and does not constitute a definitive benchmark of Interside's performance potential. A full multi-node distributed setup, which requires substantially more infrastructure and operational resources, is planned for a subsequent phase of this research. Future evaluations will include multi-peer Fabric deployments, relay clustering, and stress testing under realistic workloads.

4.4. Latency Interpretation and Architectural Implications

The performance gap should be viewed as a prototype artifact rather than a flaw in the Interside architecture. Testing in a single-machine setup with serialized relay processing, synchronous event handling, and non-optimized chaincode paths introduces additional latency during cross-chain operations, especially for read flows that traverse multiple layers. In production, improvements such as parallel relay processing, batched verification, asynchronous acknowledgments, dedicated side-chain nodes, and separate event channels can significantly reduce this impact. Further multi-node testing can be planned to assess architectural impacts and determine whether better processing times can be achieved.

4.5. Implications for Supply Chain Adoption

The comparative evaluation highlights that blockchain interoperability frameworks must be assessed not only on performance but also on their ability to preserve decentralization, enforce governance autonomy, and ensure auditable security. For global supply chains, these attributes are more decisive than raw transaction throughput.

In practice, the findings suggest that Interside is well-suited to sectors with multiple stakeholders operating under independent governance who require trusted, cross-border data exchange. For example, in trade finance, Interside enables banks and customs authorities to validate shipment data without relying on a centralized hub. In provenance and traceability, logistics providers, manufacturers, and regulators can share signed proofs of product origin while retaining control of their local ledgers. In telecom supply chains, where equipment vendors, network operators, and regulators must collaborate across jurisdictions, Interside's policy-aware interoperability ensures that sensitive infrastructure data is shared selectively and verifiably.

These implications underscore the importance of side-by-side interoperability as a pathway to industry adoption, distinguishing Interside from failed consortium models such as We.Trade, which struggled with centralization, limited scalability, and adoption barriers.

4.6. Limitations of the Study

While the evaluation shows promising results, several limitations must be acknowledged. First, the comparative assessment was conducted in Hyperledger Fabric testbed environments, which may not fully reflect the scalability challenges of global-scale deployments. Second, the analysis was limited to two baseline interoperability approaches (Direct and Cactus); including Layer-0 frameworks such as Cosmos IBC, Polkadot XCMP, or LayerZero would provide a broader comparative perspective. Third, the performance evaluation was limited to simulated supply chain scenarios; real-world case studies with industry partners would strengthen the generalizability of the findings. Finally, although Interside emphasizes auditability and policy enforcement, the framework's usability and governance processes in large consortia remain to be tested in practice.

4.7. Future Research Directions

Building on these limitations, several avenues for future research are identified. One promising direction is to integrate Interside with Layer-0 interoperability protocols (e.g., Cosmos, Polkadot, Avalanche [58], LayerZero) to explore hybrid approaches that combine side-by-side autonomy with high-throughput messaging protocols. Another area is optimizing the performance of interoperability flows, particularly in high-volume supply chain networks, such as those in telecom or cross-border trade, where latency and throughput remain critical. Furthermore, research should investigate legal and regulatory alignment, assessing how frameworks like Interside can comply with emerging digital trade standards and data sovereignty laws. Finally, extending the evaluation to multi-domain

ecosystems, such as telecom, energy, and healthcare, will demonstrate the generalizability of the side-by-side approach beyond supply chains.

Together, the results, validation, and implications underscore that interoperability in permissioned blockchains cannot be reduced to technical performance alone. By prioritizing decentralization, governance autonomy, and auditability, the Interside framework addresses the shortcomings of prior models and offers a viable path to enterprise adoption. Future work will expand its scalability, cross-domain applicability, and regulatory compliance, ensuring its readiness for production-grade deployment across global supply chain ecosystems.

4.8. Contribution to the Research Space

This study makes the following contributions to research on blockchain interoperability in supply chains:

- Problem Identification: Provides a systematic analysis of existing interoperability approaches (direct, hub-based, and middleware) and highlights their limitations in permissioned blockchain supply chains, particularly regarding decentralization, governance autonomy, and scalability.
- Framework Design: Introduces Interside, a novel side-by-side interoperability framework that enables secure, auditable cross-chain communication while preserving each blockchain network's autonomy and governance.
- Technical Implementation: Demonstrates Interside's feasibility through conceptual modeling and prototyping on Hyperledger Fabric, defining explicit smart contract roles, data models, and transaction flows to enable interoperability.
- Comparative Evaluation: Benchmarks Interside against direct integration and Hyperledger Cactus across twelve criteria, demonstrating high achievement in decentralization, governance, security, and auditability, with acceptable trade-offs in transaction throughput.
- Practical Implications: Provides actionable insights for adopting interoperability in real-world supply chains, including logistics, trade finance, and telecom.

5. Conclusions

Global supply chains increasingly rely on blockchain technologies to enhance transparency, provenance, and trust across distributed ecosystems. However, as this study emphasizes, poor interoperability among permissioned blockchains undermines these objectives by maintaining data silos, causing governance conflicts, and reducing operational efficiency. Existing interoperability strategies, whether through direct point-to-point connections, hub-based coordination, or middleware solutions, offer limited effectiveness and often entail trade-offs among scalability, decentralization, and trustworthiness. To mitigate these limitations, this study presents Interside, a decentralized interoperability framework tailored explicitly for permissioned blockchains. Unlike hub-based or direct models, Interside maintains governance autonomy while enabling secure, auditable, and policy-compliant cross-chain communication. The framework was developed using a design science methodology and empirically validated through comparative analysis with representative models, such as direct bridges and Hyperledger Cactus. The findings substantiate that Interside provides a high degree of decentralization, governance autonomy, and security assurances, coupled with auditability and production readiness that align with supply-chain operational requirements. Although Interside's performance is significantly lower than that observed in direct integration approaches, it shall be confirmed whether the preliminary results meet acceptable thresholds for enterprise application contexts, thereby corroborating the research hypotheses (H1–H3). These outcomes emphasize

the overarching principle that, in regulated multi-stakeholder environments, governance and trust considerations outweigh raw throughput metrics. Practically, the adoption of frameworks such as Interside has significant implications for logistics coordination, trade finance, telecommunications, and regulatory compliance, where autonomous actors must interoperate without compromising control or exposing sensitive data.

Interside delivers practical benefits across supply chain scenarios by enabling controlled, verifiable data exchange via its dedicated side-chain system. In trade finance, for instance, banks and insurers can access verified transaction proofs from the side-chain without accessing sensitive operational data stored on the main chains, supporting compliance while preserving privacy. Likewise, in logistics and customs processes, the side-chain can aggregate shipment-level events from multiple independent networks to enable faster auditing, cross-border verification, and regulatory checks. Even at the prototype stage, the side-chain reduces reconciliation efforts by providing a unified ledger for third-party verification, eliminating the need for bilateral information sharing between organizations. Early observations indicate reduced manual effort and faster retrieval of proof data, though a full quantitative evaluation of these efficiency gains will occur during the next research phase.

The proposed architecture mitigates key risks of cross-chain interoperability by using a side-by-side model that does not alter, overload, or expand participating blockchains' consensus processes. As a result, the number of consensus rounds, validator actions, and ledger-write events on the main chains remains unchanged, keeping both computational and operational costs confined to the lightweight side-chain layer. The design also reduces reliance on external oracles by anchoring verification in on-chain proofs rather than off-chain data sources, thereby decreasing exposure to oracle failures or manipulation. Although relays may introduce an attack surface, they operate within authenticated channels and restricted trust domains. Future versions will include relay clustering, threshold-based verification, and isolated execution environments to minimize single-point vulnerabilities. Governance remains decentralized because each blockchain retains full control over its membership, identity management, and policy rules; the sidechain only allows selective disclosure without affecting main-chain decision-making. Finally, dispute resolution is improved through tamper-evident audit trails on both the main chains and the side-chain, providing verifiable, cross-network evidence for multi-party conflict resolution, while recognizing that legal adjudication may be necessary in some cases.

This study advances the current state of research on blockchain interoperability by demonstrating a viable, scalable alternative to centralized or consortium-bound models. Future research should build on this work by integrating Interside with emerging Layer-0 protocols, optimizing performance for high-volume deployments, and validating adoption through industry pilot programs. Addressing these challenges may position Interside as a fundamental component of next-generation blockchain-enabled supply chain systems, thereby enhancing operational efficiency and systemic resilience.

Author Contributions: Conceptualization, S.B.; methodology, S.B. and S.G.; software, S.B.; validation, S.B.; formal analysis, S.B. and S.G.; investigation, S.B.; resources, S.B. and S.G.; data curation, S.B.; writing—original draft preparation, S.B.; writing—review and editing, S.B. and S.G.; visualization, S.B.; supervision, S.G.; project administration, S.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: During the preparation of this manuscript, the authors used Grammarly 1.119.0.0 for the purposes of grammar checks and inconsistencies in the sentences. No text, graphic, table is generated by using AI tools. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. HyperLedger. Case Study: Dubai's Digital Silk Road modernizes trade with HyperLedger Fabric. 2022. Available online: https://www.lfdecentralizedtrust.org/hubfs/Hyperledger/Printables/Hyperledger_CaseStudy_Avanz_Printable_022221.pdf (accessed on 24 October 2026).
2. Grossman, M. Blockchain in the Middle East and North Africa (MENA): Opportunities for regional integration and economic growth. *J. Int. Bus. Manag.* **2022**, *5*, 01–19. [CrossRef] [PubMed]
3. Hyperledger Fabric. Available online: https://www.hyperledger.org/projects/fabric (accessed on 24 October 2026).
4. Polge, J.; Robert, J.; Le Traon, Y. Permissioned blockchain frameworks in the industry: A comparison. *Ict Express* **2021**, *7*, 229–233. [CrossRef]
5. Peng, L.; Feng, W.; Yan, Z.; Li, Y.; Zhou, X.; Shimizu, S. Privacy preservation in permissionless blockchain: A survey. *Digit. Commun. Netw.* **2021**, *7*, 295–307. [CrossRef]
6. Kshetri, N. Blockchain Standardization in Practice: Contrasting European Union and US Approaches. *Computer* **2025**, *58*, 100–108. [CrossRef]
7. Li, W.; Liu, Z.; Chen, J.; Liu, Z.; He, Q. Towards blockchain interoperability: A comprehensive survey on cross-chain solutions. *Blockchain Res. Appl.* **2025**, *6*, 100286. [CrossRef]
8. Belchior, R.; Vasconcelos, A.; Guerreiro, S.; Correia, M. A survey on blockchain interoperability: Past, present, and future trends. *ACM Comput. Surv.* **2021**, *54*, 168. [CrossRef]
9. Bayraktar, S.; Gören, S.; Serif, T. Blockchain Interoperability for Future Telecoms. *Telecom* **2025**, *6*, 20. [CrossRef]
10. Minz, S.S.; Mikkilineni, R.; Dewangan, S. Transformation of the Telecom Industry as a Result of Blockchain Technology in India. In *Building Secure Business Models Through Blockchain Technology: Tactics, Methods, Limitations, and Performance*; IGI Global: Hershey, PA, USA, 2023; pp. 66–87.
11. Raval, S. *Decentralized Applications: Harnessing 's Blockchain Technology*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2016.
12. Ren, K.; Ho, N.-M.; Loghin, D.; Nguyen, T.-T.; Ooi, B.C.; Ta, Q.-T.; Zhu, F. Interoperability in Blockchain: A Survey. *IEEE Trans. Knowl. Data Eng.* **2023**, *35*, 12750–12769. [CrossRef]
13. Akyuz, G.A.; İleri, O. A Comparative Analysis of Blockchain-Smart Contracts-ERP Integration Strategies for Supply Network (SN) Collaboration. *IEEE Access* **2025**, *13*, 144887–144907. [CrossRef]
14. Al-Rakhami, M.; Al-Mashari, M. Interoperability approaches of blockchain technology for supply chain systems. *Bus. Process Manag. J.* **2022**, *28*, 1251–1276. [CrossRef]
15. Anagnostakis, A.G.; Glavas, E. The New CAP Theorem on Blockchain Consensus Systems. *Future Internet* **2025**, *17*, 157. [CrossRef]
16. Brewer, E. A certain freedom: Thoughts on the CAP theorem. In Proceedings of the 29th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, Zurich, Switzerland, 25–28 July 2010; p. 335.
17. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://assets.pub-pub.org/d8wct41f/31611263538139.pdf (accessed on 20 August 2025).
18. Turing, A. *Intelligent Machinery (1948)*; Copeland, J.B., Ed.; Clarendon Press: Oxford, UK, 2004; p. 395.
19. Sriman, B.; Ganesh Kumar, S.; Shamili, P. Blockchain technology: Consensus protocol proof of work and proof of stake. In *Intelligent Computing and Applications: Proceedings of ICICA 2019*; Springer: Singapore, 2020; pp. 395–406.
20. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. White Paper. 2014. Available online: https://github.com/ethereum/ethereum-org-website/tree/dev/public/content/whitepaper/whitepaper-pdf (accessed on 25 October 2026).
21. Baset, S.A.; Desrosiers, L.; Gaur, N.; Novotny, P.; O'Dowd, A.; Ramakrishna, V. *Hands-on Blockchain with Hyperledger: Building Decentralized Applications with Hyperledger Fabric and Composer*; Packt Publishing Ltd.: Birmingham, UK, 2018.
22. Buterin, V. Ethereum Whitepaper. GitHub Repositories. 2013. Available online: https://static.peng37.com/ethereum_whitepaper_laptop_3.pdf (accessed on 25 October 2026).
23. R3 Corda. Available online: https://r3.com/ (accessed on 24 October 2026).
24. Ezzat, S.K.; Saleh, Y.N.M.; Abdel-Hamid, A.A. Blockchain oracles: State-of-the-art and research directions. *IEEE Access* **2022**, *10*, 67551–67572. [CrossRef]
25. Ramanan, P.; Li, D.; Gebraeel, N. Blockchain-based decentralized replay attack detection for large-scale power systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *52*, 4727–4739. [CrossRef]

26. Putz, B.; Pernul, G. Detecting blockchain security threats. In *Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain)*; IEEE: Piscataway, NJ, USA, 2020; pp. 313–320.
27. Iqbal, M.; Matulevičius, R. Exploring sybil and double-spending risks in blockchain systems. *IEEE Access* **2021**, *9*, 76153–76177. [CrossRef]
28. Kumar, A.; Sah, B.K.; Mehrotra, T.; Rajput, G.K. A review on double spending problem in blockchain. In *Proceedings of the 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*; IEEE: Piscataway, NJ, USA, 2023; pp. 881–889.
29. Cosmos. Cosmos Network. Available online: https://cosmos.network/ (accessed on 25 October 2026).
30. Kwon, J.; Buchman, E. Cosmos whitepaper. A Network of Distributed Ledgers. 2019. Available online: https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md (accessed on 25 October 2026).
31. Goes, C. The interblockchain communication protocol: An overview. *arXiv* **2020**, arXiv:2006.15918.
32. Wood, G. Polkadot: Vision for a Heterogeneous Multi-Chain Framework. White Paper. 2016. Available online: https://github.com/polkadot-io/polkadotpaper/raw/master/PolkaDotPaper.pdf (accessed on 25 October 2026).
33. Montgomery, H.; Borne-Pons, H.; Hamilton, J.; Bowman, M.; Somogyvari, P.; Fujimoto, S.; Belchior, R. Hyperledger Cactus Whitepaper. 2020. Available online: https://github.com/hyperledger/cactus/blob/main/whitepaper/whitepaper.md (accessed on 24 October 2026).
34. Verdian, G.; Tasca, P.; Paterson, C.; Mondelli, G. *Quant Overledger Whitepaper. Release V0.1*; Quant Network: London, UK, 2018; Volume 1, p. 31.
35. Rohrer, E.; Tschorsch, F. Blockchain layer zero: Characterizing the bitcoin network through measurements, models, and simulations. In *Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN)*; IEEE: Piscataway, NJ, USA, 2021; pp. 9–16.
36. Ahmed, W.A.; Rios, A. Digitalization of the international shipping and maritime logistics industry: A case study of TradeLens. In *The Digital Supply Chain*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 309–323.
37. Jovanovic, M.; Kostić, N.; Sebastian, I.M.; Sedej, T. Managing a blockchain-based platform ecosystem for industry-wide adoption: The case of TradeLens. *Technol. Forecast. Soc. Change* **2022**, *184*, 121981. [CrossRef]
38. Petersen, D. Transforming trade finance via blockchain: The We. Trade platform. In *Blockchain in Supply Chain Digital Transformation*; CRC Press: Boca Raton, FL, USA, 2023; pp. 74–93.
39. Wilson, S.; Adu-Duodu, K.; Li, Y.; Solaiman, E.; Rana, O.; Ranjan, R. Exploring blockchain interoperability: Frameworks, use cases, and future challenges. *Systems* **2026**, *14*, 388. [CrossRef]
40. ITU-T. *Technical Requirements on Inter-Chain Interoperability for Permissioned Distributed Ledger Technologies*; Recommendation, document ITU-T F.751.21, 2024; International Telecommunication Union: Geneva, Switzerland, 2024.
41. Yakovenko, A. Solana: A New Architecture for a High Performance Blockchain v0. 8.13.2018. Available online: https://coincode-live.github.io/static/whitepaper/source001/10608577.pdf (accessed on 20 August 2025).
42. Foschini, L.; Gavagna, A.; Martuscelli, G.; Montanari, R. Hyperledger fabric blockchain: Chaincode performance analysis. In *Proceedings of the ICC 2020 IEEE International Conference on Communications (ICC)*; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
43. Shalaby, S.; Abdellatif, A.A.; Al-Ali, A.; Mohamed, A.; Erbad, A.; Guizani, M. Performance evaluation of hyperledger fabric. In *Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*; IEEE: Piscataway, NJ, USA, 2020; pp. 608–613.
44. Mafike, S.S.; Mawela, T. An enterprise framework for blockchain interoperability. *Electron. Mark.* **2026**, *36*, 14. [CrossRef]
45. Tate, R.V.; Mane, S.B. A review on current state of art of a blockchain interoperability. *ICT Express* **2026**, *12*, 444–458. [CrossRef]
46. Weaver. Available online: https://hyperledger-cacti.github.io/cacti/weaver/introduction/ (accessed on 24 October 2026).
47. Said, H.E.; Al Barghuthi, N.B.; Badi, S.M.; Hashim, F.; Girija, S. Developing a Decentralized Blockchain Framework with Hyperledger and NFTs for Secure and Transparent Patient Health Records. In *The International Conference on Innovations in Computing Research*; Springer Nature: Cham, Switzerland, 2024; pp. 478–489.
48. Hyperledger Fabric SDKs. Hyperledger Foundation. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/fabric-sdks.html (accessed on 20 August 2025).
49. Wang, G.; Wang, Q.; Chen, S. Exploring blockchains interoperability: A systematic survey. *ACM Comput. Surv.* **2023**, *13*, 290. [CrossRef]
50. Bodo, B.; De Filippi, P. Trust in context: The impact of regulation on blockchain and DeFi. *Regul. Gov.* **2024**, *19*, 740–760. [CrossRef]
51. Zala, K.; Modi, V.; Giri, D.; Acharya, B.; Mallik, S.; Qin, H. Unlocking blockchain interconnectivity: Smart contract-driven cross-chain communication. *IEEE Access* **2023**, *11*, 75365–75380. [CrossRef]
52. Kareem, Y.; Djenouri, D.; Ghadafi, E. A Survey on Emerging Blockchain Technology Platforms for Securing the Internet of Things. *Future Internet* **2024**, *16*, 285. [CrossRef]
53. Sutradhar, S.; Karforma, S.; Bose, R.; Roy, S.; Djebali, S.; Bhattacharyya, D. Enhancing identity and access management using hyperledger fabric and oauth 2.0: A block-chain-based approach for security and scalability for healthcare industry. *Internet Things Cyber-Phys. Syst.* **2024**, *4*, 49–67. [CrossRef]

54. Kalapaaking, A.P.; Khalil, I.; Yi, X.; Lam, K.Y.; Huang, G.B.; Wang, N. Auditable and verifiable federated learning based on blockchain-enabled decentralization. *IEEE Trans. Neural Netw. Learn. Syst.* **2024**, *36*, 102–115. [CrossRef] [PubMed]
55. Can, O.; Dag, T.; Kantarcioglu, M. A blockchain based hybrid architecture for auditable consent management. *IEEE Access* **2024**, *12*, 100419–100445. [CrossRef]
56. Guggenberger, T.; Sedlmeir, J.; Fridgen, G.; Luckow, A. An in-depth investigation of the performance characteristics of Hyperledger Fabric. *Comput. Ind. Eng.* **2022**, *173*, 108716. [CrossRef]
57. Gorenflo, C.; Lee, S.; Golab, L.; Keshav, S. FastFabric: Scaling hyperledger fabric to 20 000 transactions per second. *Int. J. Netw. Manag.* **2020**, *30*, e2099. [CrossRef]
58. Tanana, D. Avalanche blockchain protocol for distributed computing security. In *Proceedings of the 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*; IEEE: Piscataway, NJ, USA, 2019; pp. 1–3.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.