Triple-Network Symbiosis: How AI Enables Cross-Domain Collaboration Among Business, Finance, and Cybersecurity (2022-2026)

Abstract

Artificial intelligence (AI) has reshaped the interaction paradigm between digital commerce, finance, and cybersecurity, forming a mutually dependent triple-network symbiosis: the value network (creating and distributing cross-domain economic value), the responsibility network (allocating risk and compliance obligations), and the governance network (establishing rules for cross-domain interaction). This review synthesizes 7 key studies (2022-2026) to unpack the operational logic of each network and their interdependent relationships: the value network is driven by AI-enabled resource integration (e.g., multi-tenant infrastructure, LSTM prediction); the responsibility network is anchored by AI-powered risk sharing (e.g., privacy-enhancing technologies, multi-agent risk balancing); the governance network is guaranteed by AI-aided rule making (e.g., modular compliance frameworks, incentive systems). Findings reveal that: the three networks are mutually reinforcing—value creation requires responsibility allocation to mitigate risks, and governance rules constrain and guide both value distribution and responsibility sharing; SMEs are the critical nodes connecting the triple networks; and modular AI architectures and privacy technologies are the core enablers of network symbiosis. This framework provides a new perspective on cross-domain AI collaboration, offering guidance for researchers, practitioners, and policymakers to build sustainable and inclusive cross-sector ecosystems.

1 Introduction

The cross-domain integration of digital commerce, finance, and cybersecurity is no longer a simple technical combination but a systemic network reconstruction driven by AI [1][4][7]. For example, Yi’s [2] multi-tenant AI infrastructure for SMEs (digital commerce) not only creates value by expanding market access (value network) but also imposes data privacy responsibilities on platform providers (responsibility network) and requires governance rules for incentive distribution (governance network); Zhou’s [5] MARL-based vulnerability planning (cybersecurity) balances security risks and financial costs (responsibility network) to protect business value creation (value network) while relying on governance rules for stakeholder coordination (governance network); Li and Liu’s [6] LSTM-based portfolio optimization (finance) enhances investment value (value network) but requires cybersecurity safeguards (responsibility network) and compliance with financial regulations (governance network). However, existing research often focuses on single-network value creation [2][6] or isolated responsibility allocation [4][5], overlooking the symbiotic relationship between value, responsibility, and governance [1][3][7]. This review addresses this gap by synthesizing 7 key studies to construct the triple-network symbiosis framework, explaining how AI enables the coordinated operation of the three networks and drives sustainable cross-domain collaboration.

2 The Triple-Network Symbiosis Framework: Value, Responsibility, Governance

2.1 Value Network: AI-Enabled Cross-Domain Resource Integration and Value Co-Creation

The value network is the core of the triple-network symbiosis, consisting of cross-domain resource flows (data, technology, capital) and value distribution mechanisms enabled by AI. Its core logic is to break down domain boundaries through AI, integrate fragmented resources, and create new value that exceeds the sum of single-domain outputs.

In digital commerce, the value network revolves around **inclusive resource access** and **privacy-compliant value extraction**. Yi [1]'s federated learning framework integrates cross-channel user data resources (without exposing raw data) to create value for retailers (accurate marketing insights), creators (monetization opportunities), and users (personalized experiences) [7]; Yi [2]'s multi-tenant infrastructure integrates advanced AI capabilities (PETs, marketing algorithms) into a shared resource pool, enabling SMEs to access high-value technical resources at low cost—turning resource constraints into value creation opportunities. The value distribution mechanism here is based on modular pricing and incentive systems: SMEs pay for only the AI modules they use [2], while platforms and creators share revenue generated by improved marketing efficiency [1][7].

In finance, the value network focuses on **data-driven investment efficiency** and **inclusive ESG value**. Li and Liu [6]'s LSTM model integrates financial time-series data resources (market trends, asset prices) to create value for investors (robust portfolio optimization, risk reduction) and financial institutions (improved service competitiveness); Liu [3]'s ESG AI tools integrate fragmented ESG data (energy consumption, carbon emissions, social responsibility) into actionable insights, enabling SMEs to create ESG value (improved ratings) that was previously only accessible to large enterprises. The value distribution mechanism is characterized by win-win outcomes: investors gain higher returns, SMEs access sustainable finance resources, and regulators achieve carbon reduction and social responsibility goals [3].

In cybersecurity, the value network centers on **risk-reducing value** and **cost-saving value**. Zhou [5]'s MARL-based M-VP2 integrates risk data (vulnerability severity, threat intelligence), financial data (patch costs, potential loss), and business data (operational impact) to create value for IT teams (effective risk mitigation), business units (cost savings), and security vendors (targeted product recommendations); Zhou [4]'s hybrid SAST-DAST-SCA-IAST framework integrates multi-dimensional testing resources to create value for organizations by reducing false positives (improving security efficiency) and avoiding unnecessary business disruptions (saving operational costs). The value here is indirect but critical: cybersecurity no longer 只是 a cost center but a value enabler that protects the value created by digital commerce and finance [4][5].

2.2 Responsibility Network: AI-Powered Cross-Domain Risk Sharing and Compliance Allocation

The responsibility network is the guarantee of the triple-network symbiosis, defining the risk-taking obligations and compliance responsibilities of stakeholders across digital commerce, finance, and cybersecurity. AI plays a key role in identifying cross-domain risks, allocating responsibility reasonably, and ensuring compliance with relevant regulations.

In digital commerce, the core responsibilities are **privacy protection** and **inclusive service obligations**. Yi [1][7]’s PETs (federated learning, zero-knowledge verification) not only enable privacy-compliant data use but also clarify responsibility allocation: platform providers are responsible for technical security (ensuring data is not leaked during federated training) [1], retailers are responsible for legal use of marketing insights (not engaging in discriminatory targeting) [7], and multi-tenant infrastructure providers are responsible for SME support (ensuring accessible technical guidance) [2]. This responsibility allocation avoids the "privacy paradox" where value creation comes at the cost of user privacy, and ensures that SMEs are not excluded due to lack of compliance capabilities [2].

In finance, the key responsibilities are **investment risk disclosure** and **ESG compliance guidance**. Li and Liu [6]’s LSTM model includes risk prediction modules that clarify the responsibility of financial institutions: disclosing the limitations of AI predictions to investors (not guaranteeing absolute returns) and providing transparent risk assessment criteria; Liu [3]’s ESG AI tools impose responsibilities on financial institutions and tool providers: guiding SMEs to make genuine ESG improvements (not greenwashing) and ensuring the accuracy and integrity of ESG data [3]. This responsibility allocation prevents excessive reliance on AI and ensures that ESG value creation is authentic and sustainable.

In cybersecurity, the core responsibilities are **risk assessment accuracy** and **stakeholder coordination**. Zhou [5]’s MARL-based framework assigns responsibilities to IT teams (providing accurate vulnerability data), business units (disclosing operational impact information), and security vendors (ensuring product effectiveness); Zhou [4]’s hybrid framework requires cybersecurity teams to take responsibility for aligning technical risk assessments with business objectives (not overemphasizing trivial vulnerabilities) [4]. This responsibility allocation avoids the "security silo" problem where cybersecurity decisions are made without considering business and financial impacts, and ensures that risk management is a shared responsibility rather than the sole burden of IT teams [5].

Notably, the responsibility network is cross-domain: a data breach in digital commerce (violating privacy responsibilities) affects financial transactions and cybersecurity risk assessments [1][4]; inadequate ESG compliance in finance (greenwashing) undermines the value of digital commerce’s sustainable marketing [3][7]; poor risk assessment in cybersecurity (missing critical vulnerabilities) leads to financial losses and business disruption [5][6]. AI enables the identification and allocation of these cross-domain responsibilities through multi-dimensional data analysis and stakeholder modeling [5][7].

2.3 Governance Network: AI-Aided Cross-Domain Rule Making and Coordination

The governance network is the foundation of the triple-network symbiosis, consisting of formal rules (laws, regulations, industry standards) and informal norms (incentive mechanisms, coordination protocols) that guide the operation of the value and responsibility networks. AI aids in formulating flexible, efficient, and inclusive governance rules, and ensures their effective implementation.

Formal governance rules are refined and adapted through AI. In privacy governance, Yi [1][7]'s PETs embed compliance with GDPR, CCPA, and other regulations into technical design (compliance-by-design), forming cross-domain privacy governance rules that are compatible with multiple regulatory regimes—avoiding the problem of conflicting domain-specific regulations. In ESG governance, Liu [3]'s AI tools align with sustainable finance standards (e.g., EU Taxonomy) and SME resource constraints, forming governance rules that balance compliance requirements and practical feasibility—enabling SMEs to participate in ESG governance without being overwhelmed by complex regulations. In cybersecurity governance, Zhou [4][5]'s frameworks adopt industry security standards (e.g., ISO 27001) and integrate business and financial KPIs, forming governance rules that align technical security with organizational objectives—breaking the disconnect between cybersecurity governance and business governance.

Informal governance rules are optimized through AI-driven incentive and coordination mechanisms. Yi [2]'s multi-tenant infrastructure designs a reward-punishment incentive system: SMEs that comply with data privacy rules and actively improve ESG performance receive preferential pricing for AI modules [2][3]; platforms that provide high-quality technical support and data security guarantees gain higher user trust and market share [1]. Zhou [5]'s MARL-based framework establishes a stakeholder coordination protocol: IT teams, business units, and security vendors vote on vulnerability patch plans through AI agents, ensuring that governance decisions reflect the interests of all parties [5]. These informal rules complement formal regulations, improving the flexibility and adaptability of the governance network.

AI also enables the dynamic adjustment of governance rules. Through continuous monitoring of value network outcomes (e.g., SME adoption rates [2], investment returns [6]) and responsibility network implementation (e.g., privacy compliance violations [1], ESG greenwashing incidents [3]), AI identifies gaps in governance rules and proposes revisions—for example, adjusting incentive intensity based on SME compliance performance [2], or updating risk assessment criteria based on emerging cybersecurity threats [4]. This dynamic adjustment ensures that the governance network keeps pace with cross-domain collaboration and technological development.

2.4 Symbiotic Relationship Between the Three Networks

The triple networks operate in a mutually reinforcing symbiosis:

- Value network drives responsibility and governance: New value creation (e.g., cross-channel marketing insights [1], ESG data sharing [3]) brings new risks (privacy leakage, greenwashing), requiring the responsibility network to allocate obligations and the governance network to establish rules.
- Responsibility network safeguards value and governance: Reasonable responsibility allocation (e.g., platform privacy protection obligations [7], cybersecurity risk sharing [5]) reduces risk losses, protecting the value created by the value network, and ensures that governance rules are implemented in practice.

- Governance network guides value and responsibility: Clear governance rules (e.g., compliance-by-design technical standards [1], incentive mechanisms [2]) guide the value network to create inclusive and sustainable value, and ensure that the responsibility network allocates obligations fairly.

Breakdown in any network leads to symbiosis failure: A value network that ignores responsibility (e.g., privacy-violating marketing [1]) will lose user trust and face regulatory penalties; a responsibility network that is overly burdensome (e.g., excessive compliance requirements for SMEs [2]) will hinder value creation; a governance network that is rigid (e.g., one-size-fits-all security standards [4]) will fail to adapt to cross-domain needs.

3 Triple-Network Symbiosis Outcomes: Inclusive, Secure, and Sustainable Cross-Domain Ecosystems

3.1 Digital Commerce: Privacy-Respecting, SME-Inclusive Growth Ecosystem

The triple-network symbiosis enables digital commerce to form an ecosystem where value creation, privacy protection, and inclusive governance coexist. The value network (multi-tenant infrastructure [2], federated marketing tools [1]) provides SMEs with equal access to growth opportunities; the responsibility network (platform privacy obligations [7], retailer compliance responsibilities [1]) ensures that growth does not come at the cost of user privacy; the governance network (flexible incentive systems [2], compliance-by-design standards [1]) balances innovation and regulation. The outcome is a growth model where large enterprises and SMEs collaborate rather than compete, and users gain personalized experiences while retaining privacy control—driving long-term and sustainable sector development.

3.2 Finance: Efficient, Authentic, and Inclusive Sustainable Finance Ecosystem

Finance benefits from the triple-network symbiosis by building an ecosystem that integrates investment efficiency, ESG authenticity, and inclusive governance. The value network (LSTM portfolio optimization [6], SME ESG tools [3]) creates value for investors and small businesses; the responsibility network (financial institution risk disclosure [6], tool provider anti-greenwashing obligations [3]) ensures that value is authentic and not based on false data; the governance network (sustainable finance standards [3], flexible compliance rules [6]) guides capital flow to real sustainable projects. The outcome is a financial system where efficiency and sustainability are not mutually exclusive, and SMEs are not excluded from sustainable finance—promoting economic transformation and carbon reduction.

3.3 Cybersecurity: Proactive, Business-Aligned, and Collaborative Risk Management Ecosystem

Cybersecurity completes the triple-network symbiosis by forming an ecosystem that aligns risk management with value creation and shared responsibility. The value network (risk-cost balancing tools [5], integrated testing frameworks [4]) creates cost-saving and risk-reducing value; the responsibility network (multi-stakeholder risk sharing [5], IT team accuracy obligations [4]) ensures that risk management is not a single-team burden; the governance network (business-aligned security standards [4], stakeholder coordination protocols [5]) guides cybersecurity to support rather than hinder business and finance. The outcome is a cybersecurity ecosystem that is proactive, adaptive, and collaborative—protecting cross-domain value creation while minimizing operational disruption.

4 Practical Implications

4.1 For Researchers

Design AI with triple-network compatibility: Develop modular and flexible AI technologies that can support value creation [2][6], responsibility allocation [1][5], and governance implementation [4][7]; embed stakeholder modeling into AI design to ensure that the value network is inclusive [2][3], the responsibility network is fair [5], and the governance network is adaptive [1]; focus on cross-domain risk identification and mitigation to strengthen the link between the three networks [4][7].

4.2 For Practitioners

Build cross-domain network thinking: Digital commerce platforms should integrate responsibility allocation (privacy protection [7]) and governance mechanisms (incentive systems [2]) into value creation tools; financial institutions should align investment value creation (LSTM optimization [6]) with ESG responsibility (anti-greenwashing [3]) and comply with cross-domain governance rules; cybersecurity teams should design risk management solutions that support value creation (business-aligned risk prioritization [5]) and clarify responsibility sharing (multi-stakeholder coordination [4]). SMEs should leverage AI tools to participate in all three networks (access value resources [2], fulfill compliance responsibilities [3], and benefit from governance incentives [2]).

4.3 For Policymakers

Promote triple-network coordinated governance: Formulate cross-domain regulatory frameworks that balance value creation (encourage AI innovation [1][6]) and responsibility fulfillment (strengthen privacy and security supervision [4][7]); support inclusive governance tools (fund multi-tenant infrastructure [2], develop SME-friendly ESG standards [3]) to ensure that SMEs can participate in the triple networks; establish dynamic governance mechanisms (use AI to monitor network operation [5], adjust rules based on implementation outcomes [1]) to adapt to technological and market changes.

5 Conclusion

This review synthesizes 7 key studies to propose the triple-network symbiosis framework (value, responsibility, governance) for AI-enabled cross-domain collaboration among digital commerce, finance, and cybersecurity. The framework reveals that sustainable cross-domain integration is not just about technical connection or value creation but about the coordinated operation of three mutually reinforcing networks: AI enables the value network to integrate resources and create inclusive value; supports the responsibility network to allocate risks and compliance obligations fairly; and aids the governance network to establish flexible and adaptive rules. SMEs are the critical nodes connecting the three networks, while modular AI architectures and privacy-enhancing technologies are the core enablers. By understanding this triple-network symbiosis, researchers, practitioners, and policymakers can unlock the full potential of AI to build an inclusive, secure, and sustainable cross-domain ecosystem—driving mutual prosperity across business, finance, and cybersecurity.

References

[1] Yi, X. (2026). A Federated and Differentially Private Incentive–Marketing Framework for Privacy-Preserving Cross-Channel Measurement in AI-Powered Digital Commerce.

[2] Yi, X. (2026). Trusted AI Commercialization Infrastructure for SMBs: A Unified Multi-Tenant Architecture Integrating Incentive Systems, Content Governance, and Standardized Recommendation APIs.

[3] Liu, T. (2022, December). Financial Constraint'Impact on Firms' ESG Rating Based on Chinese Stock Market. In *2022 4th International Conference on Economic Management and Cultural Industry (ICEMCI 2022)* (pp. 1085-1095). Atlantis Press.

[4] Zhou, D. (2026). AI-Driven Hybrid SAST–DAST–SCA–IAST Framework for Risk-Based Vulnerability Prioritization in Microservice Architectures.

[5] Zhou, D. (2025, December). M-VP2: Microservice-Oriented Vulnerability Patch Planning-A Cost-Aware Approach using Multi-Agent Reinforcement Learning. In *2025 5th International Conference on Computer, Internet of Things and Control Engineering (CITCE)* (pp. 248-254). IEEE.

[6] Li, H., & Liu, T. (2023). Portfolio optimization based on the LSTM forecasting model. In *Proceedings of the 2nd International Conference on Financial Technology and Business Analysis* (Vol. 48, No. 1, pp. 97-106).

[7] Yi, X. (2026). Privacy-Enhanced Ad Targeting for Social E-Commerce: A Federated Learning Framework with Zero-Knowledge Verification for Creator Monetization. *Frontiers in Business and Finance*, 3(1), 102-113.