Trust-Aware Reinforcement Learning Mechanisms for Dynamic Capacity Sharing in Decentralized Supply Networks

Xiaozhou Tao
Department of Computer Science, University of Central Florida, Orlando, FL, USA.
tao1972@ucf.edu

Rishi A. Malhotra
School of Information Technology, University of Cincinnati, Cincinnati, OH, USA.
rishimalhotra@uc.edu

Abstract

Decentralized supply networks have become the dominant architecture for producing and delivering goods, yet they face persistent coordination failures when capacity must be dynamically shared among autonomous firms. Traditional contract-based mechanisms and centralized optimization often prove brittle in the face of demand volatility, information asymmetry, and the absence of enforceable authority. This paper proposes a novel class of trust-aware reinforcement learning mechanisms that enable dynamic capacity sharing by synthesizing multi-agent learning with computational models of inter-organizational trust. We conceptualize trust not as a static binary variable but as a continuously updated, multidimensional representation of a partner's reliability, reciprocity, and fairness, which directly shapes the reward structures and policy updates of RL agents. The system-level architecture is presented as a hybrid governance layer in which decentralized learning nodes interact through a shared trust ledger, while a lightweight digital coordination layer handles the broadcasting of capacity requests and reputation signals. We examine structural trade-offs between exploration for network efficiency and the preservation of trust capital, highlighting how myopic RL policies erode long-term collaboration potential. The discussion extends to infrastructure requirements for deploying such mechanisms at scale, including the role of industrial data spaces, digital twins for counterfactual training, and regulatory frameworks for algorithmic capacity allocation. Additionally, we analyze fairness and robustness, demonstrating that trust-aware mechanisms can mitigate bullwhip amplification and reduce the frequency of cascading shortages in disrupted supply networks. By integrating computational trust into the RL objective, the proposed mechanisms reframe capacity sharing as a cooperative sequential decision problem in which agents jointly learn to balance self-interest with systemic resilience. We conclude by outlining policy considerations for promoting algorithmic transparency and accountability in autonomous supply networks.

Keywords

Decentralized supply networks; dynamic capacity sharing; trust-aware reinforcement learning; multi-agent systems; governance; fairness.

1. Introduction

Global supply chains have evolved from vertically integrated, hierarchical structures into sprawling networks of legally independent yet operationally interdependent firms. This

decentralization yields benefits in specialization, cost efficiency, and geographic flexibility, but simultaneously fragments decision-making authority and obscures visibility across tiers. In such environments, the dynamic sharing of production, warehousing, and logistics capacity emerges as a critical coordination mechanism to absorb demand shocks, pool surplus resources, and maintain service levels without excessive buffer stocks. However, capacity sharing in decentralized networks is inherently plagued by strategic uncertainty: firms possess private information about their true available capacity, cost structures, and future demand projections, and they must decide whether to share resources with partners who may not reciprocate in the future. The resulting coordination problem goes beyond inventory allocation; it is a socio-technical challenge in which mutual reliance, reputation, and perceived fairness directly influence economic outcomes. Recent disruptions, from the COVID-19 pandemic to geopolitical realignments, have starkly demonstrated that purely market-based or contract-driven capacity sharing lacks the adaptive speed required to reconfigure supply networks under stress [1,2]. Consequently, there is a pressing need for computational mechanisms that can automate capacity allocation while embedding the nuanced social fabric of trust that underpins resilient inter-firm collaboration.

The traditional toolkit for supply chain coordination relies on quantity-flexibility contracts, option pricing, and game-theoretic mechanism design that assume well-defined payoff functions and rational, profit-maximizing agents [3]. These approaches, although theoretically elegant, often fail when confronted with the non-stationary dynamics of real supply networks wherein demand signals shift abruptly, production lead times are stochastic, and firms' internal policies evolve over time [4,5]. Even when information-sharing platforms reduce opacity, the combinatorial complexity of simultaneous bilateral capacity exchanges renders centralized optimization computationally intractable and organizationally unacceptable due to confidentiality concerns. Reinforcement learning (RL) has recently gained traction as a method for learning near-optimal policies in complex, high-dimensional supply chain environments without explicit modeling of transition probabilities [6,7]. Multi-agent RL extends this paradigm to systems where autonomous learners interact, making it a natural fit for decentralized capacity sharing. Yet, most current applications of RL in supply chains treat agents as isolated entities optimizing local costs, neglecting the relational context in which repeated interactions build trust capital. The introduction of trust-aware RL mechanisms thus represents a strategic shift from purely self-interested learning to cooperative learning anchored in reciprocation.

Trust in a supply network is not merely a philosophical concept; it is an empirically measurable construct that influences ordering behavior, information veracity, and willingness to invest in partner-specific assets. Without trust, capacity sharing degenerates into short-term opportunistic gaming where agents over-report needs and under-report surpluses, leading to systemic inefficiencies akin to the bullwhip effect but amplified across a mesh of horizontal ties [2]. Incorporating trust signals into the reward function and state representation of RL agents can transform capacity sharing into a repeated social dilemma in which defection is penalized not only by immediate revenue loss but by a decay in future collaboration opportunities. This paper develops a conceptual architecture and governance framework for such trust-aware RL mechanisms, arguing that they constitute a necessary evolution toward autonomous yet resilient supply networks. The following sections explore the structural foundations, algorithmic design principles, infrastructural enablers, and policy implications of this class of mechanisms.

2. Foundations of Decentralized Capacity Sharing and Trust

2.1 Supply Networks as Complex Adaptive Systems

Modern supply chains can be understood as complex adaptive systems characterized by distributed control, emergent behavior, and adaptation through local interactions. In this view, network-level properties such as resilience, ripple effects, and capacity pooling arise not from a central orchestrator but from the collective decisions of autonomous firms responding to local information [1]. The shift toward platform-driven ecosystems and manufacturing-as-a-service models intensifies this decentralization, enabling firms to dynamically source production capacity from a fluid pool of contract manufacturers and logistics providers. This fragmentation creates a tension between the flexibility gains of market-based access to capacity and the coordination costs of managing trust relationships across a large, evolving set of partners. When a firm suddenly faces a surge order that exceeds its own capacity, it must quickly identify which adjacent nodes in the network can absorb the overflow, negotiate terms, and monitor fulfillment, all while protecting proprietary data. The speed and quality of such lateral capacity transfers can determine whether a local disturbance escalates into a network-wide disruption [5,6].

2.2 The Role of Trust in Lateral Collaboration

Trust in inter-organizational relationships is a multi-faceted construct comprising competence, integrity, benevolence, and predictability. In the context of capacity sharing, competence trust refers to the belief that a partner actually possesses the surplus capacity it claims and can deliver to the required quality standards. Integrity trust involves confidence that the partner will not strategically misrepresent its availability or engage in post-agreement renegotiation. Benevolence trust captures the willingness to accept short-term costs to assist a partner in distress, anticipating future reciprocity. These dimensions are not exogenous constants but co-evolve with the history of interactions, making them inherently learnable from past transaction data. From a computational standpoint, trust can be encoded as a reputation score that aggregates several signals: on-time delivery rate, divergence between promised and actually provided capacity, premium or discount applied during urgent requests, and consistency of communication [8,9]. Such trust scores become valuable state variables for RL agents, allowing them to differentiate between a reliable long-term partner and an opportunistic node that exploits capacity-sharing protocols during crises only to defect later.

2.3 Limitations of Static Contractual Mechanisms

Conventional capacity reservation contracts set ex-ante terms for a predetermined quantity of capacity, often with fixed unit prices and penalty clauses for non-utilization or shortfall. These instruments provide stability but lack the flexibility to handle highly variable and correlated demand spikes that ripple through networks [3,4]. Option-based mechanisms offer more flexibility by allowing firms to purchase call options on capacity, yet they still presume a liquid market with sufficient transparency and cannot easily accommodate the qualitative trust aspect. Moreover, rigid contracts can perversely discourage spontaneous mutual aid when a partner encounters an unexpected shortage, because providing unplanned capacity may violate existing capacity commitments to other buyers, exposing the helping firm to contractual penalties. The resulting inertia undermines the very agility that decentralized networks need to cope with black swan events. Trust-aware RL mechanisms differ fundamentally because they do not attempt to specify all contingencies ex-ante. Instead, they

learn adaptive policies that weigh the immediate profit from a capacity trade against the long-term reputational consequences, thereby internalizing trust as a dynamic asset.

3. Reinforcement Learning as a Coordination Backbone

3.1 Multi-Agent Reinforcement Learning for Supply Chains

Reinforcement learning provides a formal framework in which an agent learns a mapping from states to actions by maximizing a cumulative reward signal through trial-and-error interaction with an environment. When multiple agents learn concurrently, the environment becomes non-stationary from the perspective of any single agent, introducing strategic dynamics that can be studied using multi-agent RL [10]. In supply chain applications, deep RL has been successfully applied to inventory management, order fulfillment, and routing problems, often outperforming heuristic policies in complex, stochastic settings [7,8]. Extending these successes to horizontal capacity sharing requires each firm to train an agent that can issue capacity requests, publish availability updates, and accept or decline incoming requests, all while learning the trustworthiness patterns of potential partners. The state space for such an agent includes local inventory levels, backlog, production schedule, and a vector of trust scores for known peers. The action space includes the decision to share a certain quantity of capacity, the price to offer, and the selection of a specific partner. The reward function must blend operational metrics such as total profit and service level with trust-related outcomes, thereby encoding the dual economic and social objectives of the firm.

3.2 Trust as a State Modulator and Reward Augmenter

We propose two principal mechanisms for embedding trust in the RL formulation. First, trust scores are incorporated directly into the state representation, enabling the policy network to condition its actions on the perceived reliability of each candidate partner. For example, an agent may learn to allocate a larger share of surplus capacity to a partner with high integrity trust during a period of low demand, even if the immediate unit margin is slightly lower, because the action maintains a high-quality relationship that will yield priority access to that partner's capacity during future shortages. Second, trust modifies the reward structure by adding a term that reflects the improvement or deterioration of bilateral trust capital resulting from a transaction. When an agent fulfills a capacity-sharing request promptly and at fair terms, the recipient's trust score towards the provider increases, generating an intrinsic reward that captures the option value of future collaboration. Conversely, reneging on a committed capacity transfer or exploiting a partner's urgent need to extract exorbitant prices damages trust capital and incurs a reputation penalty in the agent's objective function [9,10]. This formulation extends the standard RL reward beyond immediate financial metrics, requiring careful calibration of the weight assigned to trust-based components to avoid either excessive risk-aversion that chokes capacity sharing or reckless trust-building that exposes the firm to exploitation.

3.3 The Trade-off Between Exploration and Trust Preservation

A central challenge in RL is balancing exploration and exploitation. In single-agent settings, exploration entails trying actions with uncertain outcomes to gather information. In multi-agent trust-aware settings, exploration takes on a social dimension because probing the trustworthiness of an unfamiliar partner risks a failed transaction that erodes the exploring agent's own reputation within the broader network. If an agent systematically experiments with new, untested partners to discover more favorable terms, it may be perceived as fickle or untrustworthy by its established partners, who might then reduce their own willingness to

share capacity. This creates a structural tension: myopic exploration for short-term cost optimization can damage the relational infrastructure that sustains long-term resilience. The trust-aware RL architecture must therefore incorporate a cautious exploration strategy, such as optimism in the face of reputational uncertainty tempered by a trust budget, where the agent is allowed to devote only a limited fraction of its cumulative capacity-sharing volume to unfamiliar partners. Alternatively, counterfactual reasoning enabled by high-fidelity digital twins can allow agents to simulate interactions with potential new partners without real-world reputational exposure [11,12]. Designing these exploration mechanisms without stifling the network's ability to reconfigure itself is a key architectural consideration.

4. System Architecture and Governance of Trust-Aware Mechanisms

4.1 A Hybrid Coordination Layer

Implementing trust-aware RL for dynamic capacity sharing across a decentralized network demands a coordination infrastructure that sits between fully centralized planning and purely peer-to-peer messaging. We envision a hybrid architecture comprising three layers: a local RL agent embedded within each firm's planning system, a distributed trust ledger that aggregates pseudonymized performance data, and a lightweight network coordination node that facilitates matchmaking between capacity requests and available offers without exposing sensitive internal data. The local RL agent owns its policy network and reward model, which includes proprietary cost functions and strategic parameters configurable by the firm's management. The trust ledger functions as a shared, tamper-evident repository where each capacity-sharing transaction is recorded along with outcome metrics such as delivery timeliness, quality conformance, and price fairness. Blockchain-based implementations of such ledgers have been explored for supply chain traceability and can be extended to encode trust-relevant transaction attributes while supporting zero-knowledge proofs that preserve the privacy of sensitive volumes or prices [13]. The network coordination node does not prescribe allocations; it simply broadcasts anonymized capacity shortages or surpluses and returns a filtered list of potential partners ranked by compatibility of technical requirements and by aggregate trust scores, leaving the final partner selection and negotiation to the RL agents.

4.2 Training and Simulation Infrastructure

Training trust-aware RL agents at scale requires access to high-fidelity simulation environments that mirror the dynamics of the actual supply network, including production lead times, transportation delays, quality inspection processes, and stochastic demand patterns. Digital twins of the physical supply chain, continuously synchronized with operational data, provide a safe sandbox in which RL agents can learn trust-sensitive policies without risking real-world disruptions. Within the digital twin environment, multi-agent training can proceed in an iterative manner where agents interact over simulated months or years of operation, allowing trust relationships to develop endogenously. Recent advances in deep multi-agent RL, including centralized training with decentralized execution and population-based training, enable agents to learn cooperative behaviors that generalize beyond the specific partners encountered during training [12,14]. The simulation framework must also support scenario injection, introducing synthetic disruptions such as supplier bankruptcies or port closures, so that agents learn the value of maintaining a diversified trust portfolio that includes redundant capacity sources. The computational cost of such training is significant but can be managed through cloud-based infrastructure and incremental learning approaches that fine-tune pre-trained base policies on the specific network topology and partner set.

4.3 Governance and Policy Enforcement in Autonomous Systems

The delegation of capacity-sharing decisions to RL agents raises profound governance questions about accountability, transparency, and compliance with antitrust regulations. When algorithms autonomously agree on terms of capacity exchange, it becomes difficult to distinguish between efficient market coordination and collusive behavior that harms competition. A trust-aware mechanism introduces an additional layer of algorithmic governance because trust scores and reputation models embed implicit norms of acceptable behavior. The network must therefore be governed by a multi-stakeholder consortium that defines the rules for trust computation, sets bounds on allowed price markups during capacity spikes, and periodically audits agent behaviors for discriminatory or exclusionary patterns. Drawing on the emerging literature on algorithmic fairness, governance frameworks can require that trust models not penalize firms based on attributes such as size or geographic location in ways that entrench existing structural inequalities [15]. Furthermore, a digital coordination authority should maintain an override capability to enforce humanitarian capacity allocation during public health emergencies, temporarily shifting agent objectives from profit to societal need. This hybrid governance model, combining algorithmic autonomy with human-supervised guardrails, is essential for building institutional trust in the system itself.

5. Fairness, Robustness, and Resilience Implications

5.1 Fairness in Autonomous Capacity Allocation

Fairness concerns arise at multiple levels in a trust-aware capacity-sharing mechanism. At the individual agent level, the reward function must balance local profit maximization with the maintenance of a positive trust reputation; an overly aggressive agent that frequently reneges on commitments may be ostracized from the network, losing access to capacity that is crucial for survival. This self-interested reason to maintain fairness converges with the normative goal of equitable access to resources across the network. However, the feedback loop between trust and access can produce virtuous or vicious cycles: firms with initially high trust scores receive more capacity requests, which allows them to demonstrate reliability further and boost their scores, while firms that experienced a few early failures due to exogenous shocks may be permanently penalized. Trust-aware mechanisms need explicit fairness adjustments, such as trust decay reset policies or periodic reinitialization windows, to ensure that the system does not lock in historical advantages [15]. On the network scale, fairness also pertains to the distribution of capacity-sharing gains. Without proper design, large firms with diversified internal resources may use the system primarily as a low-cost buffer, while small and medium enterprises depend on it for survival. The mechanism's parameters can be tuned to enforce a minimum capacity access guarantee for all participating nodes, ensuring that trust-based prioritization does not violate egalitarian principles essential for long-term ecosystem stability.

5.2 Robustness Against Strategic Manipulation

Any reputation-based system is vulnerable to strategic manipulation, including whitewashing attacks where a firm rebrands to erase a poor trust record and sybil attacks where a single entity operates multiple identities to collude or inflate mutual trust ratings. In a business-to-business supply network, the cost of changing a legal identity is non-trivial, which limits the ease of whitewashing but does not eliminate it entirely. Trust-aware RL mechanisms can incorporate identity binding through digital certificates issued by trusted certificate authorities and enforce a minimum activity history before a firm gains full access to the capacity-sharing

market. Moreover, the trust model should weigh long-term interaction history more heavily than short-lived bursts of positive transactions, making it costly for a manipulator to rapidly build a false reputation. At the algorithmic level, adversarial training techniques can be employed to harden RL policies against partners who learn to exploit the trust dynamics, for instance by cooperating only during low-demand periods to inflate trust and then defecting during a major crisis. Such robustness is crucial because the very adaptivity of RL agents can be turned against the system if adversaries understand the trust model's update rules. The architecture should therefore treat the trust scoring function itself as a dynamic, learnable component that co-evolves with the strategies of participating agents in a continual arms-race dynamic informed by mechanism design theory [16].

5.3 Resilience and Systemic Risk Mitigation

The ultimate test of capacity-sharing mechanisms lies in their ability to dampen rather than amplify systemic disruptions. Trust-aware RL can contribute to resilience by enabling rapid formation of ad-hoc capacity alliances when a node or a region is hit by an unexpected shock. Because agents have already learned which partners are trustworthy, they can bypass prolonged negotiation and due diligence procedures and immediately redirect capacity flows to affected areas. The bullwhip effect, which originates in part from gaming behaviors and exaggerated orders under scarcity, can be mitigated because trust-based policies incentivize truthful signaling of demand and genuine capacity constraints; an agent that inflates its needs to hoard capacity will see its trust degrade once the discrepancy is revealed, undermining its future ability to secure help [2,17]. Furthermore, the global reward signal that includes network-level resilience metrics can be approximated during training by aggregating individual agent rewards with a network health index that measures the variance of capacity utilization across nodes. Agents thus learn that highly unequal distributions of capacity, even if locally profitable for a few, create fragility that eventually harms all through cascading failures. Trust-aware mechanisms therefore internalize a systemic perspective without requiring a central optimizer, achieving a form of polycentric resilience that aligns with the complex adaptive nature of modern supply ecosystems.

6. Deployment Constraints and Future Pathways

6.1 Infrastructure and Interoperability

Deploying trust-aware RL mechanisms at scale demands a robust digital infrastructure encompassing industrial IoT for real-time capacity monitoring, secure data-sharing platforms, and interoperability standards that allow heterogeneous enterprise resource planning systems to publish and consume capacity events in a common format. Reference architectures such as the International Data Spaces (IDS) and GAIA-X provide governance frameworks for sovereign data sharing, which align well with the need to share trust-relevant performance data without revealing proprietary information. The digital twin layer must be able to ingest data from multiple firms while respecting data ownership boundaries, which can be accomplished through federated simulations where each participant maintains its own twin and only aggregated, anonymized training signals are shared with a central model aggregator. This federated RL paradigm preserves the confidentiality of local cost functions and demand forecasts, addressing one of the primary barriers to inter-firm collaboration [18]. At the network level, edge computing nodes co-located with manufacturing and logistics facilities can execute local agent inference with low latency, ensuring that capacity-sharing decisions are made in milliseconds. The path to deployment will likely begin with industry consortia in

semi-integrated sectors such as automotive or consumer electronics, where supply relationships are already dense and the benefits of dynamic capacity sharing are substantial.

6.2 Regulatory and Ethical Dimensions

As algorithmic agents begin to autonomously negotiate capacity, regulators will scrutinize whether such systems violate competition law, create new channels for price fixing, or systematically disadvantage certain classes of firms. The use of trust scores derived from transaction histories raises questions analogous to credit scoring, including rights to explanation, rectification, and appeal when a firm is denied capacity based on an opaque reputation model. Emerging AI regulations in the European Union and elsewhere impose requirements for high-risk AI systems to ensure human oversight, transparency, and robustness, criteria that directly apply to trust-aware RL mechanisms operating in critical supply chain functions [19]. To preempt regulatory friction, system designers should implement interpretable trust modules that can generate natural language explanations of why a particular partner was selected or why capacity was refused, and maintain comprehensive audit trails logged on distributed ledgers. Additionally, the network governance body should include representatives from civil society and regulatory agencies to oversee the calibration of fairness parameters and to adjudicate disputes. These regulatory mechanisms are not extraneous burdens but integral components that build the institutional trust necessary for firms to agree to delegate capacity-sharing authority to learning algorithms.

6.3 Toward Self-Governing Supply Ecosystems

Looking forward, trust-aware RL mechanisms can serve as the kernel for fully self-governing supply ecosystems in which capacity is continuously rebalanced across the network through a combination of autonomous agents and smart contracts that trigger predefined transfers when trust and capacity thresholds align. Such ecosystems would blur the boundaries between strategic alliances and market transactions, realizing a form of algorithmic coopetition that has long been envisioned but rarely executed due to trust deficits and coordination overhead. Technological advances in large-scale multi-agent RL, secure multi-party computation, and decentralized identity management will progressively lower the barriers to such systems. Nevertheless, the evolution must be guided by broad stakeholder dialogues that align the incentives of private firms with societal objectives including supply chain sustainability, carbon footprint reduction, and equitable access to critical goods. Trust-aware RL is not a silver bullet but a design paradigm that acknowledges that in highly interconnected, decentralized production systems, algorithmic efficiency cannot be divorced from social embeddedness. Its successful implementation will require not only technical rigor but also a deep appreciation of the organizational, economic, and ethical dimensions of inter-firm trust.

7. Conclusion

Dynamic capacity sharing in decentralized supply networks represents a grand challenge at the intersection of operations management, artificial intelligence, and governance. This paper has argued that integrating computational trust models into the reward and state representation of multi-agent reinforcement learning constitutes a promising pathway to overcome the coordination failures that have long hindered lateral capacity exchange. By conceptualizing trust as a dynamic, learnable asset that simultaneously enables efficient resource allocation and disciplines opportunistic behavior, the proposed mechanisms encourage agents to internalize the long-term network consequences of their actions. The hybrid architecture combining local RL agents, a shared trust ledger, and a matchmaking coordination node

provides a concrete blueprint for implementation that respects the autonomy and confidentiality requirements of independent firms while enabling systemic coordination. We examined the multi-dimensional trade-offs regarding exploration, fairness, and robustness, showing that trust-aware design can mitigate risks of cascading shortages, reputation manipulation, and entrenched inequality. The deployment pathway is contingent on advances in digital twin technology, federated learning, and regulatory frameworks for algorithmic supply chain decisions. As supply chains transition from linear chains to digital ecosystems, trust-aware reinforcement learning mechanisms will likely become essential instruments for building the allegiant, resilient networks that global commerce demands.

References

1. Choi, T. Y., Dooley, K. J., & Rungtusanatham, M. (2001). Supply networks and complex adaptive systems: control versus emergence. Journal of Operations Management, 19(3), 351–366.

2. Lee, H. L., Padmanabhan, V., & Whang, S. (1997). Information distortion in a supply chain: The bullwhip effect. Management Science, 43(4), 546–558.

3. Cachon, G. P., & Lariviere, M. A. (2001). Contracting to assure supply: How to share demand forecasts in a supply chain. Management Science, 47(5), 629–646.

4. Simchi-Levi, D., Kaminsky, P., & Simchi-Levi, E. (2008). Designing and managing the supply chain: Concepts, strategies, and case studies (3rd ed.). McGraw-Hill.

5. Tang, C. S. (2006). Perspectives in supply chain risk management. International Journal of Production Economics, 103(2), 451–488.

6. Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: Extending the supply chain resilience angles towards survivability. International Journal of Production Research, 58(10), 2904–2915.

7. Oroojlooyjadid, A., Nazari, M., Snyder, L. V., & Takáč, M. (2020). A deep Q-network for the beer game: Deep reinforcement learning for inventory management. European Journal of Operational Research, 285(2), 594–609.

8. Boute, R. N., Gijsbrechts, J., van Jaarsveld, W., & Vanvuchelen, N. (2022). Deep reinforcement learning for inventory control: A roadmap. European Journal of Operational Research, 298(2), 401–421.

9. Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction (2nd ed.). MIT Press.

10. Ramchurn, S. D., Huynh, T. D., & Jennings, N. R. (2004). Trust in multi-agent systems. The Knowledge Engineering Review, 19(1), 1–25.

11. Sabater, J., & Sierra, C. (2005). Review on computational trust and reputation models. Artificial Intelligence Review, 24(1), 33–60.

12. Zhang, C., & Shah, J. A. (2014). Fairness in multi-agent sequential decision-making. In Advances in Neural Information Processing Systems (Vol. 27).

13. Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., ... & Petersen, S. (2015). Human-level control through deep reinforcement learning. Nature, 518(7540), 529–533.

14. Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., van den Driessche, G., ... & Dieleman, S. (2017). Mastering chess and shogi by self-play with a general reinforcement learning algorithm. arXiv preprint arXiv:1712.01815.

15. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135.

16. Nowak, M. A., & Sigmund, K. (2005). Evolution of indirect reciprocity. Nature, 437(7063), 1291–1298.

17. Hu, X., & Caldentey, R. (2023). Trust and reciprocity in firms' capacity sharing. Manufacturing & Service Operations Management, 25(4), 1436-1450.

18. Chen, F. (2003). Information sharing and supply chain coordination. In A. G. de Kok & S. C. Graves (Eds.), Handbooks in operations research and management science: Supply chain management (Vol. 11, pp. 341–421). Elsevier.

19. Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C. (2019). Digital twin in industry: State-of-the-art. IEEE Transactions on Industrial Informatics, 15(4), 2405–2415.

20. Dwork, C., Hardt, M., Pitassi, T., Reingold, O., & Zemel, R. (2012). Fairness through awareness. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (pp. 214–226). ACM.

21. Rahwan, I., Cebrian, M., Obradovich, N., Bongard, J., Bonnefon, J. F., Breazeal, C., ... & Wellman, M. (2019). Machine behaviour. Nature, 568(7753), 477–486.

22. Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. International Journal of Production Research, 57(3), 829–846.

23. European Commission. (2020). Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). COM(2020) 108 final.