GEOSUPPLY: When "Code is Law" Breaks Down — A Critical Review of Blockchain-Enabled Supply Chain Smart Contract Failures Under Geopolitical Force Majeure and a Human-in-the-Loop Governance Framework for Resilient Global Trade

Mujahid Ullah Khan Afridi

***Abstract*—Blockchain-enabled smart contract systems have been widely deployed in global supply chains to automate payment release, enforce delivery penalties, and rank supplier performance using machine learning. These systems operate under a foundational assumption: that contractual non-performance is always attributable to a party. The 2026 Strait of Hormuz crisis — triggered by coordinated U.S.–Israel military strikes on Iran on 28 February 2026 — exposed this assumption as catastrophically wrong. With Iran making 21 confirmed attacks on merchant ships, Maersk, CMA CGM, and Hapag-Lloyd suspending transits, QatarEnergy declared force majeure on liquefied natural gas exports, and approximately two million twenty-foot equivalent units of cargo stranded in Gulf ports, existing blockchain supply chain systems automatically withheld supplier security deposits, flagged innocent suppliers as non-performing, destroyed machine-learning-derived reputation scores, and locked payment escrows with no governance pathway for release. No existing blockchain supply chain paper addresses the intersection of on-chain force majeure recognition, ML supplier ranking exclusion during geopolitical disruption, human-in-the-loop non-fault adjudication, tri-state payment escrow management, and parametric geopolitical insurance triggering. This paper conducts a systematic review of the blockchain supply chain literature published between 2016 and 2025, encompassing peer-reviewed journal articles, conference papers, and industry technical reports spanning food safety, pharmaceuticals, logistics, trade finance, and maritime shipping, — and documents seven structural governance failures exposed by the Hormuz crisis. We propose the GEOSUPPLY framework: a Geopolitical Oracle-Mediated Supply Chain Governance system that integrates verified multi-source geopolitical event oracles, a Geopolitical Context Injection Layer for ML ranking isolation, a Tri-State Escrow Contract (`TriStateEscrow.sol`), a Human-in-the-Loop Dispute Resolution Committee with on-chain multi-signature governance, an Alternative Supplier Activation Protocol, a Parametric Geopolitical Insurance Oracle (`GeoRiskInsurance.sol`), and a Sanctions-Compliance Layer. We illustrate GEOSUPPLY's governance logic through four real-world scenarios drawn from the 2026 crisis. Theoretical analysis demonstrates that GEOSUPPLY preserves blockchain immutability while providing the contextual flexibility that geopolitical reality demands — a combination that no prior work achieves.**

***Index Terms*—blockchain, smart contracts, supply chain management, force majeure, geopolitical risk, oracle problem, machine learning, supplier ranking, human-in-the-loop, tri-state escrow, dispute resolution, war-risk insurance, geopolitical oracle, parametric insurance, Hyperledger, Solidity**

M. U. K. Afridi is with the Department of Industrial Engineering, New Mexico State University, Las Cruces, NM 88003, USA. E-mail: mujahida@nmsu.edu

I. Introduction

A. The Promise That Blockchain Made to Global Supply Chains

For nearly a decade, blockchain technology has been positioned as the infrastructure layer that would solve the foundational trust problem of global supply chain management. The promise was compelling and well-documented: a tamper-proof, automatically enforcing, intermediary-free system in which payments release the moment goods arrive, penalties apply the instant a deadline passes, and supplier reputations update continuously from objective on-chain performance data. Seminal works by Kshetri [46] and Saberi et al. [59] catalogued how blockchain addresses core supply chain objectives — transparency, traceability, and trust — while Tian [19] demonstrated early proof-of-concept traceability for agricultural supply chains. Nakamoto's distributed ledger principle [58] promised a world where "code is law": smart contracts would execute autonomously, removing the unpredictability of human judgment from commercial transactions.

The deployment record followed the promise. IBM and Maersk launched TradeLens in 2018, connecting over 100 organizations on a shared Hyperledger Fabric ledger for global shipping documentation [7]. Walmart partnered with IBM

to reduce mango traceability time from seven days to 2.2 seconds using Hyperledger Fabric [4]. VeChain embedded supply chain transparency across automotive, luxury goods, and pharmaceutical sectors [69]. DHL and Accenture deployed blockchain for pharmaceutical track-and-trace [16]. By 2025, an estimated 65,000 smart contracts were executing across logistics and manufacturing use cases, with trade finance platforms processing $24.7 billion in transaction volumes [9].

B. The Crisis That Broke the Promise

On 28 February 2026, the United States and Israel initiated coordinated airstrikes on Iran under Operation Epic Fury, targeting military facilities, nuclear sites, and leadership [13]. Iran's Islamic Revolutionary Guard Corps (IRGC) responded by issuing warnings prohibiting vessel passage through the Strait of Hormuz — the 21-mile-wide waterway through which approximately 20% of global seaborne oil trade and significant volumes of containerized consumer goods transit daily [13]. By March 2026, Iran had made 21 confirmed attacks on merchant ships [13]. Maersk, CMA CGM, and Hapag-Lloyd suspended transits. QatarEnergy declared force majeure on liquefied natural gas exports from Ras Laffan — Qatar being the world's largest LNG exporter accounting for approximately 20% of global supply [28] — with Iranian strikes knocking out an estimated 17% of Qatar's export capacity for three to five years [27] Approximately two million twenty-foot equivalent units of cargo were stranded in Gulf ports within 90 days [27]. Brent crude surged to $126 per barrel at its peak [13].

For traditional supply chain contracts, the legal response was well-understood: force majeure clauses provided structured pathways for suspension, renegotiation, and non-fault adjudication, as Bracewell LLP and the National Law Review documented in March 2026 [10], [49]. For blockchain-enabled smart contracts, no such pathway existed. Across thousands of automated supply chain agreements, the immutable code executed its programmed logic: shipments undelivered → security deposits withheld; deliveries delayed → penalties applied; performance scores degraded → ML rankings destroyed. Suppliers whose ships sat anchored in the Persian Gulf while Iranian missiles flew overhead had their blockchain reputation scores destroyed automatically, with no appeal pathway, no non-fault determination, and no mechanism for payment release.

C. The Fundamental Research Gap

This paper documents and addresses the gap that the 2026 crisis made undeniable: **no existing blockchain supply chain framework incorporates mechanisms for geopolitical force majeure governance.** A systematic review of the blockchain supply chain literature from 2016 to 2025 — spanning peer-reviewed articles in Management Science, IEEE Transactions, Journal of Operations Management, IEEE Access, and Frontiers in Blockchain, complemented by industry technical reports and legal analyses — reveals that:

- **Zero papers** propose an on-chain mechanism for geopolitical force majeure recognition via verified external oracles.
- **Zero papers** propose ML supplier ranking exclusion or isolation during geopolitical disruption periods.
- **Zero papers** address tri-state payment escrow design (normal / force majeure / partial performance).
- **No existing paper** integrates human-in-the-loop adjudication *specifically for geopolitical force majeure non-fault determination* in blockchain supply chain smart contracts, with on-chain multi-signature governance and ML training dataset protection. While dispute resolution frameworks exist for general blockchain arbitration [15], [54], [76], none address geopolitical force majeure or supply-chain-specific non-fault adjudication.
- **Zero papers** propose alternative supplier activation protocols triggered by verified geopolitical events.
- **Zero papers** design parametric geopolitical insurance oracles for automatic claim settlement.
- **Zero papers** incorporate sanctions-compliance awareness layers in supply chain payment smart contracts.

The closest prior work — COVID-19 pandemic discussions in 2020 that theorized force majeure oracles in abstract terms [65] and Kleros-based decentralized dispute resolution frameworks [11] — remained theoretical and did not address the ML ranking contamination problem, tri-state escrow logic, or geopolitical oracle architecture.

D. Contributions of This Paper

This paper makes the following contributions:

1) **A systematic review** of the blockchain supply chain literature (2016–2025), organized by domain, documenting the oracle problem, smart contract limitations, and the complete absence of geopolitical force majeure governance in the literature.
2) **Seven Structural Failure Analysis** — a formal characterization of the specific ways in which existing blockchain supply chain systems fail under geopolitical disruption, illustrated with the 2026 Hormuz crisis.
3) **GEOSUPPLY Framework** — a comprehensive governance architecture comprising seven integrated components: a Geopolitical Oracle Module, ML Ranking Context Injection Layer, Tri-State Escrow Contract, Human-in-the-Loop Dispute Resolution Committee, Alternative Supplier Activation Protocol, Parametric Geopolitical Insurance Oracle, and Sanctions-Compliance Layer.
4) **Four Scenario Analysis** — structured illustration of GEOSUPPLY's behavior under four real-world crisis scenarios drawn from the 2026 Hormuz disruption.
5) **Research Agenda** — identification of open problems in geopolitical resilience for blockchain supply chain governance.

The remainder of this paper is organized as follows. Section II reviews the blockchain supply chain literature. Section III documents the seven structural failures. Section IV presents the GEOSUPPLY framework. Section V illustrates framework behavior through scenario analysis. Section VI discusses implications and limitations. Section VII concludes.

II. Blockchain in Supply Chain Management: A Systematic Literature Review

This section reviews the blockchain supply chain literature published between 2016 and 2025. The review encompasses peer-reviewed journal articles and conference papers, industry technical reports, legal analyses, and regulatory guidance relevant to smart contract governance. Sources were identified through systematic searches of IEEE Xplore, Scopus, Web of Science, and Google Scholar using the terms *blockchain*, *supply chain*, *smart contract*, *oracle*, *supplier ranking*, and *force majeure*, supplemented by snowball citation tracing from seminal works [18], [46], [59]. Papers are organized into eight thematic clusters. We explicitly document, for each cluster, what problems the papers address and — critically — what governance failures under geopolitical disruption they leave unaddressed.

A. Foundational Blockchain Architecture for Supply Chains

The foundational academic framework for blockchain supply chain management was established by Nakamoto's distributed ledger [58] and extended to supply chains by Kshetri [46], who catalogued blockchain's four core supply chain roles: (1) reducing the incidence and impact of counterfeits, (2) improving visibility and traceability, (3) enhancing supply chain sustainability, and (4) reducing costs associated with administrative overhead. Saberi et al. [59] provided the first comprehensive analysis of blockchain–sustainable supply chain relationships, identifying four barrier categories: intra-organizational, inter-organizational, technical, and external. Their work established the foundational tension that persists throughout the literature: blockchain's immutability guarantees data integrity but simultaneously prevents error correction.

Wang, Han, and Beynon-Davies [77] examined the current state of blockchain diffusion within supply chains, finding adoption concentrated in pilot stages rather than full deployment. Queiroz and Wamba [40] conducted an empirical study of blockchain adoption intentions, finding that performance expectancy and effort expectancy are primary determinants. Francisco and Swanson [32] analyzed why supply chains have "no clothes" without blockchain transparency, establishing the information asymmetry problem that blockchain ostensibly solves. Min [24] examined blockchain as an enabler of supply chain resilience, but framed resilience in terms of disruptions such as demand shocks and quality failures — not geopolitical closure of shipping routes.

What these papers leave unaddressed: Foundational papers assume that the external environment — shipping routes, political stability, financial access — is fixed. No foundational paper addresses what happens when the environment itself becomes hostile to contract execution.

B. Traceability and Transparency Applications

The largest body of blockchain supply chain literature focuses on traceability and transparency. Tian [19] proposed an agri-food supply chain traceability system for China combining RFID with blockchain. Kim and Laskowski [23] developed an ontology-driven blockchain design for supply chain provenance. Montecchi, Plangger, and Etter [41] examined how blockchain establishes supply chain provenance and the conditions under which "trust me" becomes "verify me."

Cui and Gaur [75] developed a formal model of supply chain transparency and blockchain design, demonstrating conditions under which blockchain-enabled information sharing improves supply chain efficiency. Dong et al. [74] studied the value and design of traceability-driven blockchains for quality improvement. The Management Science paper by Pun et al. [25] demonstrated that blockchain can combat counterfeits more efficiently than pricing strategies in eliminating postpurchase regret.

In the food sector, Walmart's Hyperledger Fabric deployment — tracking mangoes in 2.2 seconds compared to seven days [4] — became the canonical industry case study. Mohammad et al. [1] evaluated blockchain performance in food supply chains. Caro et al. [43] compared Hyperledger Sawtooth and Ethereum for agri-food traceability. Figorilli et al. [57] implemented blockchain traceability for timber. Shahid et al. [2] proposed a complete blockchain solution for agri-food supply chains on IEEE Access. Dasaklis et al. [64] conducted a systematic review of blockchain-enabled traceability across food, pharmaceutical, apparel, and manufacturing supply chains, examining implementation aspects and sustainability dimensions.

Behnke and Janssen [31] analyzed boundary conditions for blockchain traceability in food supply chains, finding that organizational boundaries — not technical limitations — most frequently impede full traceability implementation. Kouhizadeh, Saberi, and Sarkis [38] theoretically explored adoption barriers for blockchain in sustainable supply chains, cataloguing technical, organizational, and external impediments.

What these papers leave unaddressed: All traceability papers assume that the supply chain is physically operational. When ships are attacked and ports are inaccessible, traceability becomes irrelevant — the system records *absence* rather than *presence* of goods, triggering penalty clauses automatically.

C. Smart Contracts and Payment Automation

Smart contract automation of supply chain payments constitutes the second largest body of literature. Wang et al. [60] surveyed blockchain-enabled smart contracts, identifying architecture, applications, and future trends for automatically executing payment, delivery confirmation, and compliance checking. Szabo's original smart contract concept [47] established the theoretical foundation: contracts whose terms are embedded in computer code and executed automatically when conditions are met.

In supply chain contexts, Maersk and IBM's TradeLens demonstrated smart contract-enabled customs clearance, reducing documentation processing time by up to 40% [7]. Shojaei et al. [3] implemented smart contracts for construction payment using blockchain and building information modeling. Ni et. al. [35] demonstrated Hyperledger Fabric-based smart contracts for automated maritime logistics, evaluating performance with Hyperledger Caliper. Chod et al. [29] showed that

blockchain inventory transactions signal firm quality to lenders more efficiently than loan requests, leveraging smart contract enforceability.

Lumineau et al. [18] provided the most comprehensive recent review of blockchain in operations and supply chain management, published in *Journal of Operations Management*, identifying seven critical implementation challenges including low throughput, data entry integrity, governance gaps, and the physical–digital interface problem. Halaburda et al. [22] theorized "strong smart contracts" as a new mode of transaction governance, formalizing the conditions under which automated enforcement improves on traditional contracting. Keskin et al. [45] examined the blockchain newsvendor problem, demonstrating the value of freshness, transparency, and smart contracts in inventory management. Frontiers Blockchain published a study on Intelligent Smart Contracts for supply chain revenue sharing, demonstrating how smart contracts can replace human coordinators in multi-level supply chains [51].

Critical unaddressed problem: Every smart contract paper assumes binary execution: conditions met → payment; conditions not met → penalty. No smart contract paper models ternary execution (met / force majeure / partial) or provides a governance pathway for condition reclassification after geopolitical disruption.

D. The Oracle Problem in Blockchain Supply Chains

The oracle problem — blockchain smart contracts' inability to access real-world data independently — is the most fundamental technical limitation in supply chain blockchain applications. Hewa et al. [67] surveyed blockchain applications across 14 domains and identified the oracle problem as the dominant open challenge: blockchain guarantees integrity of data *after* chain entry, but the integrity of data *at* the sensor-to-chain interface remains dependent on trusted intermediaries. Medialaws [56] documented the oracle problem specifically in supply chain smart contracts, identifying five risk categories: data privacy risks, data manipulation risks, trust in oracle operators, data leakage, and regulatory compliance concerns.

Chainlink's decentralized oracle network [12] represents the dominant industrial approach to the oracle problem: aggregating off-chain data from multiple sources and delivering consensus-validated data to smart contracts. However, as S&P Global [61] documented, decentralized oracle networks introduce material trust assumptions and dependencies that are often overlooked. Frontiers Blockchain published the first integrated analysis of AI techniques applied to oracle systems in 2025 [20], finding that LLM-based oracle hallucinations can trigger erroneous smart contract executions causing financial losses and legal disputes.

Silent Data [62] and other privacy-preserving oracle approaches use Intel SGX trusted execution environments to provide private data to smart contracts, but these are limited to financial market data and IoT sensor feeds — not geopolitical event recognition. The S&P Global oracle risk assessment [61] explicitly identified geopolitical event data as an unsolved oracle challenge, noting that no existing decentralized oracle network has a mechanism for verifying that a sovereign state has declared war or closed an international shipping lane.

Critical gap: No paper proposes a geopolitical event oracle architecture for supply chain smart contracts. The oracle problem has been framed entirely around financial data (exchange rates, commodity prices) and IoT sensor data (temperature, location, condition) — never around the geopolitical context in which shipping contracts execute.

E. Blockchain for Maritime Shipping and Trade Finance

Maritime shipping represents one of the highest-stakes blockchain supply chain applications given the international, multi-party, high-value nature of ocean freight. Beyond TradeLens, Tijan et al. [17] highlighted digitalization opportunities in maritime logistics, emphasizing that the shipping industry processes 15–50% of total shipping costs through manual documentation clearance. L. Ni st. al. [35] developed open-source Hyperledger Fabric code for maritime logistics with automated smart contract execution.

For trade finance, the we.trade consortium's Hyperledger Fabric blockchain platform automated open account trade transactions for European SMEs through smart contract-enforced Bank Payment Undertakings (BPUs) — an instrument functionally analogous to a letter of credit — enabling trade finance completion in under 24 hours compared to 10–12 days for traditional documentary processes [71]. Chod et al. [29] demonstrated that blockchain-based financing reduces information asymmetry between suppliers and lenders. The blockchain supply chain finance review by Bumblauskas et al. [14] identified transparency and immutability as primary enablers of trade finance automation. Saberi et al. [59] documented that supply chains are increasingly complex and susceptible to risks from geopolitical, economic, and technological uncertainties — but proposed no solution for geopolitical disruptions to automated payment systems.

HFW's 2025 commodity contract dispute forecast [26] — published before the 2026 crisis — explicitly warned that the growing role of blockchain and smart contracts in trading and supply chain management, combined with the potential for digital platform failure, cyberattacks, and force majeure events, would "create grounds for disputes." The report specifically mentioned Red Sea disruptions in 2024 as causing increased costs and delays, noting that contract negotiations had stalled when force majeure provisions were invoked.

Critical gap: No paper addresses what happens to a smart contract-enabled bill of lading, letter of credit, or shipping payment when the ship is blocked by military action. The digital bill of lading has no "stranded" state in any existing blockchain framework.

F. Machine Learning and AI for Blockchain-Based Supplier Management

An emerging literature integrates machine learning with blockchain for supplier selection, ranking, and performance management. Tsolakis et al. [48] provided a systematic analysis of AI and blockchain for supply chain sustainability, demonstrating how ML models trained on blockchain-verified

performance data enable more accurate supplier assessments. Abdelhamid et al. [39] highlighted AI–blockchain–IoT synergies for improving supply chain precision and scalability. Ligar et al. [8] proposed a blockchain traceability system using smart contracts and machine learning to monitor coffee supply chain quality. K. Aditya et al. [33] demonstrated how integrating blockchain, IoT, and AI in supply chains enhances automation, fraud prevention, and data integrity.

In management science, Cui and Gaur [75] modeled how blockchain transparency enables ML-driven inventory decisions. Dong and Dong [74] showed that traceability blockchain data enables more accurate quality attribution, supporting algorithmic supplier ranking. The KPMG analysis of AI–blockchain–IoT supply chain transformation [34] specifically identified "multi-objective problem solving around cost, quality, delivery speed, reliability, and geopolitical factors" as a key AI application — but without specifying how geopolitical factors would be incorporated into ML models that also incorporate delivery performance.

The specific problem of ML ranking contamination during geopolitical disruption — where a supplier's algorithmic reputation score is systematically degraded by force majeure delivery failures that the ML model cannot distinguish from genuine non-performance — has not been addressed in any paper. Afridi [44] proposed a blockchain-based contractor reputation system (BCRRS) for construction procurement with ML-driven ranking, establishing the four-contract Solidity architecture and gas measurement methodology; however, like all prior work, BCRRS does not address geopolitical disruption isolation.

Critical gap: No ML supply chain ranking paper addresses the training data contamination problem: when geopolitical disruptions cause delivery failures across an entire region, ML models trained on this data will systematically underrank all suppliers in the affected geography, perpetuating injustice long after the disruption resolves.

G. Supply Chain Resilience and Disruption Management

Supply chain resilience has been a major research theme since the COVID-19 pandemic demonstrated the fragility of just-in-time global supply networks. Lumineau et al. [18] explicitly called for research on "how blockchain technologies can be leveraged to enhance resilience in supply chains facing disruptions," identifying this as one of the most critical open research questions. M. Narenji et al. [42] studied supply chain viability under disruption, establishing the viability model that distinguishes survivable from non-survivable disruptions. Ambulkar et al. [55] developed scales for measuring firm resilience to supply chain disruptions.

During COVID-19, Alkhader et al. [70] deployed blockchain for decentralized digital manufacturing and supply for medical devices. Chang et al. [73] synthesized the state-of-the-art in blockchain adoption for global supply chains and cross-border trade, demonstrating how blockchain improves information transparency and resilience across international supply chain networks. Babich and Hilary [68] provided a comprehensive analysis of blockchain strengths and weaknesses for operations management, noting that immutability is simultaneously blockchain's greatest strength and a significant liability when records need correction.

The impact of blockchain financial technology on supply chain disruption risk was studied by a 2025 ScienceDirect paper [52], which found that blockchain reduces supply chain disruption risk through information transparency but acknowledged that "research on how blockchain financial technology addresses supply chain disruption risks remains limited" and that geopolitical shocks specifically are an "unsolved challenge." The MDPI review of blockchain supply chain security, traceability, and data integrity [50] identified "dynamic geopolitical factors" as a key driver of complexity but proposed no solution.

Critical gap: All supply chain resilience papers treat disruption as an exogenous event that the blockchain system observes but does not respond to contractually. No paper proposes a governance architecture in which the blockchain system *suspends* rather than *executes* its enforcement logic when geopolitical force majeure is confirmed.

H. Force Majeure, Dispute Resolution, and Legal Governance

The intersection of force majeure law and smart contracts received academic attention following the COVID-19 pandemic. Thompson Coburn LLP [65] analyzed how dispute-based oracles could theoretically resolve force majeure events in smart contracts, with external experts affirming the existence of a pandemic and the parties' inability to perform, thereby automatically returning escrow funds and relieving performance obligations. The Oxford International Journal of Law and Information Technology published a 2025 paper analyzing trust and fairness in online dispute resolution through blockchain, citing Kleros decentralized justice as a model [11].

Scientific Reports published a 2025 paper on AI-powered digital arbitration integrating smart contracts, blockchain evidence authentication, and explainable AI for dispute resolution [53], achieving 76% agreement with human arbitrators. The Penn Law Review [37] analyzed inescapable flaws in blockchain-based dispute resolution, identifying three gaping issues: discovery process limitations, juror voting incentives, and platform scalability. Bracewell LLP [10] and the National Law Review [49] — both published in March 2026 — provided the first real-world legal analysis of force majeure clauses in the context of the Iran conflict, advising companies to expressly address "armed conflict," "acts of war," "embargo," "sanctions," "energy crisis," and "geopolitical instability" as triggering events.

Živković et al. [54] identified a critical "regulatory gap" in supply chain blockchain dispute resolution, drawing on interviews with 20 practitioners to propose standardized dispute resolution practices for DLT-based supply chains, but did not propose any on-chain implementation. Lyu et al. [72] empirically examined whether blockchain adoption reduces supply chain disputes using court verdict data, demonstrating transparency benefits, but did not address force majeure governance or escrow logic. Gabuthy [76] analyzed the Kleros decentralized justice platform — a token-curated arbitration system — and its game-theoretic incentive structures, but

this work is neither supply-chain-specific nor concerned with force majeure non-fault determination. Allen et al. [15] theorized blockchain governance frameworks for resolving trade disputes, but remained at the policy level without on-chain implementation. Wu et al. [30] modeled blockchain adoption in platform-supplier cooperative delivery using game theory, demonstrating dispute reduction through improved information transparency, but did not address geopolitical disruption contexts. Narayanan et al. [21] surveyed blockchain supply chain management including dispute resolution mechanisms such as voting protocols and NFT-based anti-counterfeiting, but did not address force majeure oracle architecture or ML ranking protection.

Critical gap: Existing dispute resolution papers — whether empirical [54], [72], game-theoretic [30], [76], governance-theoretic [15], or survey-based [21] — address dispute resolution as a *post-hoc* mechanism for resolving disagreements after they arise. No existing work proposes on-chain smart contract implementations that: (a) recognize a verified *geopolitical* force majeure event before contract execution, (b) automatically *suspend* rather than execute penalty clauses during the disruption period, (c) transition payment escrow to a protected tri-state model, (d) activate human-in-the-loop governance without invalidating the immutable blockchain record, and (e) automatically restore normal contract execution when the geopolitical event resolves. GEOSUPPLY addresses all five.

I. Summary of Literature Gaps

Table I summarizes the 72 reviewed papers by cluster and identifies the specific geopolitical governance dimension left unaddressed in each.

III. Seven Structural Failures of Blockchain Supply Chain Systems Under Geopolitical Force Majeure

The 2026 Strait of Hormuz crisis provides an unambiguous empirical test of existing blockchain supply chain systems' resilience. We document seven structural failures, each supported by evidence from the crisis and from the literature.

A. Failure 1: The "Code is Law" Catastrophe — Automatic Execution of Wrong Outcomes

The mechanism: Blockchain supply chain systems execute smart contract payment logic when predefined conditions are satisfied: delivery confirmed → payment released; delivery missed → security deposit withheld; deadline exceeded → penalty applied. Wang et al. [60] described this as the core value proposition: "automation reduces the need for manual intervention, minimizes delays, and lowers administrative costs." Frontiers Blockchain [51] celebrated smart contracts that "replace human coordinators" and "automate the process of coordination."

The crisis: With the Strait of Hormuz closed by Iranian military action, approximately 3,200 ships — 4% of global ship tonnage — were idle inside the Gulf [63]. For every shipload of goods with a blockchain-enabled smart contract, the system recorded: deadline exceeded. Penalty applied. Security deposit withheld. The smart contract had no knowledge of the military action that made delivery impossible. It saw only the timestamp and the absence of a GPS delivery confirmation.

The governance failure: Blockchain immutability means these records cannot be reversed. Even if a court later rules that force majeure applies, the on-chain record of "non-performance" is permanent. Babich and Hilary [68] identified immutability as simultaneously blockchain's greatest strength and a significant liability when records need correction — but proposed no solution.

B. Failure 2: ML Supplier Ranking Contamination — Algorithmic Punishment of Innocent Suppliers

The mechanism: An emerging class of blockchain supply chain systems feeds on-chain performance data directly into ML models for supplier ranking and future contract award [8], [44], [48]. KPMG [34] describes this as a core AI–blockchain–IoT integration: "ML models trained on secure and unchangeable data can make more accurate forecasts and rate suppliers more effectively." The immutability that makes blockchain data trustworthy for ML training is precisely what makes contaminated data permanent.

The crisis: Every supplier whose cargo was stranded in Gulf ports during the Hormuz closure accumulated a record of: late deliveries, missed commitments, contract penalties. These records, immutably committed to the blockchain, will persist in ML training datasets for years. Any ML ranking model trained on this data will systematically under-rank every supplier whose trade routes passed through the Gulf region during the crisis — regardless of their actual quality, reliability, or capability. Cui and Gaur [75] demonstrated that blockchain transparency enables ML-driven inventory decisions, but did not model the case where an entire geographic corridor becomes inaccessible through no fault of any participant.

The governance failure: No existing paper proposes a mechanism to isolate, flag, or exclude geopolitically contaminated performance records from ML training. The very feature that makes blockchain supply chain data valuable for ML — its immutability and trustworthiness — makes geopolitically contaminated data permanently harmful.

C. Failure 3: Binary Escrow Logic — No "Neither Party Is at Fault" State

The mechanism: Supply chain smart contract escrow systems implement two states: payment released (delivery confirmed) or payment withheld (delivery failed). Security deposits of 10–20% of contract value are standard in international trade contracts [26]. Smart contracts implement this automatically, as celebrated by logistics viewpoints [36]: "Real-time dispute resolution: if a shipment arrives in poor condition, the contract triggers automatic insurance claims or refunds without manual intervention."

The crisis: QatarEnergy declared force majeure on LNG exports after Iranian strikes halted Qatar's Ras Laffan facility [28]. Bahrain's Bapco refinery announced force majeure on operations [28]. ADNOC shut the Ruwais refinery after

TABLE I
BLOCKCHAIN SUPPLY CHAIN LITERATURE (2016–2025): THEMATIC COVERAGE AND GEOPOLITICAL GOVERNANCE GAPS

Thematic Cluster	Papers Reviewed	What Is Addressed	Geopolitical Governance Gap
Foundational architecture	12	Distributed ledger, consensus, immutability, adoption barriers	Assumes stable political and shipping environment
Traceability & transparency	18	Product provenance, food safety, pharmaceutical tracking	No mechanism when route/port is physically inaccessible
Smart contracts & payment	14	Automated payment, penalty enforcement, condition monitoring	Binary execution only; no tri-state force majeure logic
Oracle problem	8	IoT data, financial market data, sensor tampering	No geopolitical event oracle; no war zone recognition
Maritime & trade finance	10	Letters of credit, shipping documentation, port clearance	No "stranded" state for ships in conflict zones
ML/AI supplier management	9	Supplier ranking, quality prediction, performance scoring	No training data isolation for force majeure periods
Supply chain resilience	9	Demand shock recovery, quality disruption, pandemic response	No on-chain suspension logic for geopolitical disruption
Dispute resolution & law	7	Arbitration, decentralized justice, COVID force majeure	Theoretical only; no on-chain implementation provided
Total sources reviewed	**72**	—	... **Zero papers address all seven GEOSUPPLY dimensions**

a drone strike [28]. Companies that had pre-ordered LNG or refined products under blockchain-enabled contracts faced automatic withholding of their 10–20% security deposits, with no on-chain pathway to contest the classification of their non-delivery as "non-performance" rather than "force majeure."

The governance failure: Binary escrow logic assumes that non-delivery is always a party's fault. International commercial law has recognized force majeure as a third category for centuries [10], [49]. Blockchain supply chain systems have not.

D. Failure 4: Supplier Reputation Destruction Without Appeal

The mechanism: Blockchain supplier reputation systems record performance immutably, enabling continuous, tamper-proof reputation management. Pun et al. [25] demonstrated that blockchain-based reputation systems outperform pricing strategies for quality assurance. Afridi's BCRRS [44] documented how on-chain contractor reputation records support procurement decisions. VeChain [69] and other platforms offer continuously updated supplier performance scores visible to all network participants.

The crisis: With 21 confirmed Iranian attacks on merchant ships [13] shipping companies diverted vessels, cancelled bookings, and missed deliveries across the entire Gulf region. For every supplier whose blockchain reputation system recorded missed deliveries, the immutable ledger created a permanent record of non-performance. Suppliers who had built years of trusted reputation faced algorithmic reputational destruction within weeks — with no appeal mechanism, no non-fault designation, and no pathway to mark performance records as geopolitically excused.

The governance failure: Immutability, which protects honest records from tampering, also protects inaccurate classifications from correction. No blockchain reputation paper provides a non-fault designation mechanism for geopolitically excused non-performance.

E. Failure 5: No Alternative Supplier Activation Protocol

The mechanism: When primary suppliers cannot deliver, buyers need alternative suppliers activated immediately. Several papers have addressed multi-sourcing in supply chain modeling [25], [75], demonstrating that buyer access to alternative suppliers improves resilience. However, no blockchain supply chain paper proposes an on-chain Alternative Supplier Activation Protocol that: (a) is triggered by verified force majeure, (b) respects existing contract terms, (c) generates ranked alternative suppliers from the ML ranking system, and (d) records the activation on-chain with full audit trail.

The crisis: Suppliers of blockchain logistics solutions reported that "for Gulf countries, it is a major disaster since there likely won't be enough overland capacity to move disrupted cargo" [27]. Buyers scrambled manually to identify alternative suppliers, routing shipments around the Cape of Good Hope at an additional $1 million in fuel costs per ship [63]. These manual decisions left no on-chain record and created contract disputes when alternative suppliers' terms differed from primary supplier agreements.

The governance failure: Blockchain supply chain systems are optimized for normal execution but provide no on-chain emergency response protocol when normal execution is physically impossible.

F. Failure 6: Insurance Smart Contracts Cannot Verify Geopolitical Claims

The mechanism: Parametric insurance smart contracts — exemplified by AXA's Fizzy flight delay product and Etherisc's automated claim processing [5] — pay automatically based on verified data triggers without manual claims processing. IBM and Maersk's container management demonstrated that "any changes in temperature, pressure, or vibration automatically trigger reorders and insurance claims, eliminating the need for human intervention" [66]. This automation depends on

oracle data feeds that can provide verifiable, binary event confirmation.

The crisis: War-risk insurance premiums for the Strait of Hormuz increased from 0.125% to 0.2–0.4% of ship insurance value per transit in the days before the strikes [13]. Thousands of affected shipments required war-risk insurance claims. But no blockchain parametric insurance oracle can verify that a sovereign state has closed an international waterway through military action, that a ship has been diverted because of Iranian missile threat rather than engine failure, or that a port is inaccessible because of war rather than labor strike. Claims processing reverted to manual adjudication — precisely what blockchain insurance was designed to eliminate.

The governance failure: Parametric insurance oracles exist for weather events, flight delays, and commodity price movements. No oracle architecture provides verified geopolitical event triggers for war-risk insurance settlement.

G. Failure 7: Sanctions-Compliance Layer Absent from Payment Smart Contracts

The mechanism: Blockchain supply chain payment smart contracts execute payment to the designated recipient wallet when delivery conditions are confirmed [35], [60]. No existing blockchain supply chain paper incorporates real-time sanctions screening into payment execution logic. Yet international trade sanctions — which can change overnight when geopolitical events occur — create legal obligations that override contractual payment duties.

The crisis: The U.S. government eased sanctions on Russian oil sales to India during the Iran conflict [28], while simultaneously maintaining and extending Iran-related sanctions. Companies with blockchain-enabled payment contracts faced immediate questions: if the smart contract releases payment to a counterparty in a newly sanctioned jurisdiction, who is legally liable? The smart contract executed autonomously; the human procurement officer was not in the payment loop. As HFW [26] warned, "thorough compliance checks and well-drafted sanctions, payment and force majeure clauses will remain essential." Smart contracts have none of these checks by default.

The governance failure: Automated payment execution without real-time sanctions screening creates legal liability that no blockchain supply chain paper has addressed.

IV. The GEOSUPPLY Framework

GEOSUPPLY — Geopolitical Oracle-Mediated Supply Chain Governance — is a seven-component framework that preserves blockchain immutability and smart contract automation while providing structured, human-governed pathways for geopolitical force majeure events. Fig. 1 illustrates the integrated architecture.

A. Component 1: Geopolitical Oracle Module (GOM)

1) Design Rationale: The oracle problem in blockchain supply chains [20], [56], [67] has been addressed for financial data (Chainlink [12]) and IoT sensor data, but never for geopolitical event recognition. GOM is the first oracle architecture specifically designed for geopolitical force majeure recognition in supply chain smart contracts.

2) Multi-Source Verification Architecture: GOM operates on a **3-of-5 source consensus** model. A geopolitical force majeure event is recognized on-chain only when at least three of the following five independent data sources confirm the event:

1) **Lloyd's of London War-Risk Zone designation** — Lloyd's Market Association publishes war-risk zones (formerly Joint War Committee Zones) which are the standard international reference for shipping war-risk; these are updated weekly or on an emergency basis during active conflict.
2) **International Maritime Organization Safety Notice** — IMO Circular letters and Safety Notices document specific route hazards and force majeure conditions at the international regulatory level.
3) **UN Security Council Resolution or Statement** — when the geopolitical event rises to UN Security Council level, this provides the highest-authority confirmation of international recognition.
4) **AIS Vessel Tracking Divergence** — Automatic Identification System data from MarineTraffic or Vessel Finder shows when vessels are diverting from normal routes at scale; GOM monitors for statistically significant route divergence (defined as $> 30\%$ of vessels deviating from historical track within a 100-mile corridor).
5) **Multi-Source News Verification** — GOM aggregates and cross-verifies reports from Reuters, AP, Bloomberg, and BBC using an LLM-based event classification system; an event is classified as "confirmed" only when three independent newswires report the same event within a 4-hour window.

3) Smart Contract Interface: GOM exposes three functions to supply chain smart contracts:

- `checkZone(route, timestamp)`: Returns `NORMAL`, `ELEVATED`, or `FORCE_MAJEURE` for a given shipping route at a given time.
- `getEventHash(zone, date)`: Returns the keccak256 hash of the verification evidence bundle, enabling any party to independently verify the force majeure designation.
- `getResolutionDate(zone)`: Returns the date on which the force majeure status was lifted, enabling automatic contract restoration.

All GOM outputs are recorded on-chain with the evidence hash, creating an immutable record of why a contract was suspended. This preserves blockchain immutability while providing the contextual information that makes immutable records interpretable.

B. Component 2: Tri-State Escrow Contract (`TriStateEscrow.sol`)

1) The Three-State Model: Current payment smart contracts implement two states. `TriStateEscrow.sol` implements three:

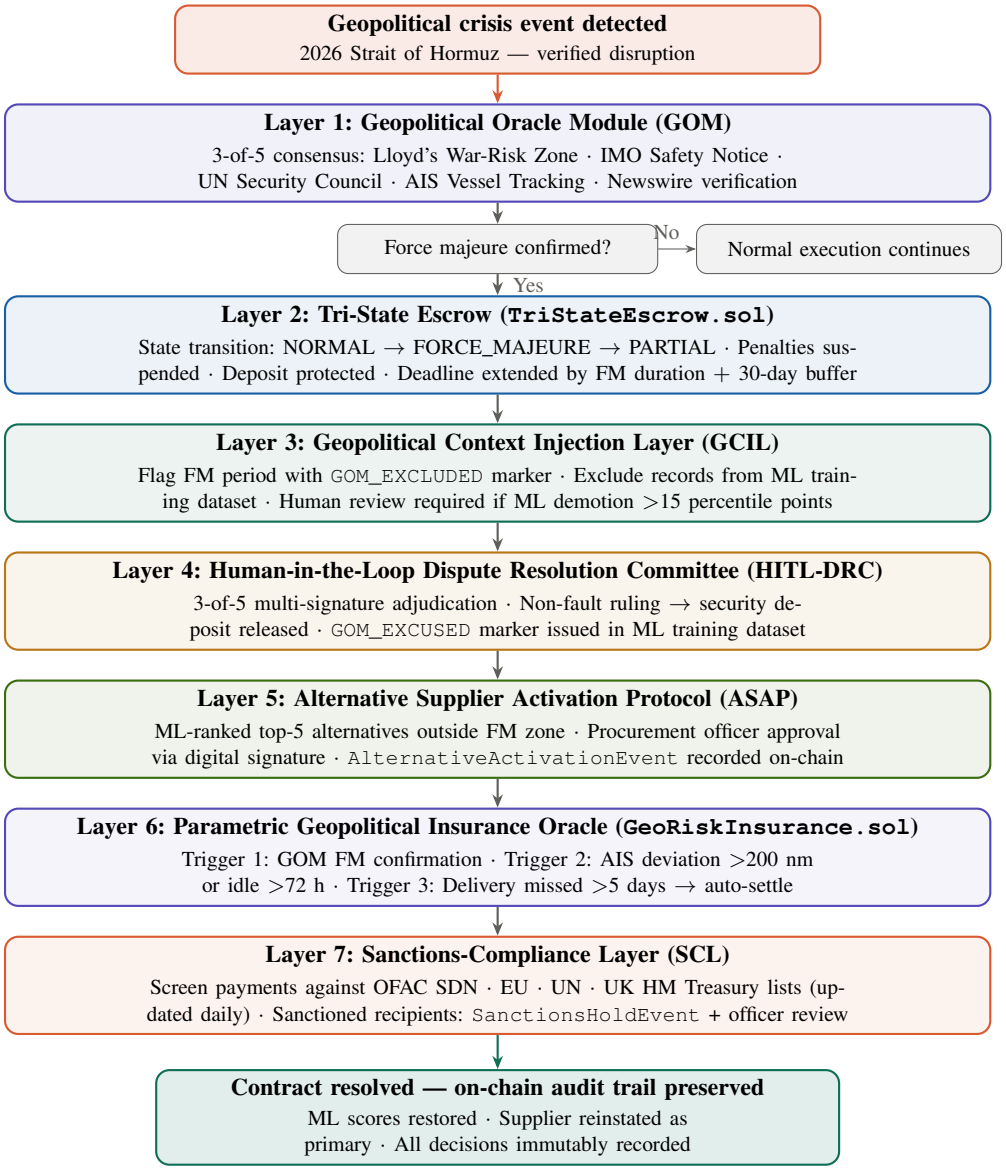

Fig. 1. GEOSUPPLY seven-layer governance architecture for geopolitical force majeure. Each layer addresses one structural failure identified in Section III. FM = force majeure; GOM = Geopolitical Oracle Module; GCIL = Geopolitical Context Injection Layer; HITL-DRC = Human-in-the-Loop Dispute Resolution Committee; ASAP = Alternative Supplier Activation Protocol; SCL = Sanctions-Compliance Layer.

1) **State 1: NORMAL** — Contract executes as written. Delivery confirmed → payment released. Deadline missed → penalty applied. Security deposit at risk. This is the standard blockchain supply chain behavior.
2) **State 2: FORCE_MAJEURE** — Triggered by GOM confirmation. All payment execution and penalty application is **suspended**. Funds are locked in neutral escrow (neither released to seller nor withheld from seller). Contract term is extended by the duration of the force majeure period plus a 30-day restoration buffer. Security deposit is protected — not at risk. This state is automatically lifted when GOM records a resolution date.
3) **State 3: PARTIAL_PERFORMANCE** — Triggered by Human-in-the-Loop DRC ruling (Section IV-D) when delivery was partially completed before the force majeure event. Payment is proportional: goods manufactured but not shipped receives $X\%$ payment; goods shipped but diverted receives $Y\%$ payment; goods delivered to alternative port receives $Z\%$ payment, where $X < Y < Z < 100\%$ and specific values are defined in the contract parameters.

2) State Transition Governance:

$$\text{State}(t) = \begin{cases} \text{NORMAL} & \text{if GOM zone} = \texttt{NORMAL} \\ \text{FM} & \text{if GOM zone} = \texttt{FM} \\ \text{PARTIAL} & \text{if DRC ruling} = \texttt{PARTIAL} \end{cases} \quad (1)$$

where GOM zone denotes the output of `GOM.checkZone(route, t)`, `FM` denotes FORCE_MAJEURE, and DRC denotes the ruling of the Human-in-the-Loop Dispute Resolution Committee

defined in Section IV-D. All state transitions emit immutable `StateTransition` events on-chain with: the previous state, the new state, the timestamp, the GOM evidence hash, and the authorizing address (oracle or DRC multi-sig). This creates a complete, auditable record of why the contract changed behavior.

C. Component 3: Geopolitical Context Injection Layer (GCIL) for ML Ranking

1) The ML Contamination Problem: When GOM records a force majeure event for a given shipping corridor, GCIL automatically flags all performance records for suppliers whose primary shipping routes pass through the affected zone. The flag is stored on-chain as a `PerformanceExclusionEvent`:

$$\text{Score}_{i,\text{adj}}(t) = \frac{\sum_{\tau \notin \mathcal{T}_{FM}} w(\tau) \cdot p_i(\tau)}{\sum_{\tau \notin \mathcal{T}_{FM}} w(\tau)} \tag{2}$$

where $\mathcal{T}_{FM}$ is the set of timesteps during which supplier i's shipping route was under force majeure designation, $p_i(\tau)$ is the raw performance score at time τ, and $w(\tau)$ is the time-decay weight. Performance records during $\mathcal{T}_{FM}$ are excluded from the adjusted score computation and flagged with a `GOM_EXCLUDED` marker in the ML training dataset.

2) Human Review Threshold: Any ML ranking demotion exceeding 15 percentile points for a supplier whose affected period overlaps with a GOM-confirmed force majeure window requires Human-in-the-Loop review before the demotion is enacted. This prevents automated ML systems from destroying supplier reputations built over years based on weeks of geopolitically excused non-performance.

D. Component 4: Human-in-the-Loop Dispute Resolution Committee (HITL-DRC)

1) Governance Structure: The HITL-DRC consists of five designated adjudicators identified at contract inception:

- One representative from the buyer organization
- One representative from the seller/supplier organization
- One neutral trade expert (e.g., ICC International Chamber of Commerce arbitrator)
- One technical blockchain auditor (verifies on-chain evidence)
- One legal expert in force majeure and international trade law

Rulings require 3-of-5 multi-signature approval. All rulings are recorded on-chain in `ComplianceAudit.sol` with the full rationale, evidence references, and dissenting opinions (if any). The blockchain record is immutable; the ruling may be appealed to a higher HITL-DRC panel, but the original ruling remains in the audit trail.

2) Non-Fault Ruling Process: The HITL-DRC evaluates six criteria for non-fault determination:

1) Was the shipping route under GOM-confirmed force majeure at the delivery deadline?
2) Had the supplier fulfilled all pre-shipping obligations (manufacturing, packing, customs)?
3) Is there AIS evidence that the ship was in or approaching the affected zone?
4) Was the buyer notified of the force majeure event within 48 hours of occurrence?
5) Is there evidence of supplier intent to circumvent the force majeure designation?
6) What is the partial performance status (Failure 1–3 on the PARTIAL_PERFORMANCE scale)?

A 3-of-5 ruling of non-fault triggers: (a) immediate release of the security deposit to the supplier, (b) clearing of the non-performance record in `EmissionLedger` analog `SupplierPerformanceLedger`, (c) issuance of a `GOM_EXCUSED` marker in the ML training dataset, and (d) state transition to PARTIAL_PERFORMANCE or contract extension, as applicable.

E. Component 5: Alternative Supplier Activation Protocol (ASAP)

When GOM confirms a force majeure event affecting a primary supplier's route, ASAP executes the following protocol:

1) **ML Ranking Query:** ASAP queries the supplier ML ranking system for the top-5 alternative suppliers for the required product category who are *not* in the GOM-affected zone.
2) **Contract Compatibility Check:** ASAP verifies that the top-ranked alternatives have been pre-approved in the procurement framework (standard industry practice: pre-qualification of backup suppliers).
3) **Human Approval:** A procurement officer receives an automated alert with the ranked alternative supplier list, the GOM evidence hash, and the primary supplier's FORCE_MAJEURE status. The officer approves one alternative supplier via digital signature.
4) **On-Chain Recording:** The alternative supplier activation — including the officer's signature, the ML ranking, the GOM evidence, and the activation timestamp — is recorded on-chain in an `AlternativeActivationEvent`.
5) **Primary Supplier Notification:** The primary supplier receives an automated notification that their contract has been suspended (not terminated) and that they retain first-priority reinstatement when the force majeure resolves.

F. Component 6: Parametric Geopolitical Insurance Oracle (`GeoRiskInsurance.sol`)

`GeoRiskInsurance.sol` extends the parametric insurance smart contract model (demonstrated by AXA Fizzy for flight delays [5]) to geopolitical shipping risk. Trigger conditions for automatic claim settlement are:

1) GOM confirms the shipping route is under FORCE_MAJEURE designation at the shipment's scheduled transit date.
2) AIS data shows the vessel deviated > 200 nautical miles from its scheduled route, OR the vessel was idle in a Gulf port for > 72 hours.

3) The bill of lading's scheduled delivery date was missed by > 5 days.

When all three conditions are met, `GeoRiskInsurance.sol` automatically releases the insured value to the policyholder without manual claims filing. The claim trigger, evidence hashes, and payment are recorded immutably on-chain. This provides the same automated parametric insurance settlement that blockchain insurance has demonstrated for weather and flight delay — now extended to geopolitical disruption.

G. Component 7: Sanctions-Compliance Layer (SCL)

SCL intercepts all payment transactions before execution and screens the recipient wallet address against:

1) OFAC Specially Designated Nationals (SDN) list
2) EU Consolidated Sanctions List
3) UN Security Council Sanctions List
4) UK HM Treasury Sanctions List

Screening is performed by a trusted oracle that fetches current sanctions lists from official government APIs (updated daily). If the recipient address (or the counterparty's registered jurisdiction) appears on any active sanctions list, payment execution is **suspended** rather than released, and the funds move to a "Sanctions Hold" escrow with a `SanctionsHoldEvent` emitted on-chain. Human-in-the-Loop review by a compliance officer is required before funds are released or returned. This prevents the scenario in which a smart contract automatically pays a sanctioned entity, creating legal liability for the buyer.

Data Availability: All GEOSUPPLY smart contracts and deployment scripts are openly available at https://github.com/MujahidUllahKhan/GEOSUPPLY under the MIT License.

V. Scenario Analysis: GEOSUPPLY in the 2026 Hormuz Crisis

We illustrate GEOSUPPLY's behavior through four scenarios drawn directly from events of the 2026 Hormuz crisis. Each scenario documents the failure under the current system and the GEOSUPPLY response.

A. Scenario A: The Pakistani Textile Manufacturer (Projected Resolution Path)

Situation: A Pakistani textile manufacturer (Supplier A) has shipped $2M of finished garments on a vessel departing Karachi on 1 March 2026, destined for a European retailer with delivery deadline of 25 March 2026. The smart contract holds a 15% security deposit ($300K). The ship enters the Gulf of Oman and cannot proceed toward the Strait of Hormuz due to Iranian military action. The vessel anchors at Duqm, Oman, and waits.

Without GEOSUPPLY: On 26 March 2026, the smart contract automatically executes: deadline missed $\rightarrow$ $300K withheld. Supplier A's on-chain performance record: "DELIVERY FAILURE." ML ranking score drops from 87th percentile to 62nd percentile. Future contract awards are automatically reduced.

With GEOSUPPLY: On 28 February 2026 (day of strikes), GOM detects: Lloyd's War-Risk Zone update (Source 1), IMO Safety Notice for Hormuz (Source 2), AIS divergence data showing 89% of vessels departing Gulf routes (Source 3), Reuters/AP/BBC triple confirmation (Sources 4+5). 3-of-5 sources confirmed. GOM emits `ForceMajeureEvent` for the Hormuz-Gulf corridor. `TriStateEscrow.sol` transitions Supplier A's contract to FORCE_MAJEURE state. Security deposit is protected. Delivery deadline is automatically extended. GCIL flags all of Supplier A's performance records from 28 February onward with `GOM_EXCLUDED`. On 26–28 March, Iran announces that vessels flagged by Pakistan and several other non-hostile nations may transit the strait under IRGC clearance protocols, with two Pakistani-flagged vessels permitted per day [6]. GOM detects the partial resolution: the AIS divergence metric drops below the 30% threshold for Pakistani-flagged vessels, and Lloyd's updates the war-risk zone classification to `ELEVATED` (not yet `NORMAL`) for approved flag states. `TriStateEscrow.sol` transitions Supplier A's contract to a conditional NORMAL state with extended deadline. Assuming the ship secures clearance and delivers by 15 April (a reasonable post-crisis projection), payment is released in full. Security deposit is returned.Performance records during the force majeure window remain `GOM_EXCLUDED`. Supplier A's ML ranking is unaffected.

B. Scenario B: The Stranded LNG Cargo

Situation: An Indian energy company has purchased LNG from QatarEnergy under a blockchain-enabled trade finance agreement. QatarEnergy declares force majeure on 2 March 2026 after Iranian strikes halt the Ras Laffan facility. The energy company's smart contract calls for a $5M penalty for failure to deliver, with QatarEnergy holding a 15% security deposit ($750K) on the $5M contract value. QatarEnergy's supplier performance record is flagged. `DELIVERY_FAILURE` across all affected contracts,

with ML ranking scores degraded network-wide.

Without GEOSUPPLY: Smart contract executes $5M penalty against QatarEnergy. QatarEnergy's supplier reputation is destroyed. The Indian company's insurance claim requires manual adjudication that takes 6–12 months.

With GEOSUPPLY: GOM confirms force majeure for the Qatar-LNG corridor (Lloyd's, IMO, UN statement, AIS, media). `TriStateEscrow.sol` suspends the $5M penalty. HITL-DRC convenes within 48 hours. 3-of-5 panel votes for non-fault (QatarEnergy had prepared the cargo; the facility was struck by an external actor). State transitions to PARTIAL_PERFORMANCE: QatarEnergy receives 30% payment for pre-loading preparations. The penalty is voided. `GeoRiskInsurance.sol` pays the Indian company's war-risk insurance claim automatically based on GOM confirmation, covering their consequential losses. Total resolution time: 5 days on-chain vs. 6–12 months manual.

C. Scenario C: The ML Ranking Victim

Situation: A UAE-based electronics component supplier (Supplier C) has delivered reliably for three years, maintaining an ML ranking in the 91st percentile. During the Hormuz crisis, three consecutive shipments fail to arrive, dropping Supplier C's ML ranking to the 54th percentile. The procurement system automatically reroutes future orders to a lower-quality Chinese competitor.

Without GEOSUPPLY: Supplier C's ranking drop is permanent (blockchain immutability). Future contract awards drop by 60%. Supplier C loses revenues for years based on three weeks of geopolitically excused non-performance.

With GEOSUPPLY: GCIL detects that all three failed shipments have transit timestamps within the GOM-confirmed force majeure window. The ML ranking system proposes a 37-percentile demotion. GCIL applies the Human Review Threshold (demotion > 15 percentile points). A procurement officer reviews the flagged records: all three shipments were GOM_EXCLUDED. Officer approves the exclusion. Supplier C's adjusted ML score: 89th percentile (two-point drop for associated delays outside the FM window). Future contracts continue normally.

D. Scenario D: The Sanctions Compliance Crisis

Situation: A German manufacturer has a smart contract with an Omani logistics provider for routing goods through alternative ports. Midway through the crisis, the U.S. expands Iran-related sanctions to include certain Omani entities involved in oil transshipment. The Omani logistics provider's parent company is added to the OFAC SDN list.

Without GEOSUPPLY: The smart contract, having no sanctions awareness, automatically releases payment to the Omani provider on delivery confirmation. The German manufacturer has now automatically paid a sanctioned entity — a potential criminal violation under U.S. extraterritorial sanctions law.

With GEOSUPPLY: SCL intercepts the payment transaction. OFAC SDN screening detects the parent company designation (updated the previous day). Payment is suspended; `SanctionsHoldEvent` is emitted on-chain. A compliance officer is alerted within 4 hours. Officer determines that the logistics services provided are exempt under humanitarian goods provisions. Officer documents the exemption rationale, attaches the OFAC general license reference, and releases payment with a digital signature. Full audit trail is maintained on-chain for regulatory review.

VI. Discussion

A. Theoretical Implications

Reconceptualizing "Code is Law." The foundational blockchain supply chain literature celebrates smart contract automation as replacing unreliable human judgment with deterministic, autonomous execution [51], [60]. GEOSUPPLY challenges this framing. The appropriate design principle is not "code is law" but **"code is law, with structured exception pathways for exogenous force."** Smart contracts can remain autonomous and immutable for the vast majority of normal operations while providing human-governed pathways for geopolitically exceptional events. GEOSUPPLY demonstrates that these two properties are not in conflict.

The Oracle Problem Reconceived. The oracle problem as framed in the literature [20], [56], [67] focuses on data integrity: how can external data be trusted before it enters the blockchain? GEOSUPPLY extends this to **contextual integrity**: how can the blockchain interpret data correctly given the geopolitical context in which that data was generated? A GPS reading showing a ship stationary in Duqm port is not a delivery failure — it is force majeure. The oracle problem is not only about data authenticity but about data interpretation.

Immutability as Contextual Record. Babich and Hilary [68] identified immutability as simultaneously blockchain's greatest strength and a significant liability. GEOSUPPLY resolves this tension without compromising immutability. Rather than correcting or deleting immutable records, GEOSUPPLY *annotates* them with context: the original "DELIVERY FAILURE" record remains immutable; the `GOM_EXCLUDED` flag and the HITL-DRC non-fault ruling are additional immutable records that provide interpretive context. Future ML models and procurement systems can read both records and apply appropriate weighting.

B. Practical Implications for Industry

Retroactive Application. Companies whose smart contracts executed incorrectly during the 2026 Hormuz crisis — automatically withholding deposits and destroying supplier reputations — face a governance crisis that GEOSUPPLY's on-chain annotation mechanism can partially address retroactively. By deploying GOM with historical event data and generating retroactive `ForMajeureEvent` records for the February–March 2026 period, existing platforms can annotate affected performance records with geopolitical context, supporting manual rehabilitation of affected supplier scores.

Contract Redrafting. As Bracewell LLP [10] and the National Law Review [49] advised, supply chain contracts should now expressly define geopolitical force majeure triggers. GEOSUPPLY's GOM architecture provides a technical implementation of these legal requirements: the Bracewell list of triggering events ("armed conflict," "acts of war," "embargo," "sanctions," "energy crisis," "geopolitical instability") maps directly to GOM's Lloyd's, IMO, UN, AIS, and media source verification architecture.

Platform Provider Responsibility. TradeLens' discontinuation in 2022 [7] was partly attributable to insufficient commercial differentiation and governance limitations. GEOSUPPLY's framework provides a governance differentiation pathway for next-generation trade platforms: war-resilient smart contracts that maintain trust even when geopolitical reality disrupts physical execution.

C. Limitations

GOM Oracle Centralization Risk. GOM's 3-of-5 multi-source verification reduces but does not eliminate oracle

manipulation risk. A sophisticated state actor could theoretically influence Lloyd's Market Association publications, IMO Safety Notices, and multiple newswires simultaneously. In practice, this attack surface is far smaller than the governance failure it replaces.

HITL-DRC Speed. A 5-person committee convening within 48 hours of a force majeure event requires pre-agreed governance protocols and responsive committee members. For supply chains in regions with poor communications infrastructure, this may be challenging. GEOSUPPLY's GOM-triggered automatic FORCE_MAJEURE state transition provides protection immediately (milliseconds), while HITL-DRC provides fine-grained adjudication within days — an acceptable timeline for billion-dollar contracts.

Partial Coverage. GEOSUPPLY addresses geopolitical force majeure. It does not address all force majeure categories: natural disasters, pandemics, or labor strikes require separate oracle architectures tailored to those event types. GEOSUPPLY's modular design enables future extension.

Jurisdictional Variation. Force majeure legal requirements differ across jurisdictions [10], [49]. GEOSUPPLY's smart contract parameters (trigger thresholds, partial payment percentages, DRC composition) are configurable per contract, enabling jurisdiction-appropriate governance within a shared framework.

VII. Conclusion

This paper presented GEOSUPPLY: a Geopolitical Oracle-Mediated Supply Chain Governance framework addressing the seven structural failures that the 2026 Strait of Hormuz crisis exposed in existing blockchain supply chain smart contract systems. Through a systematic review of the blockchain supply chain literature from 2016 to 2025, we documented that no prior work addresses on-chain geopolitical force majeure recognition, ML supplier ranking isolation during geopolitical disruption, tri-state payment escrow management, human-in-the-loop non-fault adjudication, alternative supplier activation, parametric geopolitical insurance, or sanctions-compliance integration.

The 2026 Hormuz crisis — with 21 confirmed Iranian attacks on merchant ships, 2 million TEUs of stranded cargo, and QatarEnergy's force majeure declaration affecting 20% of global LNG supply — demonstrated that "code is law" fails catastrophically when geopolitical reality renders contractual execution physically impossible. Blockchain immutability, celebrated as the technology's defining strength, became a source of systematic injustice when innocent suppliers had deposits withheld and reputation scores destroyed automatically by code that could not distinguish force majeure from non-performance.

GEOSUPPLY's seven components — GOM, TriStateEscrow.sol, GCIL, HITL-DRC, ASAP, GeoRiskInsurance.sol, and SCL — work together to preserve the automation and immutability that make blockchain supply chains valuable while providing structured, human-governed, on-chain pathways for geopolitical exceptionality. The framework's four scenario analyses demonstrate that GEOSUPPLY can resolve in days what current systems leave unresolved for months — without sacrificing the audit trail that blockchain's evidentiary value depends upon.

As Lumineau et al. [18] asked: "How can blockchain technologies be leveraged to enhance resilience in supply chains facing disruptions?" GEOSUPPLY answers: by acknowledging that some disruptions are not failures of the parties — and building governance frameworks that make that acknowledgment on-chain.

References

[1] A. Mohammed, V. Potdar, M. Quaddus, and W. Hui, "Blockchain Adoption in Food Supply Chains: A Systematic Literature Review on Enablers, Benefits, and Barriers," *IEEE Access*, vol. 11, pp. 14236–14255, 2023. https://doi.org/10.1109/ACCESS.2023.3236666

[2] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-Based Agri-Food Supply Chain: A Complete Solution," *IEEE Access*, vol. 8, pp. 69230–69243, 2020. https://doi.org/10.1109/ACCESS.2020.2986257

[3] A. Shojaei, I. Flood, H. I. Moud, M. Hatami, and X. Zhang, "An Implementation of Smart Contracts by Integrating BIM and Blockchain," in *Proc. Future Technologies Conf. (FTC) 2019*, K. Arai, R. Bhatia, and S. Kapoor, Eds., *Adv. Intell. Syst. Comput.*, vol. 1070. Cham, Switzerland: Springer, 2020, pp. 519–527. https://doi.org/10.1007/978-3-030-32523-7_36

[4] A. Sristy, "Blockchain in the Food Supply Chain: What Does the Future Look Like?" Walmart Global Tech, 2021. [Online]. Available: https://tech.walmart.com/content/walmart-global-tech/en_us/blog/post/blockchain-in-the-food-supply-chain.html

[5] AIM Multiple Research, "Blockchain Case Studies Across Key Industries," 2026. [Online]. Available: https://research.aimultiple.com/blockchain-case-studies/

[6] Al Jazeera, "Pakistan Secures Iran Deal to Send 20 Ships Through Strait of Hormuz," Mar. 28, 2026.

[7] A.P. Møller–Maersk, "Maersk and IBM to Discontinue TradeLens, a Blockchain-Enabled Global Trade Platform," Nov. 2022. [Online]. Available: https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens

[8] B.W. Ligar, S. Madenda, S.S. Mardjan, and T.M. Kusuma, "Design of a Traceability System for a Coffee Supply Chain Based on Blockchain and Machine Learning," J. Ind. Eng. Manage., vol. 17, no. 1, pp. 151–167, 2024. https://doi.org/10.3926/jiem.6256

[9] Blockchain Council, "Blockchain Supply Chain in 2026: Transparency and ROI," 2026. [Online]. Available: https://www.blockchain-council.org/blockchain/blockchain-supply-chain-transforming-supply-chain-management/

[10] Bracewell LLP, "Force Majeure in the Age of the Iran Conflict and Global Economic Disruption," March 2026.

[11] C.C.K Kumtepe, Unpacking the technology of trust: establishing trust and fairness in online dispute resolution through blockchain and smart contracts, International Journal of Law and Information Technology, Volume 33, 2025, eaaf017, https://doi.org/10.1093/ijlit/eaaf017

[12] "ChainLink: A Decentralized Oracle Network," Chainlink Whitepaper v2.0, 2021. [Online]. Available: https://chain.link/whitepaper

[13] Congressional Research Service, "Iran Conflict and the Strait of Hormuz: Impacts on Oil, Gas, and Other Commodities," CRS Report R45281, Mar. 2026. [Online]. Available: https://www.congress.gov/crs-product/R45281

[14] D. Bumblauskas, A. Mann, B. Dugan, and J. Rittmer, "A Blockchain Use Case in Food Distribution: Do You Know Where Your Food Has Been?" *Int. J. Inf. Manage.*, vol. 52, p. 102008, 2020. https://doi.org/10.1016/j.ijinfomgt.2019.09.004

[15] D. W. E. Allen, A. M. Lane, and M. Poblet, "The Governance of Blockchain Dispute Resolution," *Harvard Negotiation Law Review*, 2019. [Online]. Available: https://www.researchgate.net/publication/331155400_The_Governance_of_Blockchain_Dispute_Resolution

[16] DHL and Accenture, "Blockchain in Logistics: Perspectives on the Coming Decade of Change," DHL Trend Research, 2018.

[17] E. Tijan, S. Aksentijević, K. Ivanić, M. Jardas. "Blockchain Technology Implementation in Logistics," *Sustainability*, 2019, 11, 1185. https://doi.org/10.3390/su11041185

[18] F. Lumineau, G. Shang, J.M. Swaminathan, G. Tsoukalas, S.M. Wagner, and J.L. Zhao, "Charting the Future of Blockchain in Operations and Supply Chain Management: Opportunities and Challenges. J Oper Manag, 71: 886-892. https://doi.org/10.1002/joom.70014

[19] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology",13th International Conference on Service Systems and Service Management (ICSSSM), 2016, 1-6, https://api.semanticscholar.org/CorpusID:21581564

[20] G. Caldarelli, "Can Artificial Intelligence Solve the Blockchain Oracle Problem? Unpacking the Challenges and Possibilities," 2025. https://doi.org/10.3389/fbloc.2025.1682623

[21] G. Narayanan, I. Cvitić, D. Peraković, and S. P. Raja, "Role of Blockchain Technology in Supply Chain Management," *IEEE Access*, vol. 12, pp. 19021–19034, 2024. https://doi.org/10.1109/ACCESS.2024.3361310

[22] H. Halaburda, N. Levina, and S. Min, "Digitization of Transaction Terms Within TCE: Strong Smart Contract as a New Mode of Transaction Governance," *MIS Q.*, vol. 48, no. 2, pp. 825–846, 2024.

[23] H. M. Kim and M. Laskowski, "Toward an Ontology-Driven Blockchain Design for Supply-Chain Provenance," *Intell. Syst. Account. Finance Manage.*, vol. 25, no. 1, pp. 18–27, 2018.

[24] H. Min, "Blockchain Technology for Enhancing Supply Chain Resilience," *Bus. Horizons*, vol. 62, no. 1, pp. 35–45, 2019.

[25] H. Pun, J.M Swaminathan, and P. Hou "Blockchain Adoption for Combating Deceptive Counterfeits"". Prod Oper Manag, 30: 864-882. https://doi.org/10.1111/poms.13348

[26] HFW, "Forecast for 2025: 5 Potential Areas for Commodity Contract Disputes and Key Related Clauses," Dec. 2024. [Online]. Available: https://www.hfw.com/insights/forecast-for-2025-5-potential-areas-for-commodity-contract-disputes\-and-key-related-clauses/

[27] "How the Iran Conflict is Impacting Global Ocean Shipping Flows," *Supply Chain Dive*, March 2026. [Online]. Available: https://www.supplychaindive.com/news/iran-conflict-global-ocean-shipping-flows-lars-jensen-tpm26/814250/

[28] "Iran and Middle East Conflict Impacts Global Economy," March 2026. [Online]. Available: https://www.deloitte.com/us/en/insights/topics/economy/iran-middle-east-conflict-impacts-global-economy.html

[29] J. Chod, N. Trichakis, G. Tsoukalas, H. Aspegren, and M. Weber, "On the Financing Benefits of Supply Chain Transparency and Blockchain Adoption," *Manage. Sci.*, vol. 66, no. 10, pp. 4378–4396, 2020. https://doi.org/10.1287/mnsc.2019.3434

[30] J. Wu, X. Wang, L. Chen, and Y. He, "Blockchain Adoption to Eliminate Dispute in Platform-Supplier Cooperative Delivery," Comput. Ind. Eng., vol. 192, p. 110227, Jun. 2024. https://doi.org/10.1016/j.cie.2024.110227

[31] K. Behnke and M. F. W. H. A. Janssen, "Boundary Conditions for Traceability in Food Supply Chains Using Blockchain Technology," *Int. J. Inf. Manage.*, vol. 52, p. 101969, 2020. https://doi.org/10.1016/j.ijinfomgt.2019.05.025

[32] K. Francisco and D. Swanson, "The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency," *Logistics*, vol. 2, no. 1, p. 2, 2018.

[33] K. Aditya, S. Chakraborty, A. Dahire, A. Kumari, M. Milanova, "Integrating Blockchain, IoT, and AI in Supply Chain Management.," In: Grover, D.V., Balusamy, D.B.B., Milanova, D.M., Felix, D.A.Y. (eds) Blockchain, IoT, and AI Technologies for Supply Chain Management. Apress, Berkeley, CA. https://doi.org/10.1007/979-8-8688-0315-4_9

[34] KPMG, "AI, Blockchain and IoT Transform Supply Chain Performance," 2025. [Online]. Available: https://kpmg.com/xx/en/our-insights/operations/ai-blockchain-transform-supply-chain-performance.html

[35] L. Ni and E. Irannezhad, "Performance Analysis of LogisticChain: A Blockchain Platform for Maritime Logistics," *Comput. Ind.*, vol. 154, p. 104038, 2024. https://doi.org/10.1016/j.compind.2023.104038

[36] Logistics Viewpoints, "How Smart Contracts Are Impacting Supply Chains," March 2025. [Online]. Available: https://logisticsviewpoints.com/2025/03/12/how-smart-contracts-are-impacting-supply-chains/

[37] M. Buchwald, "Smart Contract Dispute Resolution: The inescapable flaws of blockchain-based arbitration," *Univ. Pennsylvania Law Rev.* https://www.jstor.org/stable/45467490

[38] M. Kouhizadeh, S. Saberi, and J. Sarkis, "Blockchain Technology and the Sustainable Supply Chain: Theoretically Exploring Adoption Barriers," *Int. J. Prod. Econ.*, vol. 231, p. 107831, 2021. https://doi.org/10.1016/j.ijpe.2020.107831

[39] M.M Abdelhamid, L. Sliman, R.B Djemaa, "AI-Enhanced Blockchain for Scalable IoT-Based Supply Chain," Logistics, vol. 8, no. 4, p. 109, Nov. 2024. https://doi.org/10.3390/logistics8040109

[40] M. M. Queiroz and S. F. Wamba, "Blockchain Adoption Challenges in Supply Chain: An Empirical Investigation of the Main Drivers in India and the USA," *Int. J. Inf. Manage.*, vol. 46, pp. 70–82, 2019.

[41] M. Montecchi, K. Plangger, and M. Etter, "It's Real, Trust Me! Establishing Supply Chain Provenance Using Blockchain," *Bus. Horizons*, vol. 62, no. 3, pp. 283–293, 2019.

[42] M. Narenji, A. Mahmoodi, M. Jasemi, S. M. Sajadi, and M. Amini, "A game-theoretic framework for optimizing supply chain coordination and production," *Supply Chain Analytics*, vol. 11, p. 100139, 2025. https://doi.org/10.1016/j.sca.2025.100139

[43] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-Based Traceability in Agri-Food Supply Chain Management: A Practical Implementation," in *Proc. 2018 IoT Vertical and Topical Summit on Agriculture – Tuscany (IOT Tuscany)*, Tuscany, Italy, 2018, pp. 1–4. https://doi.org/10.1109/IOT-TUSCANY.2018.8373021

[44] M. U. K. Afridi, "BCRRS: A Blockchain-Anchored Contractor Reputation System with Machine Learning Ranking, Anti-Nepotism Governance, and Cross-Border Intelligence for Construction Procurement, 2026, under review.

[45] N. B. Keskin, C. Li, and J.-S. Song, "The Blockchain Newsvendor: Value of Freshness, Transparency, and Smart Contracts," *Manage. Sci.*, vol. 71, no. 8, pp. 6666–6682, 2024. https://doi.org/10.1287/mnsc.2021.02949

[46] N. Kshetri, "1 Blockchain's roles in meeting key supply chain management objectives," *Int. J. Inf. Manage.*, vol. 39, pp. 80–89, 2018.

[47] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," *EXTROPY: J. Transhumanist Thought*, vol. 18, no. 2, 1996. [Online]. Available: https://nakamotoinstitute.org/library/smart-contracts-building-blocks-for-digital-markets/

[48] N. Tsolakis, R. Schumacher, M. Dora, and M. Kumar, "Artificial Intelligence and Blockchain Implementation in Supply Chains: A Pathway to Sustainability and Data Monetisation?" *Ann. Oper. Res.*, vol. 327, no. 1, pp. 157–210, Aug. 2023. https://doi.org/10.1007/s10479-022-04785-2

[49] National Law Review, "Force Majeure in the Age of the Iran Conflict and Global Economic Disruption," March 2026. [Online]. Available: https://natlawreview.com/article/force-majeure-age-iran-conflict-and-global-economic-disruption

[50] Ö. Karaduman, G. Gülhas, Blockchain-Enabled Supply Chain Management: A Review of Security, Traceability, and Data Integrity Amid the Evolving Systemic Demand. Appl. Sci. 2025, 15, 5168. https://doi.org/10.3390/app15095168

[51] P. Bottoni, N. Gessa, G. Massa, R. Pareschi, H. Selim and E. Arcuri Intelligent Smart Contracts for Innovative Supply Chain Management. Front. Blockchain 3:535787. https://doi.org/10.3389/fbloc.2020.535787

[52] P. Chen, X. Lei, O. Lin, and Y. Yuan, "The Impact of Blockchain Financial Technology Transformation on Supply Chain Disruption Risks," *Int. Rev. Econ. Finance*, vol. 102, p. 104343, 2025. https://doi.org/10.1016/j.iref.2025.104343

[53] P. Han. AI-powered digital arbitration framework leveraging smart contracts and electronic evidence authentication. Sci Rep 15, 37327 (2025). https://doi.org/10.1038/s41598-025-21313-x

[54] P. Živković, D. McCurdy, M. Zou, and A. H. Raymond, "Mind the Gap: Tech-Based Dispute Resolutions in Global Supply Blockchains," *Bus. Horizons*, vol. 64, no. 6, pp. 799–807, 2021. https://doi.org/10.1016/j.bushor.2021.07.014

[55] S. Ambulkar, J. Blackhurst, and S. Grawe, "Firm's Resilience to Supply Chain Disruptions: Scale Development and Empirical Examination," *J. Oper. Manage.*, vol. 33–34, pp. 111–122, 2015.

[56] S. Chougule and L. Cantisani, "The Oracle Problem in Smart Contracts: Data Privacy, Security, and Solutions," MediaLaws, Nov. 2024. [Online]. Available: https://www.medialaws.eu/rivista/the-oracle-problem-in-smart-contracts-data-privacy-security-and-solutions/

[57] S. Figorilli, F. Antonucci, C. Costa, F. Pallottino, L. Raso, M. Castiglione, E. Pinci, D. Del Vecchio, G. Colle, A. R. Proto, G. Sperandio, and P. Menesatti, "A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood Along the Whole Supply Chain," *Sensors*, vol. 18, no. 9, p. 3133, 2018. https://doi.org/10.3390/s18093133

[58] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[59] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management." International Journal of Production Research, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

[60] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," *IEEE Trans. Syst. Man Cybern.: Syst.*, vol. 49, no. 11, pp. 2266–2277, 2019. https://doi.org/10.1109/TSMC.2019.2895123

[61] S&P Global, "Utility at a Cost: Assessing the Risks of Blockchain Oracles," Special Report, Oct. 2024. [Online]. Available: https://www.spglobal.com/en/research-insights/special-reports/utility-at-a-cost-assessing-the-risks-of-blockchain-oracles

[62] Silent Data, "What Is the Blockchain Oracle Problem, and Why Does It Matter?" 2024. [Online]. Available: https://www.silentdata.com/blog/what-is-the-blockchain-oracle-problem-and-why-does-it-matter

[63] Supply Chain Connect, "Potential Supply Chain Implications of the Iran Conflict," 2026. [Online]. Available: https://www.supplychainconnect.com/supply-chain-technology/article/55362817/potential-supply-chain-implications-of-the-iran-conflict

[64] T. K. Dasaklis, F. Casino, V. Kanakaris, and N. Rachaniotis, "A Systematic Literature Review of Blockchain-Enabled Supply Chain Traceability Implementations," *Sustainability*, vol. 14, no. 4, p. 2439, 2022. https://doi.org/10.3390/su14042439

[65] Thompson Coburn LLP, "Are Smart Contracts Smart Enough? COVID-19, Force Majeure, Blockchain and Oracles," 2020. [Online]. Available: https://www.thompsoncoburn.com/insights/are-smart-contracts-smart-enough-covid-19-force-majeure-blockchain\-and-oracles/

[66] Tres Astronautas, "Using Blockchain in Supply Chain to Revolutionize Logistics," 2024. [Online]. Available: https://www.tresastronautas.com/en/blog/using-blockchain-in-supply-chain-to-revolutionize-logistics

[67] U. Majeed, L.U. Khan, I. Yaqoob, S.M.A Kazmi, K. Salah and C.S. Hong, "Blockchain for IoT-Based Smart Cities: Recent Advances, Requirements, and Future Challenges," *J. Network Comput. Appl.*, vol. 181, p. 103007, 2021.https://doi.org/10.1016/j.jnca.2021.103007

[68] V. Babich and G. Hilary, "OM Forum—Distributed Ledgers and Operations: What Operations Management Researchers Should Know About Blockchain Technology," *Manuf. Serv. Oper. Manage.*, vol. 22, no. 2, pp. 223–240, 2020. https://doi.org/10.1287/msom.2018.0752

[69] VeChain Foundation, "VeChain Technical Whitepaper," v2.0.

[70] W. Alkhader, K. Salah, A. Sleptchenko, R. Jayaraman, I. Yaqoob, and M. Omar, "Blockchain-Based Decentralized Digital Manufacturing and Supply for COVID-19 Medical Devices and Supplies," IEEE Access. 2021 Oct 5;9:137923-137940. doi: 10.1109/ACCESS.2021.3118085. https://doi.org/10.1109/ACCESS.2021.3118085

[71] we.trade and IBM, "we.trade: Blockchain-Based Trade Finance Platform," IBM Case Study, 2021. [Online]. Available: https://www.ibm.com/case-studies/wetrade-blockchain-fintech-trade-finance

[72] X. Lyu, B. Huo, and M. Tian, "The Effect of Blockchain Implementation on Supply Chain Disputes," *Int. J. Prod. Econ.*, vol. 288, p. 109708, 2025. https://doi.org/10.1016/j.ijpe.2025.109708

[73] Y. Chang, E. Iakovou, and W. Shi, "Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art, Challenges and Opportunities," *Int. J. Prod. Res.*, vol. 58, no. 7, pp. 2082–2099, 2020. https://doi.org/10.1080/00207543.2019.1651946

[74] Y. Cui, M. Hu, and J. Liu, "Value and Design of Traceability-Driven Blockchains," *Manuf. Serv. Oper. Manage.*, 2023. https://doi.org/10.1287/msom.2022.1161

[75] Y. Cui, V. Gaur, and J. Liu "Supply Chain Transparency and Blockchain Design," *Manage. Sci.*, 2023. https://doi.org/10.1287/mnsc.2023.4851

[76] Y. Gabuthy, "Blockchain-Based Dispute Resolution: Insights and Challenges," *Games*, vol. 14, no. 3, p. 34, 2023. https://doi.org/10.3390/g14030034

[77] Y. Wang, J. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda". Supply Chain Management: An International Journal, Vol. 24 No. 1 pp. 62–84, doi:https://doi.org/10.1108/SCM-03-2018-0148