

Article

Technology-Enabled Traceability and Sustainable Governance: An Evolutionary Game Perspective on Multi-Stakeholder Collaboration

Wei Xun ¹, Xuemei Du ^{1,*} , Meiling Li ¹, Jianfeng Lu ² and Xinyi Bao ¹

¹ School of Economics and Management, Tongji University, Shanghai 200092, China; xxbzka@163.com (W.X.); lml_199905@163.com (M.L.); 2431151@tongji.edu.cn (X.B.)

² CIMS Research Center, College of Electronic and Information Engineering, Tongji University, Shanghai 201804, China; lujianfeng@tongji.edu.cn

* Correspondence: duxuemei@tongji.edu.cn

Abstract

Ensuring product quality and safety is fundamental to sustainable production and consumption. With the rapid advancement of digital technologies such as blockchain and big data, quality and safety traceability systems have become essential tools to enhance transparency, accountability, and governance efficiency across supply chains. The sustainable functioning of these systems, however, depends on the coordinated actions of multiple stakeholders—including governments, enterprises, consumers, and industry associations—making the study of technological and institutional interactions particularly significant. This paper extends evolutionary game theory to the context of technology-enabled sustainable governance by constructing a tripartite game model involving government regulators, traceability enterprises, and consumers from both technological and institutional perspectives. Unlike existing studies, which focused solely on government regulation, this research explicitly incorporates the role of industry associations in shaping stakeholder behavior and integrates consumer rights protection mechanisms as well as the adoption of emerging technologies such as blockchain into the model. Analytical derivations and MATLAB-based simulations reveal that strengthening reward–penalty mechanisms and improving digital maturity significantly enhance enterprises’ incentives for truthful information disclosure; consumers’ verification and reporting behaviors generate bottom-up pressure that encourages stricter governmental supervision; and active participation of industry associations helps share regulatory costs and stabilize cooperative equilibria. These findings suggest that combining technological innovation with institutional collaboration not only improves transparency and strengthens consumer trust but also reshapes the incentive structures underlying traceability governance. The study provides new insights into how multi-stakeholder coordination and technological adoption jointly foster transparent, credible, and resilient traceability systems, offering practical implications for advancing digital transformation and co-governance in sustainable supply chains.

Keywords: digital technologies; traceability; evolutionary game; industry association; sustainable governance



Academic Editor: Giada La Scalia

Received: 25 October 2025

Revised: 28 November 2025

Accepted: 29 November 2025

Published: 4 December 2025

Citation: Xun, W.; Du, X.; Li, M.; Lu, J.; Bao, X. Technology-Enabled Traceability and Sustainable Governance: An Evolutionary Game Perspective on Multi-Stakeholder Collaboration. *Sustainability* **2025**, *17*, 10855. <https://doi.org/10.3390/su172310855>

Copyright: © 2025 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article

distributed under the terms and

conditions of the Creative Commons

Attribution (CC BY) license

(<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Product quality and safety are fundamental pillars of sustainable economic and social development. Despite continuous improvements in regulatory frameworks and enforce-

ment capacity, recurrent incidents in food and related sectors still threaten public health, disrupt markets, and erode consumer confidence [1]. Recent events—such as the 2018 nationwide foodborne illness outbreak involving contaminated romaine lettuce in the United States [2], and the 2017–2018 listeriosis outbreak in South Africa [3] associated with processed meat products—highlight persistent systemic weaknesses in supervision and traceability mechanisms, including inadequate source control, insufficient inspection, and opaque logistics management. Empirical studies further indicate that recurring problems such as excessive pesticide residues, illegal additives, and counterfeit products are driven by structural factors, including firms' cost-cutting incentives, moral hazard, and limited regulatory resources, which jointly hinder the establishment of credible quality assurance and traceability systems [4]. Against this backdrop, emerging digital technologies such as blockchain, big data analytics, and artificial intelligence offer new tools for building transparent and trustworthy traceability systems. However, technological capacity alone does not automatically translate into effective governance: actual outcomes depend on whether government regulators, firms, consumers, and industry associations can form incentive-compatible and clearly defined collaborative governance arrangements. Developing a robust traceability framework that ensures data integrity and accountability along the supply chain has thus become essential for rebuilding consumer trust, strengthening risk prevention, and advancing sustainable quality governance.

At the policy level, traceability has become a core issue in supply chain regulation, and many jurisdictions are embedding digital and collaborative requirements into their institutional designs. More recently, the EU introduced the Digital Product Passport (DPP) [5] as a mandatory tool to enhance lifecycle-wide transparency. It expands digital traceability beyond the food sector and establishes it as a binding regulatory requirement. In the United States, the Food and Drug Administration (FDA) issued the Food Traceability Final Rule [6] to mandate digital record-keeping at critical tracking events for high-risk foods, enabling faster identification and recall. In China, the Outline for Building a Quality Power (2023) [7] calls for traceability systems for key products, while subsequent 2025 policies [8,9] emphasize security auditing and digital traceability mechanisms supported by technologies such as digital fingerprints, digital watermarks, and blockchain, reinforcing the shift from ex post checks to full-lifecycle online monitoring. At the same time, FAO and WHO guidance on the digitalization of national food-control systems highlights that, amid increasingly complex cross-border supply chains, information opacity and fragmented oversight pose global challenges that require digital infrastructures to strengthen risk identification and regulatory coordination [10]. Taken together, these initiatives reflect a broad policy consensus: reliable, verifiable, and digitally enabled traceability mechanisms are now indispensable for transparency, accountability, and progress toward the Sustainable Development Goals.

On the technological side, traceability systems have evolved from basic identification to intelligent data capture and integrated platform governance [11]. Early systems relied on barcodes and QR codes to record product origins and track key nodes [12]. Subsequently, automatic identification and data capture (AIDC) technologies, such as radio frequency identification (RFID) [13] and near-field communication (NFC) [14], enabled item-level tracking and cold-chain temperature monitoring across supply chains. Advances in sensors, wireless communication, and positioning technologies have embedded these devices into Internet-of-Things (IoT) architectures [15], shifting static record-keeping toward continuous monitoring of variables such as temperature, humidity, and location. Building on this sensing layer, firms and regulators developed electronic traceability platforms that integrate data across production, warehousing, and logistics. Yet traditional architectures still face limitations, including data silos, difficulties in verifying information authenticity, and low cross-organizational coordination efficiency.

In recent years, sensing and recording infrastructures have increasingly integrated with new digital technologies, transforming traceability systems into digital foundations that support regulation, decision-making, and collaborative governance [16]. At the operational level, intelligent manufacturing has enhanced interconnection and automated decision-making, shifting quality management from *ex post* inspection to real-time perception, process control, and predictive warning. At the system level, cloud manufacturing coordinates distributed production resources through shared cloud platforms, generating inherent demand for transparent and efficient traceability. Within this transformation, IoT, blockchain, and big data have become core technologies: IoT devices generate fine-grained, time-stamped data; blockchain provides tamper-resistant, auditable ledgers; and big data analytics integrate heterogeneous information for risk identification and regulatory optimization. For example, Zheng et al. [15] designed an RFID–IoT–big data traceability system that records production, processing, inspection, and logistics events on a distributed ledger, enabling verification of product origins and responsible entities. Feng et al. [17] proposed a blockchain architecture framework and applicability flowchart to support traceability development, allowing consumers to obtain traceability information through code scanning and enhancing supply-chain transparency. Although scalability and privacy concerns remain [18], blockchain-based supply chain systems show substantial potential for enhancing data integrity and sustainability communication [19]. In parallel, regulators and platform operators increasingly integrate inspection records, firm-reported data, transactions, and complaints to build big data–based early-warning systems that identify high-risk products and firms and enhance regulatory targeting. Recent studies demonstrate that integrating multisource heterogeneous data with algorithmic models enables accurate identification and early warning of hazards such as pesticide residues and biopharmaceutical risks.

Despite technological progress, sustainable traceability operation continues to face behavioral and governance challenges. Digital and cloud-based production models facilitate resource sharing but also blur regulatory boundaries and increase governance complexity. Traceability reliability still depends heavily on firms' voluntary participation and self-discipline, which are constrained by high construction and maintenance costs and low short-term returns. Consumers' awareness, verification willingness, and trust levels also vary across regions and sectors. Industry associations [20] increasingly promote standardization, collective supervision, and data sharing, yet their involvement remains fragmented and unstable. These factors indicate that effective traceability governance is not merely a technical issue but a behavioral and institutional challenge. Understanding how stakeholders adjust strategies under evolving technological and regulatory conditions is thus essential for building transparent and sustainable traceability ecosystems.

Against this backdrop, a growing body of research has examined the behavior and incentives of governments, enterprises, and consumers in quality and safety traceability. Existing studies highlight the central role of governmental intervention in reconciling conflicting interests between information suppliers and demanders, as consumer demand for transparency often conflicts with producers' incentives to conceal operational information [21]. Empirical evidence shows that stronger penalties can deter non-compliance [22], that consumer preference for traceable agricultural products can pressure firms to adopt traceability systems [23], and that although implementation increases costs, it can enhance competitiveness by improving risk management and information reliability [24,25]. Governmental financial and technical support has also been shown to increase participation among producers [26,27]. Methodologically, game-theoretic models are widely used to analyze strategic interactions among stakeholders in food and product traceability [28–30]. Most existing work focuses on bilateral relationships—such as government–enterprise, consumer–enterprise, or farmer–enterprise interactions—to examine incentive mechanisms

and participation behavior. For example, Song et al. [31] model traceability information disclosure between governments and food enterprises, emphasizing the role of public oversight in deterring false reporting; Wang et al. [32] study farmers' and enterprises' willingness to participate under different consumer preferences. Tu [33] extends this framework to a three-party model involving enterprises, regulators, and the public. Zheng et al. [34] established a tripartite game model that reveals the key role of the government's reward and punishment mechanisms in promoting the adoption of blockchain traceability. Cui et al. [35] construct an evolutionary game model involving producers, supermarkets, and e-commerce platforms and analyze how the conversion of traceability costs and benefits and spillover effects dynamically shape strategy choices in dual-channel supply chains. More recent studies incorporate digital platforms and data-sharing mechanisms [36]. Zhao et al. [37] examine stakeholder decisions on agricultural data platforms under information asymmetry. Cao et al. [38] emphasize that sustainable blockchain adoption requires integration of technological, governance, and trust dimensions.

Nevertheless, existing research remains limited in two respects. First, few studies systematically integrate the institutional influence of industry associations and the role of digital technologies into multi-agent governance models for traceability. Second, the feedback mechanisms through which new technologies reshape information asymmetry, regulatory costs, and public trust—and thereby alter stakeholder behavior—remain underexplored. While recent applied studies show that blockchain, IoT, and big data can enhance transparency and accountability [15,39], they also highlight that technological effects depend critically on alignment with governance structures and incentive systems.

Building on these insights, this study adopts a dual perspective integrating technological application with multi-stakeholder governance to examine the sustainable operation of product quality traceability systems. The main contributions are threefold. First, we develop a tripartite evolutionary game model involving government regulators, traceability enterprises, and consumers as core strategic players, and explicitly embed the institutional influence of industry associations as an environmental intermediary rather than an independent strategic agent, thereby addressing the narrow stakeholder scope and the limited treatment of institutional intermediaries in much of the existing literature. Second, to maintain clarity and interpretability, we focus on two representative digital traceability technologies—blockchain and big data—that are widely adopted in practice and directly linked to information credibility and regulatory efficiency, and examine how changes in their maturity adjust payoff structures and reshape the evolutionary trajectories of stakeholder strategies, offering a new perspective on technology-driven governance mechanisms. Third, using numerical simulations, we analyze the evolutionary paths of stakeholder strategies under different policy tools, incentive schemes, and technology-maturity levels, and derive targeted policy insights for building credible, transparent, and sustainable product quality traceability systems. The remainder of the paper is structured as follows: Section 2 presents the model assumptions and construction; Section 3 analyzes the evolutionary dynamics; Section 4 reports the simulation results and discussion; and Section 5 concludes with key findings and policy recommendations.

2. Methods Development

2.1. Model Framework and Participants

Product quality and safety traceability are inherently a systems-engineering task shaped by structural and technological constraints. End-to-end traceability spans production, processing, logistics, and consumption, generating heterogeneous data across multiple platforms. Achieving verifiable chain-wide transparency requires interoperable records and governance mechanisms that both constrain key behaviors *ex ante* and enable reliable

verification *ex post*—demands that cannot be met by any single technology or governance actor. From the perspective of digital architecture, traceability systems can be broadly understood as comprising three functional layers: perception, responsible for front-end data acquisition (e.g., RFID, NFC, environmental sensors); analytics, which processes and analyzes heterogeneous information; and application/governance, which supports rule enforcement, responsibility attribution, and collaborative oversight. Although modern systems employ a wide range of technologies—such as AI, machine learning, cloud computing, and sensor networks—their governance implications differ substantially. Perception- and analytics-layer technologies strengthen monitoring and risk detection, but do not directly alter the incentive structures or strategic interactions among regulators, enterprises, and consumers.

In contrast, blockchain and big data are embedded in the governance and core analytics layers and directly reshape mechanisms critical to evolutionary behavior. Blockchain ensures immutability and auditability through distributed ledgers, enhancing information credibility and increasing the cost of dishonest behavior; real-world pilots have shown that tamper-resistant records significantly support trust and accountability. Big data analytics integrates multisource supervisory information to detect risk patterns, reduce information asymmetry, and improve regulatory targeting. By enabling differentiated supervision, joint rewards and penalties, and enhanced consumer transparency, these technologies directly influence payoff structures and strategic stability. Given their direct impact on information integrity, regulatory efficiency, and behavioral incentives, blockchain and big data are incorporated as the core technological variables in the evolutionary game model developed in this study, ensuring theoretical clarity and explanatory strength.

Based on these features, this study considers the quality and safety traceability system as operating within a blockchain–big data environment. The overall framework follows a six-layer architecture (Figure 1):

1. Data acquisition layer: Collects life-cycle information from suppliers, manufacturers, third-party logistics providers, distributors, retailers, and consumers.
2. Data processing layer: Formats, validates, and cleans raw data, attaching timestamps and hashes before on-chain storage.
3. Network layer: Manages secure interconnection through access control, peer-to-peer networking, and identity authentication mechanisms.
4. Consensus layer: Uses a membership-based mechanism (e.g., Delegated Proof of Stake (DPoS)/Proof of Stake (PoS)) jointly governed by public authorities and authorized institutions to manage participant admission and maintain system integrity.
5. Contract layer: Encodes regulatory policies, legal frameworks, and industry standards as smart contracts, transforming institutional rules into enforceable digital protocols.
6. Application layer: Provides query and service portals for regulators, enterprises, consumers, and industry associations, supporting multi-channel access via websites, mobile applications, or terminals.

This architecture provides the technical and institutional foundation for the behavioral assumptions and incentive mechanisms formalized in the subsequent model. The technology adoption level (θ) reflects the degree to which blockchain anchoring and big data analytics are implemented, while the association participation degree (β) captures the engagement of industry associations through the consensus and contract layers. These parameters jointly affect supervision costs, detection probabilities, and credibility gains, which are incorporated as key variables in the model's payoff functions. These technological and institutional foundations not only support data sharing and oversight but also shape the behavioral logic of key actors in the traceability system. The interaction between digital infrastructure and institutional arrangements determines how stakeholders—governments,

enterprises, and consumers—form strategies under varying levels of information transparency and regulatory capacity.

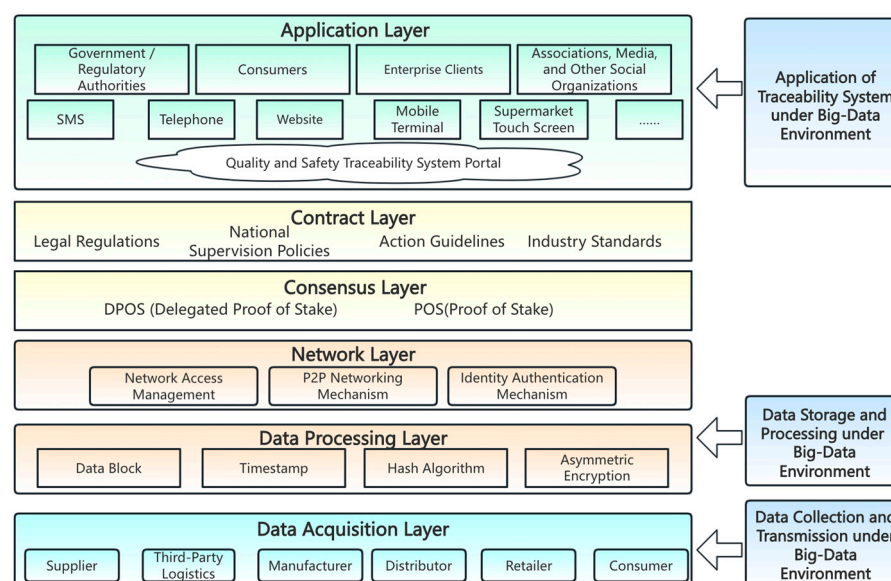


Figure 1. Six-layer framework for a blockchain- and big data-enabled quality and safety traceability system.

Within the traceability system, the primary stakeholders include government regulators, traceability enterprises, consumers, and industry associations. Among these actors, government authorities hold a central regulatory position. They are responsible for improving traceability-related laws and standards, promoting the adoption of emerging digital technologies, safeguarding consumer rights, and implementing reward–penalty mechanisms for enterprises. However, due to information asymmetry and administrative limitations, regulatory enforcement may not always be strict. As a result, the effective functioning of the traceability system also relies on the participation of enterprises, consumers, and industry associations. Traceability enterprises are defined as firms that comply with product quality and safety requirements, record key information throughout the production and circulation processes using digital means, and disclose relevant information through product certificates, packaging, or official traceability platforms. Their compliance behavior constitutes the core supply of traceability information and directly affects the system’s overall credibility. Consumers represent the demand-side actors and form an essential bottom-up supervisory force. Behaviors such as verifying product information, filing complaints, and engaging in public reporting shape firms’ reputational payoffs and may trigger regulatory responses. In reality, consumers’ willingness to verify and their trust levels vary across regions and product categories and are influenced by perceived risk, information accessibility, and digital literacy. In the model, consumers choose between active verification and passive acceptance; their decisions affect both enterprise incentives and the enforcement intensity adopted by regulators.

Industry associations serve as institutional intermediaries linking governments and enterprises. Through their dual functions of coordination and self-regulation, they help disseminate standards, support public regulators in monitoring industry behavior, reduce supervision costs, and encourage compliance among member firms. Evidence from China’s recent traceability initiatives shows that industry associations increasingly play a “support-and-constrain” role—supporting regulatory oversight while shaping enterprises’ normative and reputational incentives. Reflecting this institutional relevance, the present study incorporates industry associations not as independent strategic actors but as environmental

parameters that modify the payoff structures and influence the behavioral tendencies of governments and enterprises.

Accordingly, this study develops a $2 \times 2 \times 2$ tripartite evolutionary game model among government regulators, traceability enterprises, and consumers (Figure 2), while the institutional effects of industry associations are embedded as environmental parameters that shape incentive mechanisms and strategic evolution. The model analyzes the evolutionary stability and convergence of the three actors' strategies under different behavioral scenarios, revealing the mechanisms through which a dynamic equilibrium is formed in the quality and safety traceability system.

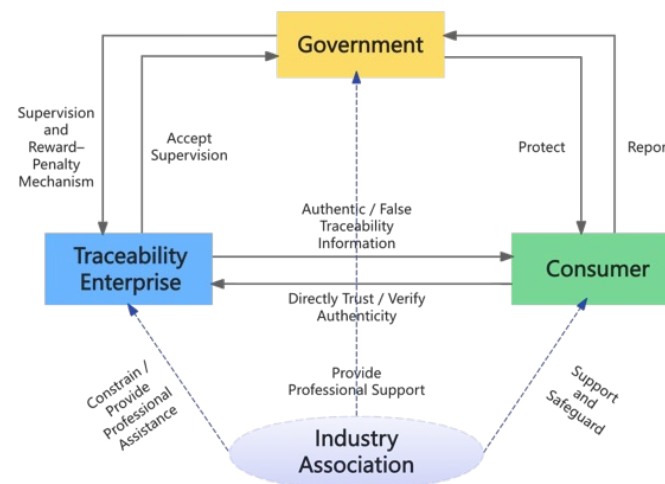


Figure 2. Tripartite game model of government regulators, traceability enterprises, and consumers.

2.2. Model Assumptions

In order to translate the above governance and technological architecture into an analyzable framework, this subsection sets out the behavioral assumptions and payoff structure underlying the tripartite evolutionary game. Building on the preceding discussion, the following assumptions specify the strategy sets of the three core agents, define the key cost–benefit parameters, and describe how the adoption of blockchain and big data technologies, as well as the participation of industry associations, are incorporated into the model.

Assumption 1. This study models the behavioral interactions among three principal agents in the quality and safety traceability system—government regulators (G), traceability enterprises (E), and consumers (C)—within an evolutionary game framework. All agents are assumed to be boundedly rational and adjust their strategies through adaptive learning to maximize expected payoffs. Industry associations influence the system as an exogenous institutional factor, shaping the strategic tendencies of governments and enterprises without directly participating in the game. Government regulators, as the rule setters and supervisory authorities, determine the level of regulatory enforcement, choosing between strict regulation and lenient regulation, denoted by the strategy set $S_g = \{\text{strict regulation}, \text{lenient regulation}\}$. Traceability enterprises decide whether to disclose truthful information or falsified information, with the strategy set $S_e = \{\text{share truthful information}, \text{share falsified information}\}$. Consumers purchasing products with traceability information choose either to verify information or to directly trust it, with the strategy set $S_c = \{\text{verify}, \text{direct trust}\}$.

Assumption 2. The three agents adopt mixed strategies. Government regulators choose strict regulation with probability x , and lenient regulation with probability $1 - x$. During disclosure, traceability enterprises share truthful information with probability y , and falsified information with probability $1 - y$. Consumers, after purchasing a product, choose to verify the provided information with probability z , or directly trust it with probability $1 - z$. Formally, $x, y, z \in [0, 1]$

represent the proportion of each population adopting a specific strategy at a given point in time. All participants are assumed to be risk-neutral and aim to maximize their expected utility through iterative interactions and adaptive learning.

Assumption 3. The costs associated with different strategies are as follows: For government regulators, the cost of strict supervision is denoted by C_{gh} , while that of lenient supervision is C_{gl} . For traceability enterprises, the cost of sharing truthful information—which requires greater investment in labor, materials, and financial resources—is C_{eh} , while the cost of sharing falsified information is C_{el} . For consumers, verifying enterprise-provided traceability information entails a verification cost C_1 , which reflects the time and effort required to conduct cross-checks. If consumers identify falsified information, a proportion α of them will choose to report the misconduct to government regulators. Each reporting action incurs an additional cost of C_2 for the individual consumer.

Assumption 4. The baseline revenue obtained by traceability enterprises from disclosing information is denoted by W . When enterprises share truthful traceability information, consumers obtain a positive utility U_c . Upon verification, consumers perceive that the government has implemented strict supervision, thereby enhancing public trust; as a result, government regulators gain reputational utility U_g . When consumers recognize the reliability of traceability information, their positive evaluations and word-of-mouth effects further enhance enterprises' market reputation, generating additional revenue P_1 . To encourage compliance, government regulators may introduce a reward subsidy U_e for enterprises that share truthful information under strict supervision. Industry associations are also assumed to play an active supportive role: with probability β , they participate in the quality traceability process by promoting exemplary enterprises and disseminating best practices. This engagement yields additional benefits P_2 for compliant enterprises and motivates broader participation across the industry. Hence, the combination of regulatory incentives and association advocacy strengthens the credibility of the entire traceability system.

Assumption 5. When traceability enterprises share falsified information, consumers experience a negative utility L_c . If government regulators adopt strict supervision, such misconduct is detected and punished with a fine F_e . Strict enforcement not only deters enterprises from future violations but also prevents consumers from using substandard products, sparing them verification and reporting costs while improving the government's reputation. Consequently, regulators obtain an additional reputational utility U_g . Moreover, when industry associations actively participate in quality traceability, they share part of the supervisory cost C_g with the government, even though the cost of strict supervision is higher $C_{gh} > C_g$. If regulators adopt a lenient approach, industry associations perceive their contributions as underrecognized and may reduce their support. Conversely, under strict supervision, associations are more likely to provide assistance and reinforcement. Moreover, associations can publicly expose or penalize enterprises that share falsified information by imposing a sanction F , serving as a warning to other members.

Assumption 6. When government regulators adopt a lenient strategy, enterprises sharing falsified information face no direct administrative penalty. In this case, consumers seeking to safeguard their interests may resort to public exposure through online and media platforms, leading to reputational damage and a decline in market revenue for the enterprise, represented as L_e . The enterprise also forfeits the baseline revenue W it would otherwise obtain from information disclosure. Meanwhile, the government suffers a reputational loss L_g , because ineffective supervision erodes public confidence. In contrast, if consumers directly trust the provided traceability information without verification, falsified data remain undiscovered, allowing enterprises to continue earning revenue W . This dynamic illustrates how weak regulatory enforcement and low consumer vigilance jointly undermine the credibility and sustainability of the quality traceability system.

Assumption 7. To address the pronounced heterogeneity in traceability systems across different regions and enterprises, the government is assumed to take the lead in establishing a comprehensive

traceability framework that integrates blockchain and big data technologies. Enterprises bear only a small portion of the corresponding technical costs, while the probability of adopting emerging technologies in the system is denoted by θ . At the enterprise level, θ represents the degree of blockchain and big data application within the firm's traceability practices. As demonstrated by Liu and Guo [40], the incorporation of blockchain-based technologies improves the authenticity and reliability of traceability information, regardless of enterprise behavior. Accordingly, even when enterprises disclose falsified information, the overall traceability system benefits from higher information credibility. The enhanced technological infrastructure thus yields additional consumer utility θU_c . After deducting the small portion of technical cost borne by enterprises, the incremental enterprise revenue is θP . Although the government undertakes the majority of technical costs, the introduction of blockchain and big data technologies also affects its supervision costs. Specifically, the costs of strict and lenient regulation are adjusted to $(1 + \theta)C_{gh}$ and $(1 + \theta)C_{gl}$, respectively. Nevertheless, the application of emerging technologies enhances regulatory efficiency, offsetting part of these expenditures. For consumers who actively participate in quality traceability, the government's leadership in constructing such a technology-enabled system increases their confidence in regulatory oversight. Consequently, this initiative enhances public trust and brings additional reputational utility of θU_g to government regulators.

According to the model assumptions outlined above, the related parameters and their definitions are presented in Table 1.

Table 1. Parameters and Definitions in the Tripartite Evolutionary Game Model.

Assumption	Role in Model	Key Parameters/Definitions
Assumption 1	Defines core actors and their strategy spaces; establishes the structural foundation of the evolutionary game.	Strategy sets: $S_g = \{\text{strict regulation, lenient regulation}\}$ $S_e = \{\text{share truthful information, share falsified information}\}$ $S_c = \{\text{verify, direct trust}\}$
Assumption 2	Introduces evolutionary dynamics; enables replicator equations to capture population-level strategic evolution.	x : strict regulation prob. y : truthful disclosure prob. z : verification prob.
Assumption 3	Specifies cost structures that shape agents' payoff functions and influence strategy convergence.	C_{gh} : Cost of strict supervision by government regulators C_{gl} : Cost of lenient supervision by government regulators C_{eh} : Cost for enterprises to disclose truthful traceability information C_{el} : Cost for enterprises to disclose falsified traceability information C_1 : Cost incurred by consumers for verifying traceability information provided by enterprises C_2 : Cost incurred by consumers for reporting falsified traceability information to regulators α : Probability that consumers who identify falsified information choose to report it to regulator
Assumption 4	Defines benefit mechanisms that reward truthful behavior and strengthen system credibility.	W : Baseline revenue obtained by enterprises from disclosing traceability information U_c : Positive utility gained by consumers from truthful traceability information U_g : Reputational utility gained by government regulators through strict supervision P_1 : Additional market revenue obtained by enterprises from consumer recognition of truthful information U_e : Reward subsidy granted by government regulators to enterprises for truthful disclosure P_2 : Additional benefits obtained by enterprises from recognition and promotion by industry associations β : Probability that industry associations actively participate in quality traceability

Table 1. Cont.

Assumption	Role in Model	Key Parameters/Definitions
Assumption 5	Establishes punishment mechanisms and cost-sharing rules that deter non-compliance.	L_c : Negative utility experienced by consumers from falsified traceability information F : Penalty imposed by industry associations on enterprises that disclose falsified information F_e : Penalty imposed by government regulators on enterprises for falsified disclosure C_g : Portion of strict supervision cost shared by industry associations
Assumption 6	Models the consequences of weak enforcement and consumer-led reputation pressure.	L_e : Market loss suffered by enterprises when consumers publicly expose falsified information L_g : Reputational loss suffered by government regulators due to lenient supervision
Assumption 7	Incorporates technological maturity into the payoff structure, shaping detection, credibility, and regulatory efficiency.	θ : Probability (or degree) of adopting blockchain and big data technologies in the traceability system

2.3. Model Construction

Building on the assumptions outlined above, the tripartite evolutionary game among government regulators (G), traceability enterprises (E), and consumers (C) is constructed. The interaction among the three players generates eight possible strategic combinations, each representing a distinct behavioral configuration within the quality and safety traceability system. These combinations form the basis for deriving the expected payoffs of all participants. The payoff outcomes corresponding to these strategic profiles are derived by integrating the parameters defined in Table 1, and the results are summarized in Table 2, which presents the payoff matrix of the tripartite game in the quality and safety traceability system. This matrix serves as the analytical foundation for the subsequent derivation of replicator dynamics and evolutionary stability analysis.

Table 2. Payoff matrix of the tripartite game in the quality safety traceability system.

Government Regulators	Traceability Enterprises	Consumers	
		Verification z	Direct Trust $1-z$
strict supervision x	truthful information y	$-(1+\theta)C_{gh} + \beta C_g - U_e + (1+\theta)U_g,$ $-C_{eh} + U_e + W + P_1 + \beta P_2 + \theta P,$ $-C_1 + (1+\theta)U_c$	$-(1+\theta)C_{gh} + \beta C_g - U_e,$ $-C_{eh} + U_e + W + \beta P_2 + \theta P,$ $(1+\theta)U_c$
	falsified information $1-y$	$-(1+\theta)C_{gh} + \beta C_g + (1+\theta)U_g + F_e,$ $-C_{el} - F_e - \beta F,$ θU_c	$-(1+\theta)C_{gh} + \beta C_g + F_e,$ $-C_{el} - F_e - \beta F,$ θU_c
lenient supervision $1-x$	truthful information y	$-(1+\theta)C_{gl} + (1+\theta)U_g,$ $-C_{eh} + W + P_1 + \beta P_2 + \theta P,$ $-C_1 + (1+\theta)U_c$	$-(1+\theta)C_{gl},$ $-C_{eh} + W + \beta P_2 + \theta P,$ $(1+\theta)U_c$
	falsified information $1-y$	$-(1+\theta)C_{gl} - \alpha L_g,$ $-C_{el} - \alpha L_e - \beta F,$ $-C_1 - \alpha C_2 + \theta U_c$	$-(1+\theta)C_{gl},$ $W - C_{el} - \beta F,$ $-L_c + \theta U_c$

3. Model Analysis

3.1. Stability Analysis of Government Regulators' Strategies

The expected payoff of government regulators when adopting the strict supervision strategy is:

$$E_x = -(1+\theta)C_{gh} + \beta C_g - yU_e + (1+\theta)zU_g + (1-y)F_e \quad (1)$$

The expected payoff of government regulators when adopting the lenient supervision strategy is:

$$E_{1-x} = -(1+\theta)C_{gl} + (1+\theta)yzU_g - \alpha(1-y)zL_g \quad (2)$$

The replicator dynamic equation for the evolution of the government's strategy is:

$$F(x) = \frac{dx}{dt} = x(E_x - \bar{E}) = x(1-x)\{\beta C_g - yU_e + (1+\theta)(C_{gl} - C_{gh}) + (1-y)[(1+\theta)zU_g + \alpha zL_g + F_e]\} \quad (3)$$

According to the stability theorem of differential equations, for the government to adopt a strict supervision strategy as an evolutionarily stable strategy (ESS), the following condition must hold: $F(x) = 0$ and $F'(x) < 0$.

$$F'(x) = (1-2x)\{(1+\theta)(C_{gl} - C_{gh}) + \beta C_g - yU_e + (1-y)[(1+\theta)zU_g + \alpha zL_g + F_e]\} \quad (4)$$

The corresponding threshold value z_0 , which determines the transition between strict and lenient supervision, is derived as:

$$z_0 = \frac{(1+\theta)(C_{gh} - C_{gl}) - \beta C_g + yU_e - (1-y)F_e}{(1-y)[(1+\theta)U_g + \alpha L_g]} \quad (5)$$

Proposition 1. When $z > z_0$, the ESS of the government regulator is strict supervision; when $z < z_0$, the ESS is lenient supervision; and when $z = z_0$, no stable strategy can be determined.

Proof. Let $H(z) = (1+\theta)(C_{gl} - C_{gh}) + \beta C_g - yU_e + (1-y)[(1+\theta)zU_g + \alpha zL_g + F_e]$. Since $\partial H(z)/\partial z > 0$, $H(z)$ is a monotonically increasing function with respect to z . When $z < z_0$, $H(z) < 0$, $F(x)|_{x=0} = 0$, and $F'(x)|_{x=1} < 0$; thus, the system has a stable equilibrium at $x = 0$, meaning lenient supervision is stable. When $z > z_0$, $H(z) > 0$, $F(x)|_{x=1} = 0$, and $F'(x)|_{x=1} < 0$; thus, a stable equilibrium exists at $x = 1$, indicating strict supervision is stable. When $z = z_0$, both equilibria are neutrally stable, and no unique stable strategy exists. $\square$

This result implies that an increase in consumers' verification probability strengthens the government's incentive to implement strict supervision. As consumers become more willing to verify traceability information, they effectively play a supervisory role within the quality and safety traceability system. To maintain its reputation and prevent reputational loss arising from potential product quality incidents, the government prefers strict supervision to demonstrate credibility and responsiveness to public concerns. Conversely, when consumers are more inclined to directly trust the traceability information without verification, the government tends to adopt a lenient supervision strategy to minimize regulatory costs.

The phase diagram of government regulators' strategic evolution is shown in Figure 3, where V_{x1} and V_{x0} represent the probabilities of adopting strict and lenient supervision strategies, respectively.

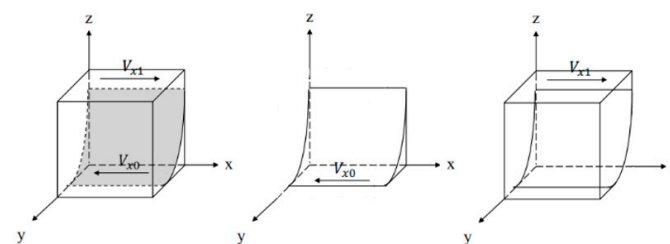


Figure 3. Phase diagram of the government regulator's strategy selection.

The probabilities of the government regulator adopting strict (V_{x1}) and lenient (V_{x0}) supervision strategies are calculated as follows:

$$V_{x0} = \iint_0^1 \frac{(1+\theta)(C_{gh}-C_{gl})}{U_e+F_e} \frac{(1+\theta)(C_{gh}-C_{gl})-\beta C_g+yU_e-(1-y)F_e}{(1-y)[(1+\theta)U_g+\alpha L_g]} dx dy$$

$$= \frac{(1+\theta)(C_{gh}-C_{gl})\beta C_g - F_e - ((1+\theta)(C_{gh}-C_{gl}) - \beta C_g + U_e) \ln\left(\frac{U_e+(1+\theta)(C_{gh}-C_{gl})-\beta C_g}{U_e+F_e}\right)}{(1+\theta)U_g+\alpha L_g}$$

$$V_{x1} = 1 - V_{x0}$$

After integration and simplification, it can be expressed as:

$$V_{x0} = \frac{(A - F_e) - (A + U_e) \ln \frac{U_e+A}{U_e+F_e}}{(1+\theta)U_g + \alpha L_g}, \quad A = (1+\theta)(C_{gh} - C_{gl}) - \beta C_g$$

This formulation allows for comparative static and parametric analysis. By differentiating V_{x0} with respect to the key parameters under the condition that $F_e > A$ —that is, when the penalty level exceeds the government’s net additional cost between strict and lenient supervision—the following partial derivatives are obtained:

$$\frac{\partial V_{x0}}{\partial F_e} = \frac{A-F_e}{[(1+\theta)U_g+\alpha L_g](U_e+F_e)} < 0,$$

$$\frac{\partial V_{x0}}{\partial \beta} = \frac{C_g}{(1+\theta)U_g+\alpha L_g} \ln \frac{U_e+A}{U_e+F_e} < 0,$$

$$\frac{\partial V_{x0}}{\partial \Delta C} = \frac{1+\theta}{(1+\theta)U_g+\alpha L_g} \left[-\ln \frac{U_e+A}{U_e+F_e} \right] > 0, \text{ where } \Delta C = C_{gh} - C_{gl}.$$

Corollary 1. *The probability of lenient supervision is inversely related to the enterprise penalty level and the proportion of supervisory costs shared by industry associations, while positively related to the cost differential between strict and lenient regulation. This suggests that higher penalties increase the expected cost of falsification for enterprises, effectively discouraging deceptive traceability behaviors and narrowing the relative payoff gap between strict and lenient supervision. As a result, strict supervision becomes more stable for government regulators. Moreover, a higher level of industry association participation also strengthens the government’s preference for strict supervision. By sharing part of the regulatory burden and promoting industry self-discipline and information disclosure, associations alleviate fiscal and administrative pressure on regulators, allowing governments to sustain stricter oversight under the same conditions. However, when strict supervision requires significantly higher administrative or technical inputs compared with lenient regulation, regulators may shift toward leniency in the absence of sufficient incentives. The effect of technological adoption θ on V_{x0} is not unidirectional. On one hand, adopting advanced technologies increases system complexity and operational costs, thereby raising A and weakening the motivation for strict regulation. On the other hand, technology adoption enhances regulatory efficiency and reputational utility, expanding the denominator and thus reducing V_{x0} , which stabilizes strict supervision. In practice, the latter effect tends to dominate. Recent studies consistently show that in institutional environments with information disclosure and external accountability, the reputational incentives of regulatory bodies often outweigh pure cost constraints, thereby promoting and sustaining stricter supervision [41–44]. Meanwhile, mandatory or voluntary disclosure mechanisms make the reputational cost of leniency or inaction explicit, forming a “naming-and-shaming” effect and price penalties through media and capital markets, which further increase the marginal benefits of maintaining strict regulation [45]. This indicates that the reputational gains U_g from strict supervision exceed the regulatory cost differential ΔC , and the transparency and efficiency improvements brought by emerging technologies reinforce this positive effect. In summary, the application of technologies such as blockchain and big data improves information transparency*

and monitoring efficiency, reduces enforcement costs, and enables regulators to achieve real-time supervision and timely correction of enterprise misconduct—thereby enhancing the sustainability of strict regulation within the quality and safety traceability system.

3.2. Stability Analysis of Traceability Enterprises' Strategies

The expected payoff to a traceability enterprise when it shares truthful information is:

$$E_y = -C_{eh} + xU_e + W + zP_1 + \beta P_2 + \theta P \quad (6)$$

The expected payoff when the enterprise shares falsified information is:

$$E_{1-y} = -C_{el} - xF_e - \beta F - \alpha z(1-x)L_e + (1-x)(1-z)W \quad (7)$$

The replicator dynamic describing the evolution of enterprises' strategies is

$$\begin{aligned} F(y) &= \frac{dy}{dt} = y(E_y - \bar{E}) \\ &= y(1-y)[W + \theta P + C_{el} - C_{eh} + x(U_e + F_e) - (1-x)(1-z)W + zP_1 + \beta(F + P_2) \\ &\quad + \alpha z(1-x)L_e] \end{aligned} \quad (8)$$

According to the stability theorem of differential equations, for “sharing truthful information” to be an evolutionarily stable strategy (ESS), it must hold that $F(y) = 0$ and $F'(y) < 0$. Hence,

$$\begin{aligned} F'(y) &= (1-2y)[C_{el} - C_{eh} + x(U_e + F_e) + zP_1 + \beta(F + P_2) \\ &\quad - (1-x)(1-z)W + W + \theta P + \alpha z(1-x)L_e] \end{aligned} \quad (9)$$

Solving for the threshold that separates the two stable regions yields:

$$x_0 = \frac{C_{el} - C_{eh} + zP_1 + \beta(F + P_2) + \theta P + \alpha zL_e + zW}{-[U_e + F_e - \alpha zL_e + (1-z)W]} \quad (10)$$

Proposition 2. When $x > x_0$, the enterprise's evolutionarily stable strategy is to share truthful information; when $x < x_0$, the ESS is to share falsified information; when $x = x_0$, no unique stable strategy can be determined.

Proof. Let $L(x) = -C_{eh} + C_{el} + x(U_e + F_e) + W + zP_1 + \beta(F + P_2) + \theta P + \alpha z(1-x)L_e - (1-x)(1-z)W$. Since $\partial L(x)/\partial x = U_e + F_e - \alpha zL_e + (1-z)W > 0$, $L(x)$ is increasing in x . When $x < x_0$, $L(x) < 0$ and hence $F(y)|_{y=0} = 0$, $F'(y)|_{y=0} < 0$, so $y = 0$ is stable. When $x > x_0$, $L(x) > 0$ and thus $F(y)|_{y=1} = 0$, $F'(y)|_{y=1} < 0$, so $y = 1$ is stable. When $x = x_0$, both boundary points are neutrally stable and no definitive stable strategy exists. $\square$

From the above analysis, it can be concluded that as the probability of strict supervision by government regulators increases, the evolutionarily stable strategy of traceability enterprises shifts from sharing falsified information to sharing truthful information. In other words, when the government is more inclined to enforce strict regulation, enterprises gain additional rewards and reputation benefits for truthful disclosure while avoiding potential penalties for falsification; hence, sharing truthful information becomes a more stable strategy. Conversely, when government regulators are more likely to adopt lenient supervision, enterprises seek to minimize their costs and risks by reducing investment in information disclosure, leading to a higher probability of falsified traceability information becoming the stable outcome.

The phase diagram of the traceability enterprises' strategy selection is shown in Figure 4, where V_{y1} and V_{y0} respectively denote the probabilities of enterprises sharing truthful and falsified traceability information.

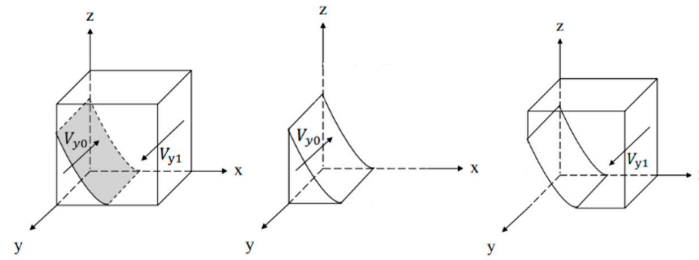


Figure 4. Phase diagram of the traceability enterprise's strategy selection.

The probabilities of the traceability enterprise sharing truthful (V_{y1}) and falsified (V_{y0}) traceability information are calculated as follows:

$$V_{y0} = \int_0^1 \int_0^1 -\frac{C_{el} - C_{eh} + zP_1 + \beta(F + P_2) + \theta P + \alpha zL_e + zW}{U_e + F_e - \alpha zL_e + (1-z)W} dydz$$

$$= 1 + \frac{P_1}{\alpha L_e + W} + \left[\frac{C_{el} - C_{eh} + \beta(F + P_2) + \theta P}{\alpha L_e + W} + \frac{(U_e + F_e + W)(P_1 + \alpha L_e + W)}{(\alpha L_e + W)^2} \right] \ln \left(\frac{U_e + F_e - \alpha L_e}{U_e + F_e + W} \right)$$

$$V_{y1} = 1 - V_{y0}$$

For subsequent comparative analysis, the expression can be simplified as:

$$V_{y0} = \frac{A_1}{B_1} + \frac{A_0 B_1 - A_1 B_0}{B_1^2} \ln \frac{B_0 + B_1}{B_0},$$

where,

$$A_0 = -(C_{el} - C_{eh} + \beta(F + P_2) + \theta P),$$

$$A_1 = -(P_1 + \alpha L_e + W),$$

$$B_0 = U_e + F_e + W,$$

$$B_1 = -(\alpha L_e + W).$$

The partial derivatives of with V_{y0} respect to key parameters are given by:

$$\frac{\partial V_{y0}}{\partial U_e} = -\frac{A_1}{B_1^2} \ln \left(\frac{B_0 + B_1}{B_0} \right) - \frac{A_0 B_1 - A_1 B_0}{B_1 B_0 (B_0 + B_1)} < 0,$$

$$\frac{\partial V_{y0}}{\partial \beta} = -\frac{F + P_2}{B_1} \ln \left(\frac{B_0 + B_1}{B_0} \right) < 0,$$

$$\frac{\partial V_{y0}}{\partial (C_{eh} - C_{el})} = \frac{1}{B_1} \ln \left(\frac{B_0 + B_1}{B_0} \right) > 0.$$

Corollary 2. *The likelihood of enterprises sharing truthful information increases with higher disclosure benefits, reduced reputational losses from consumer exposure, and greater government reward subsidies, but decreases as the cost gap between truthful and falsified disclosure widens. This implies that when the government increases rewards for truthful disclosure or strengthens penalties for falsification, the expected return structure of enterprises improves, thereby reducing their incentive to falsify traceability information. Similarly, a higher level of industry association participation, greater publicity returns, and stronger punitive measures all enhance enterprises' motivation to provide accurate information. At the consumer level, an increase in reporting probability and reputational loss further elevates the potential risks of falsification, compressing its expected benefits and encouraging truthful behavior. Conversely, when the cost of truthful disclosure significantly exceeds that of falsification, enterprises' willingness to share accurate traceability information diminishes, and the system may tend toward a false-information equilibrium. Thus, the multi-agent incentive and constraint mechanisms among government regulators, industry associations, and consumers jointly form a positive feedback structure that promotes truthful information sharing within the dynamic evolutionary game.*

3.3. Stability Analysis of Consumer Strategies

The payoff of consumers when choosing to verify traceability information is given by:

$$E_z = \theta U_c + yU_c - yC_1 - (1-x)(1-y)(C_1 + \alpha C_2) \quad (11)$$

The payoff of consumers when choosing to directly trust traceability information is:

$$E_{1-z} = \theta U_c + yU_c - (1-x)(1-y)L_c \quad (12)$$

Accordingly, the replicator dynamic equation describing the evolution of consumer strategies can be expressed as:

$$F(z) = \frac{dz}{dt} = z(E_z - \bar{E}) = z(1-z)[-yC_1 + (1-x)(1-y)(L_c - C_1 - \alpha C_2)] \quad (13)$$

Based on the stability condition of differential equations, the strategy in which consumers choose to verify traceability information must satisfy: $F(z) = 0$ and $F'(z) < 0$.

Therefore,

$$F'(z) = (1-2z)[-yC_1 + (1-x)(1-y)(L_c - C_1 - \alpha C_2)] \quad (14)$$

The threshold value is given by:

$$y_0 = \frac{(1-x)(L_c - C_1 - \alpha C_2)}{(1-x)(L_c - C_1 - \alpha C_2) + C_1} \quad (15)$$

Proposition 3. When $y > y_0$, consumers' ESS is to directly trust the provided traceability information as authentic. When $y < y_0$, the ESS is to verify the traceability information. When $y = y_0$, no stable strategy can be determined.

Proof. Let $M(y) = -yC_1 + (1-x)(1-y)(L_c - C_1 - \alpha C_2)$. Since $\partial M(y)/\partial y < 0$, $M(y)$ is a monotonically decreasing function with respect to y . When $y < y_0$, $M(y) > 0$, $F(z)|_{z=1} = 0$ and $F'(z)|_{z=1} < 0$, indicating that $z = 1$ is stable. When $y > y_0$, $M(y) < 0$, $F(z)|_{z=0} = 0$ and $F'(z)|_{z=0} < 0$ indicating that $z = 0$ is stable. When $y = y_0$, $M(y) = 0$, $F(z) = 0$ and $F'(z) = 0$; thus, for $z \in [0, 1]$, the system exhibits no definite stability, and both strategies coexist. $\square$

These results indicate that as the probability of enterprises sharing truthful information increases, consumers are more likely to trust the traceability information rather than verify it. When enterprises tend to disclose authentic traceability data, consumers perceive the information as reliable and prefer to save time, cost, and effort by directly trusting it, leading to a stable equilibrium of trust. Conversely, when the probability of falsified disclosure rises, consumers become more vigilant and are inclined to verify the information to safeguard their interests and ensure product safety. Hence, the stable strategy for consumers shifts dynamically in response to the credibility of enterprises' traceability behavior.

As shown in Figure 5, V_{z1} and V_{z0} , respectively, represent the probabilities that consumers choose to verify or directly trust traceability information.

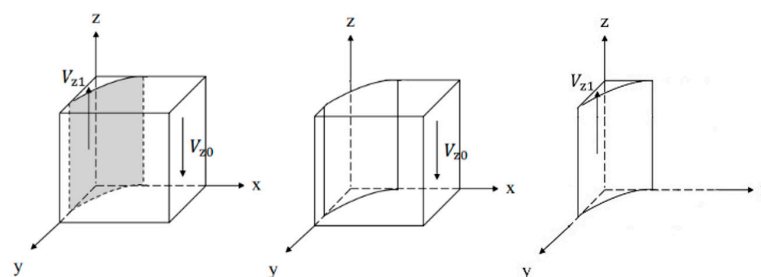


Figure 5. Phase diagram of the consumer's strategy selection.

The probabilities of the consumer choosing to verify (V_{z1}) and to directly trust (V_{z0}) are calculated as follows:

$$V_{z1} = \iint_0^1 \frac{(1-x)(L_c - C_1 - \alpha C_2)}{(1-x)(L_c - C_1 - \alpha C_2) + C_1} dx dz = 1 - \frac{C_1}{C_1 + \alpha C_2 - L_c} \ln \frac{C_1}{L_c - \alpha C_2}$$

$$V_{z0} = 1 - V_{z1} = \frac{C_1}{C_1 + \alpha C_2 - L_c} \ln \frac{C_1}{L_c - \alpha C_2}$$

To ensure the mathematical validity of subsequent derivations and the sign consistency of partial derivatives, this study assumes $L_c - \alpha C_2 > C_1 > 0$. This implies that the potential loss incurred by consumers when facing falsified traceability information (including reporting and verification costs) is greater than the one-time verification cost—an assumption that holds in most real-world contexts. For instance, in sectors such as food safety or pharmaceutical supply chains, consumers face substantial health and reputational risks from misinformation, far exceeding the marginal cost of verification, thereby motivating verification behavior.

To examine the effect of key parameters on V_{z1} , partial derivatives are obtained as follows:

$$\frac{\partial V_{z1}}{\partial C_1} = - \left[\frac{(\alpha C_2 - L_c)}{(C_1 + \alpha C_2 - L_c)^2} \ln \frac{C_1}{L_c - \alpha C_2} + \frac{1}{C_1 + \alpha C_2 - L_c} \right],$$

$$\frac{\partial V_{z1}}{\partial C_2} = \alpha C_1 \left(\frac{\ln \frac{C_1}{L_c - \alpha C_2}}{(C_1 + \alpha C_2 - L_c)^2} - \frac{1}{(C_1 + \alpha C_2 - L_c)(L_c - \alpha C_2)} \right),$$

$$\frac{\partial V_{z1}}{\partial \alpha} = C_2 C_1 \left(\frac{\ln \frac{C_1}{L_c - \alpha C_2}}{(C_1 + \alpha C_2 - L_c)^2} - \frac{1}{(C_1 + \alpha C_2 - L_c)(L_c - \alpha C_2)} \right),$$

$$\frac{\partial V_{z1}}{\partial L_c} = C_1 \left(- \frac{\ln \frac{C_1}{L_c - \alpha C_2}}{(C_1 + \alpha C_2 - L_c)^2} + \frac{1}{(C_1 + \alpha C_2 - L_c)(L_c - \alpha C_2)} \right).$$

Since $L_c - \alpha C_2 > C_1 > 0$ it follows that $\ln \frac{C_1}{L_c - \alpha C_2} < 0$. Combining these relationships: $\ln t > 1 - \frac{1}{t}$ ($t > 1$), and $\ln r < r - 1$ ($0 < r < 1$), it can be inferred that:

$$\frac{\partial V_{z1}}{\partial C_1} < 0, \frac{\partial V_{z1}}{\partial C_2} < 0, \frac{\partial V_{z1}}{\partial \alpha} < 0, \frac{\partial V_{z1}}{\partial L_c} > 0$$

Corollary 3. *The probability that consumers verify traceability information is negatively correlated with verification and reporting costs, and positively correlated with the perceived losses caused by falsified information. In other words, the greater the potential harm consumers may suffer from false traceability information, the stronger their concern for authenticity and their willingness to verify. Conversely, when verification and reporting costs are high, consumers tend to remain silent or directly trust the provided information, gradually evolving into passive participants within the game system. These results suggest that the stability of consumer strategies is closely linked to both the institutional environment and cognitive awareness. When government regulators respond promptly to consumer reports, provide timely feedback, and offer material or reputational incentives, consumers develop positive expectations and become more willing to participate actively in the collective co-governance of product traceability. To facilitate this process, governments and digital platforms should make use of digital traceability tools—such as QR-code verification, online complaint portals, and one-click reporting systems—to lower verification costs and enhance the feasibility and immediacy of consumer oversight. At the societal level, public education, media exposure, and industry training can raise consumers’ awareness of the potential risks associated with false traceability information (i.e., increasing their perceived value of L_c), and strengthen their motivation to safeguard their rights through rational verification. In summary, reducing verification and reporting costs, reinforcing feedback incentives, and enhancing risk perception can effectively encourage consumers to act as rational supervisors within the traceability ecosystem. Such multi-stakeholder co-governance—linking government regulation, enterprise transparency,*

and public participation—supports the sustainable evolution and positive reinforcement of the overall traceability governance mechanism.

3.4. Stability Analysis of Strategy Combinations

According to Lyapunov's first method, if at least one of the real parts of the eigenvalues of the Jacobian matrix is positive, the equilibrium point is unstable. If all real parts are negative, the equilibrium point is asymptotically stable. If one or more eigenvalues are zero while the others are negative, the equilibrium point is in a critical state. Based on the replicator dynamic equations of the three evolutionary agents, the Jacobian matrix J of the system can be expressed as:

$$J = \begin{bmatrix} \partial F(x)/\partial x & \partial F(x)/\partial y & \partial F(x)/\partial z \\ \partial F(y)/\partial x & \partial F(y)/\partial y & \partial F(y)/\partial z \\ \partial F(z)/\partial x & \partial F(z)/\partial y & \partial F(z)/\partial u \end{bmatrix}$$

When the government regulator's equilibrium strategy is loose supervision, the corresponding condition is: $(1 + \theta)(C_{gl} - C_{gh}) + \beta C_g - yU_e + (1 - y)[(1 + \theta)zU_g + \alpha zL_g + F_e] > 0$. This implies that the system remains in a state where the strict-regulation equilibrium is not evolutionarily stable (i.e., any perturbation will drive the system away from it). As shown in Table 3, when the government adopts a strict supervision strategy, the system's pure-strategy equilibrium does not exist. The stability analysis of eigenvalues under strict regulation indicates that if the government chooses strict supervision, enterprises adopt truthful traceability, and consumers verify information, the system is unstable. In this case, consumers can directly trust traceability information without additional verification. However, as demonstrated by the eigenvalue analysis, when consumers tend to directly trust traceability information, the government—aiming to reduce supervision costs—will gradually shift toward loose supervision, making the strict-regulation equilibrium unsustainable.

Table 3. Asymptotic stability analysis of equilibrium points in the replicator dynamic system under strict government regulation.

Equilibrium Point	Eigenvalues $\lambda_1, \lambda_2, \lambda_3$	Sign of Real Parts	Stability
(1,0,0)	$0, C_{gh} - C_{gl} - F_e - \beta C_g + \theta C_{gh} - \theta C_{gl}, C_{el} - C_{eh} + F_e + U_e + W + \beta F + \beta P_2 + \theta P$	$(0, U, +)$	Unstable
(1,0,1)	$0, C_{gh} - C_{gl} - F_e - (\theta + 1)L_g U_g - \beta C_g + \theta C_{gh} - \theta C_{gl} - \alpha L_g, C_{el} - C_{eh} + F_e + U_e + P_1 + W + \beta F + \beta P_2 + \theta P$	$(0, U, +)$	Unstable
(1,1,0)	$0, -C_1, (\theta + 1)(C_{gh} - C_{gl}) - F_e + U_e - \beta C_g$	$(0, -, -)$	Indeterminate
(1,1,1)	$0, C_1, (\theta + 1)(C_{gh} - C_{gl}) - F_e + U_e - \beta C_g$	$(0, +, -)$	Unstable

Therefore, to maintain the long-term stability of truthful traceability and ensure consumers' legitimate rights, the government must balance regulatory intensity with effective incentive–constraint mechanisms. This requires not only appropriate supervision costs but also regulatory frameworks that align punishment and reward, ensuring the dynamic system of quality traceability evolves toward a stable equilibrium that supports truthful information disclosure and sustainable governance. Under strict supervision, the results of the asymptotic stability analysis are summarized in Table 3.

When the government regulator's equilibrium strategy is loose supervision, the condition becomes: $(1 + \theta)(C_{gl} - C_{gh}) + \beta C_g - yU_e + (1 - y)[(1 + \theta)zU_g + \alpha zL_g + F_e] < 0$. As shown in Table 4, when the government adopts a loose supervision strategy, the equilibrium point (0,0,0) may become stable. This suggests that if enterprises prefer to share falsified traceability information and consumers tend to trust such information directly—while

the government maintains a low level of supervision and the adoption of emerging technologies (e.g., blockchain and big data) remains limited—the system will evolve toward the equilibrium (0,0,0). In this scenario, false information sharing becomes the dominant strategy, and government supervision loses its effectiveness. To avoid such unfavorable outcomes, it is crucial to enhance industry association participation, strengthen the regulatory capacity of public authorities, and promote the integration of blockchain and big data technologies in traceability systems. These efforts will improve information transparency, reduce regulatory asymmetry, and facilitate the establishment of a stable, cooperative equilibrium among governments, enterprises, and consumers—thereby advancing the sustainable development of product quality and safety governance.

Table 4. Asymptotic stability analysis of equilibrium points in the replicator dynamic system under loose government regulation.

Equilibrium Point	Eigenvalues $\lambda_1, \lambda_2, \lambda_3$	Sign of Real Parts	Stability
(0,0,0)	$L_c - C_1 - \alpha C_2, C_{el} - C_{eh} + \beta F + \beta P_2 + \theta P, (\theta + 1)(C_{gl} - C_{gh}) + F_e + \beta C_g$	(U, U, −)	Asymptotically stable (ESS) if condition (a) holds
(0,0,1)	$-L_c + C_1 + \alpha C_2, C_{el} - C_{eh} + P_1 + W + \beta F + \alpha L_e + \beta P_2 + \theta P, (\theta + 1)(C_{gl} - C_{gh}) + F_e + \beta C_g + \alpha L_g + (\theta + 1)L_g U_g$	(U, +, −)	Unstable
(0,1,0)	$0, -C_1, (\theta + 1)(C_{gl} - C_{gh}) + F_e - U_e + \beta C_g$	(0, −, −)	Indeterminate
(0,1,1)	$0, C_1, (\theta + 1)(C_{gl} - C_{gh}) + F_e - U_e + \beta C_g$	(0, +, −)	Unstable

Condition (a): $L_c - C_1 - \alpha C_2 < 0, C_{el} - C_{eh} + \beta F + \beta P_2 + \theta P < 0$. U = positive real part; − = negative real part; 0 = zero real part. ESS = Evolutionarily Stable Strategy.

4. Simulation Analysis

4.1. Parameter Settings and Simulation Design

To intuitively illustrate how key variables shape the evolutionary dynamics and equilibrium outcomes among government regulators, traceability enterprises, and consumers in a quality and safety traceability system, this study conducts numerical simulations in the MATLAB 2022b environment. To enhance the interpretability of the simulation results, agricultural product quality and safety traceability are selected as a representative application scenario, and the model is contextualized based on China's regulatory practices in this field [46]. All parameters are specified as dimensionless structural values. They are designed to capture generic cost–benefit relations in quality traceability rather than the absolute magnitudes for any specific region or firm. In practice, truthful traceability typically entails higher operating costs but helps to build long-term brand value; falsification may bring short-term gains but is exposed to high penalties and reputational risks; and consumer verification and reporting require non-negligible time and monetary effort. Under these assumptions, the evolutionary game framework focuses on relative payoffs and strategy adjustment paths. As long as the relative parameter relationships are preserved and cost–benefit coefficients are appropriately rescaled, the framework can be extended to other quality-sensitive sectors such as pharmaceuticals, e-commerce and cross-border cold chains.

To ensure the rationality of parameter settings, all values are grounded in economic assumptions and empirical judgments, and are assigned based on the functional meaning of each parameter as well as existing research [1]. Cost and benefit parameters relevant to the government and enterprises are drawn primarily from the studies of Zhu L [47] and Sun S [48], while government reward–penalty and loss coefficients are referenced from Tu [33], with moderate amplification to reflect the significant public governance impact of food safety incidents. Specifically, the government's cost of strict supervision

is set to $C_{gh} = 8$, and that of loose supervision to $C_{gl} = 1$. Under strict supervision, enterprises that share truthful traceability information receive a reward subsidy $U_e = 6$, whereas those that disclose falsified information are fined $F_e = 12$; at the same time, the government gains reputational utility $U_g = 20$. Given that the Chinese government has strongly encouraged industry associations to participate in co-regulation, while the relevant institutional framework is still evolving [49], the probability of active association participation is set to $\beta = 0.3$. When participating, associations share part of the supervision cost, represented by $C_g = 2$.

On the enterprise side, choosing low-quality products and sharing falsified information requires relatively small human, material and managerial inputs, so the falsification cost is set to $C_{el} = 2$, generating a negative utility for consumers of $L_c = 4$. Providing high-quality products and truthful traceability involves a higher cost $C_{eh} = 10$, but brings additional revenue from increased sales, firm value and brand reputation, summarized as $W = 18$. When industry associations participate actively, their positive publicity further enhances compliant firms' reputation and yields an extra benefit $P_2 = 5$, while they impose additional sanctions on enterprises that share falsified information in the form of a penalty $F = 6$.

Consumer-related parameters combine evidence on consumer-rights protection with available statistics. Consumers incur a verification cost $C_1 = 0.5$ when processing and checking traceability information. According to China's Economic Transformation and Quality-Power Strategy Study, 17.14% of consumers who purchased substandard products lodged complaints with regulatory agencies; based on this, the initial probability that a consumer reports falsified information after verification is set to $\alpha = 0.2$. Because defending rights generally requires considerable time and financial expenditure, the reporting cost is set to $C_2 = 5$. When consumers verify or perceive that an enterprise shares truthful traceability information, their word-of-mouth improves the firm's reputation and brings additional income $P_1 = 7$. If, under loose supervision, the government fails to respond to consumer reports in a timely manner, consumers may resort to media exposure, causing reputational and trust losses to the government and enterprises, as denoted by $L_g = 24$ and $L_e = 25$, respectively.

Although blockchain and big data technologies have been widely discussed in the context of traceability, there remains a gap between theoretical research and practical implementation. Zhang et al. [50] report that the adoption of blockchain can increase the overall efficiency of a fruit supply chain by nearly 50% and improve profitability. Reflecting the current stage of application, the probability that the traceability system adopts such emerging technologies is set to $\theta = 0.3$, corresponding to a moderate but rising level of digitalisation, and the additional revenue brought to enterprises by these technologies is set to $P = 10$.

Building on the above parameterization, this subsection first examines how different initial strategy probabilities affect the evolutionary trajectories of the three participants, thereby assessing the model's sensitivity to initial conditions. When the initial probabilities are set to $(x, y, z) = (0.5, 0.5, 0.5)$ (Figure 6a), the simulation results show that the system undergoes oscillations throughout the simulation period, with no clear convergence to a stable equilibrium. The probability that enterprises share truthful information fluctuates between 1 and 0 in a regular pattern, while the probability of consumer verification oscillates within the interval 0.4–0.1. As time evolves and enterprises increasingly disclose falsified information, the government gradually shifts toward loose supervision, with the probability of strict supervision declining from 0.5 to nearly 0. When the initial strategy probabilities are set to $(x, y, z) = (0.6, 0.4, 0.2)$ (Figure 6b), the government maintains a relatively strong intention for strict supervision in the early stage. However, as enterprises

accumulate short-term gains from falsification and consumers exhibit weak verification incentives, the system gradually moves toward a state in which enterprises adopt truthful strategies only intermittently. Consumers eventually reduce verification efforts as well, and the government later transitions to loose supervision to minimize regulatory costs. In contrast, when the initial consumer verification intention is relatively strong, as in $(x, y, z) = (0.5, 0.5, 0.6)$ (Figure 6c), consumers' early verification efforts exert stronger pressure on enterprises, accelerating their switch to truthful information sharing. After a short adjustment phase, enterprises converge to stable truthful strategies, consumers' verification probability rapidly declines to zero due to reduced need for monitoring, and the government ultimately adopts loose supervision to save costs. Despite short-term fluctuations, all three participants converge to a stable equilibrium.

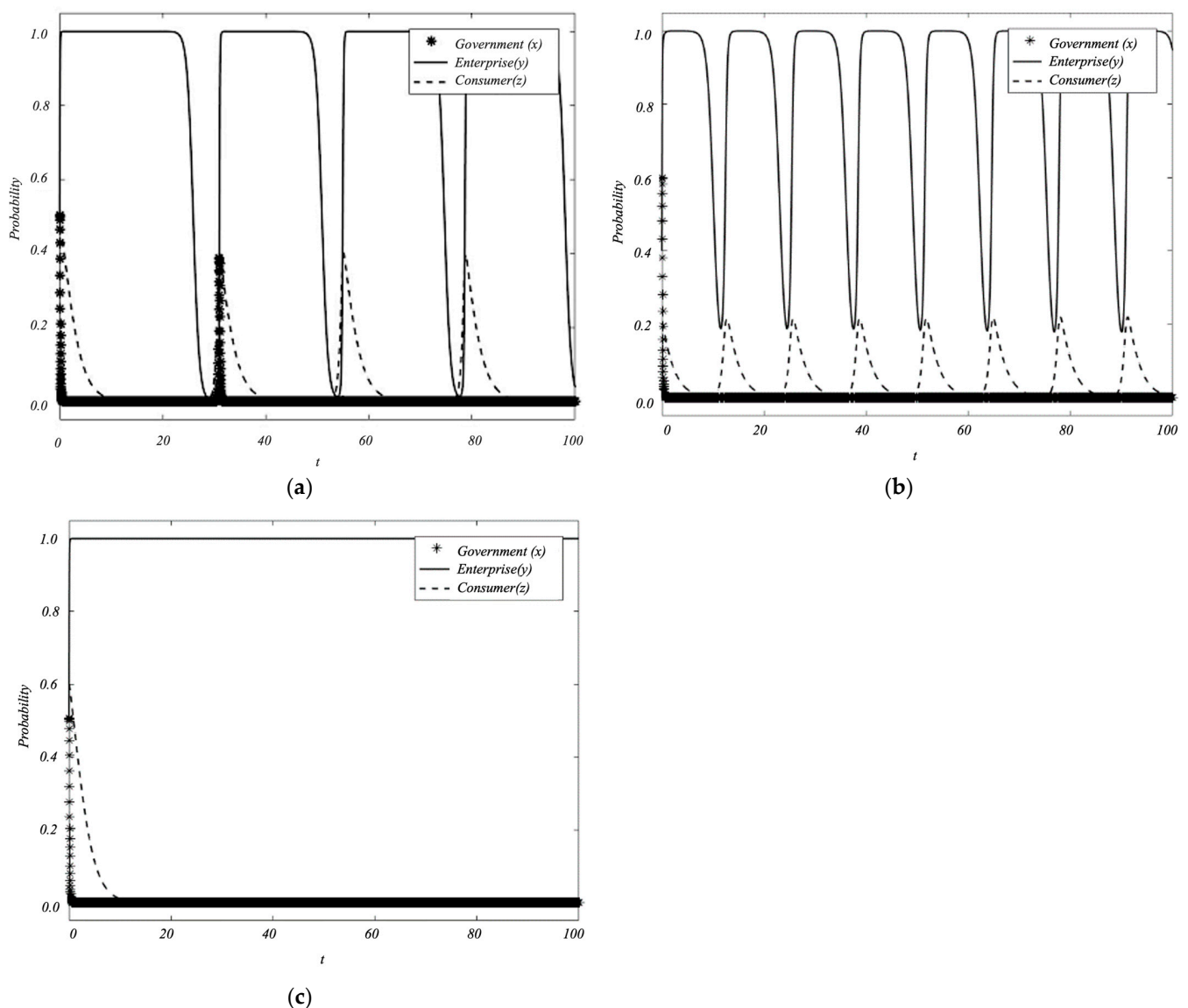


Figure 6. Evolution results of different initial strategy probabilities. (a) $(x, y, z) = (0.5, 0.5, 0.5)$. (b) $(x, y, z) = (0.6, 0.4, 0.2)$. (c) $(x, y, z) = (0.5, 0.5, 0.6)$.

For the parameter sensitivity analysis conducted in the subsequent sections, we selected $(0.5, 0.5, 0.5)$ as the benchmark initial state due to its neutrality, representing a balanced scenario where the government, enterprises, and consumers each start with equal probabilities of choosing strict supervision, truthful traceability sharing, and verification. This

choice allows us to observe how the system behaves under typical conditions without any initial biases favoring any participant's strategy.

4.2. Impact of Key Parameters on the Strategic Evolution of Participants

4.2.1. Evolutionary Impact of Varying Government Strict Supervision Cost (C_{gh})

To examine how government enforcement expenditures influence the strategic interactions among the three parties, this subsection varies the cost of strict supervision $C_{gh} = 2, 8, 12$ while keeping all other parameters unchanged. The simulation results are shown in Figure 7.

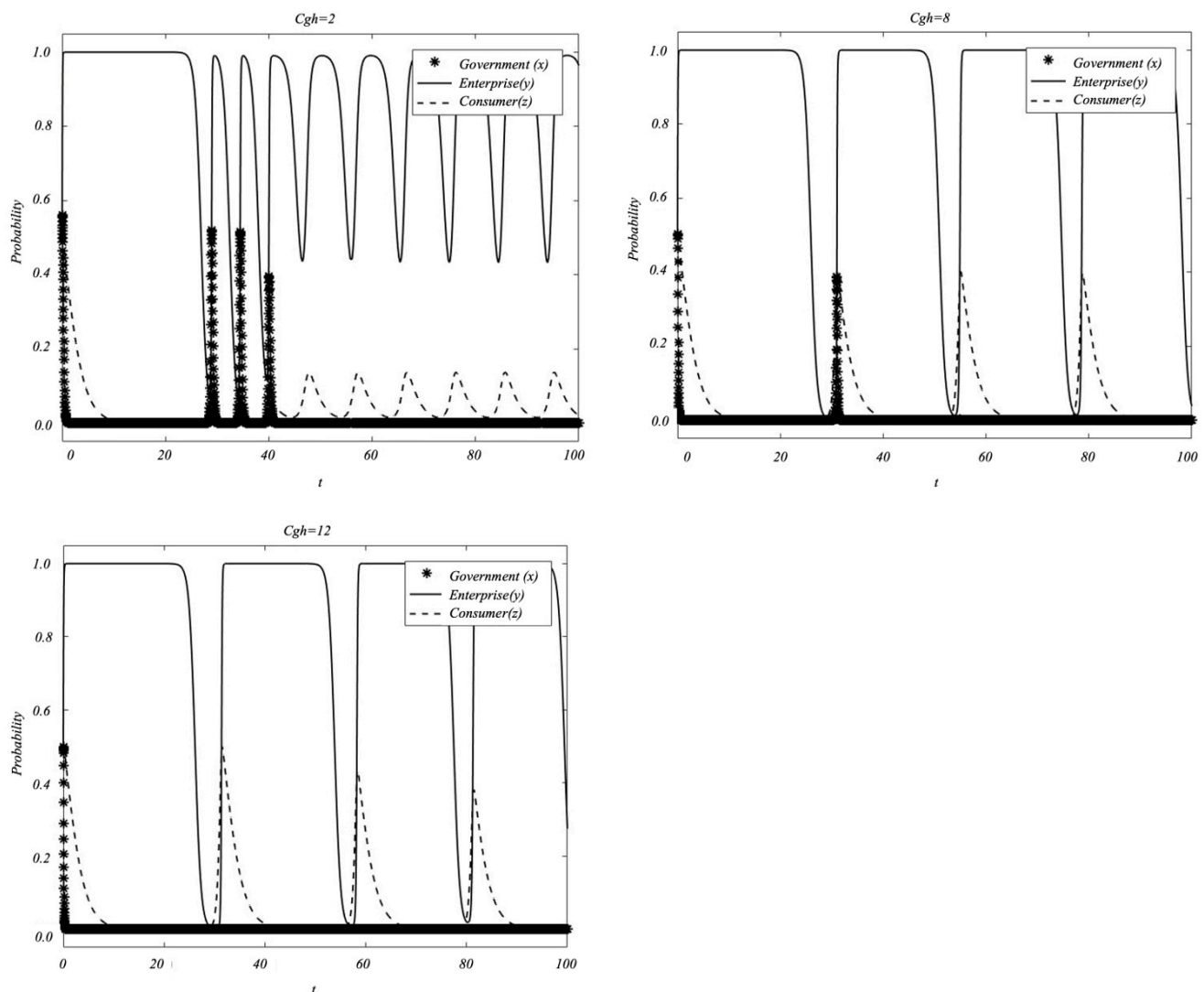


Figure 7. The impact of the strict regulation costs of government regulators on the evolution of tripartite strategies.

Excessive supervision costs impair the government's willingness to sustain strong enforcement and weaken the deterrence effect on falsification.

Overall, the results demonstrate that a moderate level of strict supervision cost is most conducive to correcting initial deviations and accelerating convergence toward truthful traceability. Excessively low supervision costs trigger prolonged oscillations, while excessively high costs shorten the strict-regulation phase prematurely, which undermines the long-term deterrence required to curb falsification. For agricultural product traceability—where regulatory credibility and the cost-effectiveness of enforcement jointly

matter—appropriate supervision cost levels, together with industry-association participation and digital traceability tools, can strengthen the government’s capacity to sustain effective oversight.

4.2.2. Evolutionary Impact of Varying Industry Association Participation (β)

Figure 8 presents the evolutionary trajectories of the government, traceability enterprises, and consumers under four levels of industry association participation probability ($\beta = 0, 0.3, 0.5, 0.8$), while all other parameters remain constant.

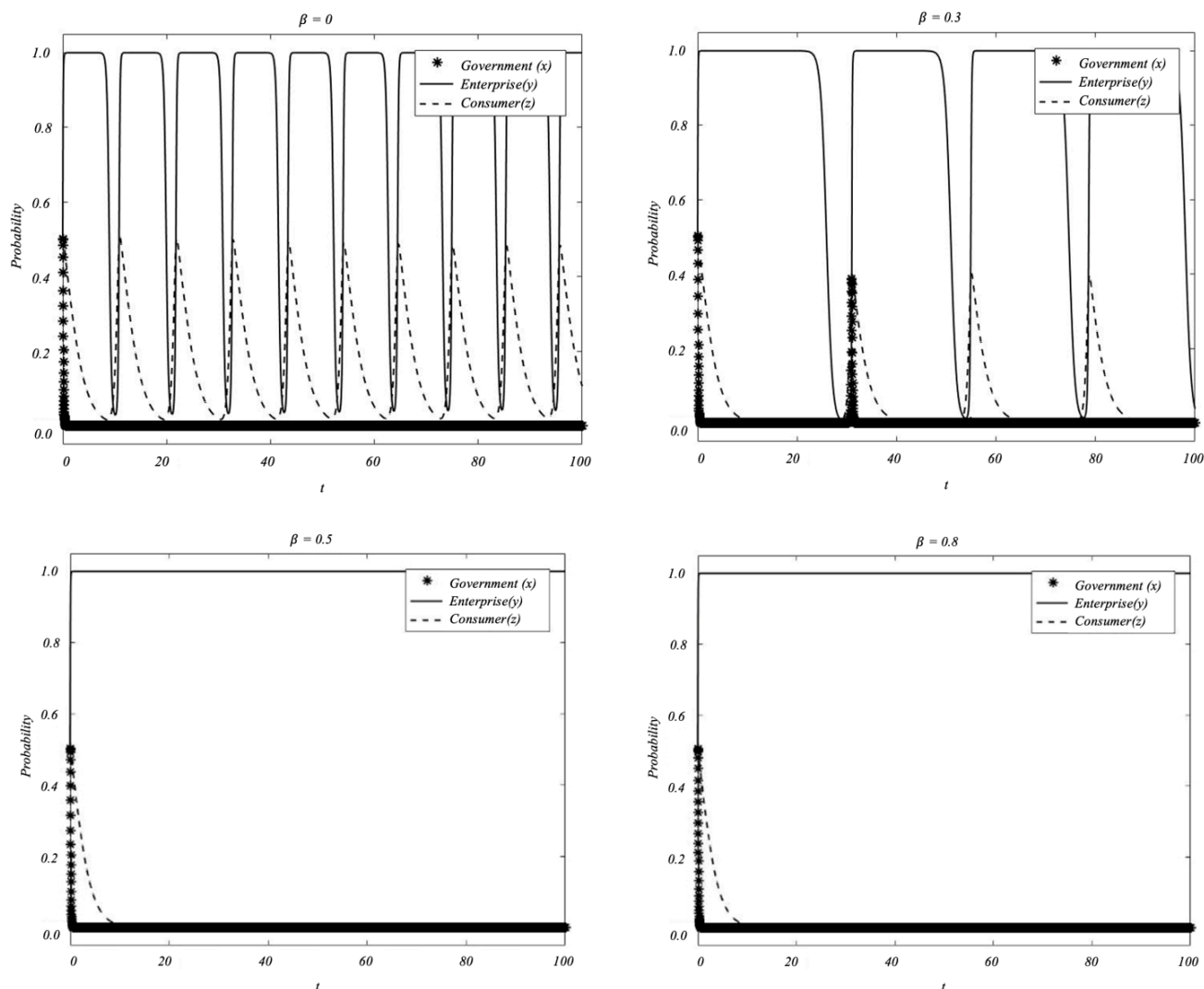


Figure 8. The impact of the participation degree of industry associations in quality traceability on the evolution of tripartite strategies.

When the association does not participate in the traceability system ($\beta = 0$), the government ultimately adopts a loose supervision strategy. During this stage, the probability that enterprises choose to share truthful traceability information fluctuates between 0 and 1 in a regular pattern, and consumers’ verification behavior oscillates between 0 and 0.5. Without the association’s involvement, the system is unable to converge to a stable equilibrium for an extended period. As β increases and the association begins to participate actively in traceability governance, notable structural changes emerge. Once β reaches 0.5, the association not only monitors enterprise traceability behavior but also provides rewards for compliant practices. Consequently, the duration that enterprises remain in the pure strategy of sharing truthful information increases steadily, and consumers’ adherence

to verification behavior also strengthens. Over time, the system transitions toward a stable configuration in which enterprises converge to the pure strategy of truthful information sharing ($y = 1$), while both the government and consumers stabilize at the non-strict strategies ($x = 0$ and $z = 0$, respectively). These results highlight the institutional importance of industry associations within traceability governance. As the participation probability rises, the system gradually shifts from an unstable state dominated by administrative regulation to a long-term equilibrium characterized by industry self-discipline. When β remains below a moderate threshold, the association primarily dampens fluctuations without fundamentally altering the system's equilibrium landscape. Once β exceeds approximately 0.5, however, the combined effects of enterprise compliance and governmental supervision reinforce one another, accelerating system stabilization and reducing volatility.

Taken together, the findings empirically support the argument that strengthening industry association participation can enhance the institutionalization of traceability governance, reduce dependence on direct government intervention, and improve the stability, credibility, and resilience of the traceability system. This underscores the practical value of developing a cooperative regulatory mechanism in which administrative regulators, industry associations, and enterprises jointly maintain the integrity and sustainability of quality and safety traceability efforts.

4.2.3. Evolutionary Impact of Varying Consumer Reporting Probability (α)

Figure 9 illustrates the evolutionary trajectories of the three stakeholders under different probabilities of consumers choosing to report falsified traceability information after verification, $\alpha = 0, 0.2, 0.5, 0.8$.

When consumers' willingness to report is low, an increase in α from 0 to 0.2 prompts the government to temporarily raise the probability of adopting strict supervision to avoid reputational losses caused by enterprises' falsification. During this stage, the time that enterprises remain in the pure strategy of sharing truthful traceability information also increases. However, as the system evolves, the government eventually converges to loose supervision to minimize regulatory costs. As consumers' awareness of rights protection strengthens and the reporting probability continues to rise, an increase to $\alpha = 0.4$ leads the government to respond more quickly with strict supervision once falsification is detected. Because the probability of enterprises engaging in falsification at this stage is relatively low, consumers tend to reduce verification efforts to save inspection costs, resulting in a low but fluctuating verification probability. When the reporting probability reaches $\alpha = 0.6$, the dynamics become more pronounced. Once falsification is detected, the expected reputational and economic losses for enterprises are substantial, prompting them to abandon falsification early in the evolution process and quickly stabilize at the pure strategy of sharing truthful information. In the long run, the government again converges to loose supervision due to cost considerations. Under a more trustworthy traceability environment, consumers no longer need to bear continuous verification costs, and their verification probability gradually declines and stabilizes near zero.

Overall, these results show that increasing consumers' reporting probability fundamentally amplifies the reputational and economic risks associated with falsification and thus strengthens the demand-side constraints on enterprise behavior. As long as reporting costs remain manageable, improving reporting convenience and success rates helps motivate enterprises to adopt and maintain truthful traceability strategies. This contributes to a healthier and more sustainable traceability governance environment without imposing additional supervision burdens on the government.

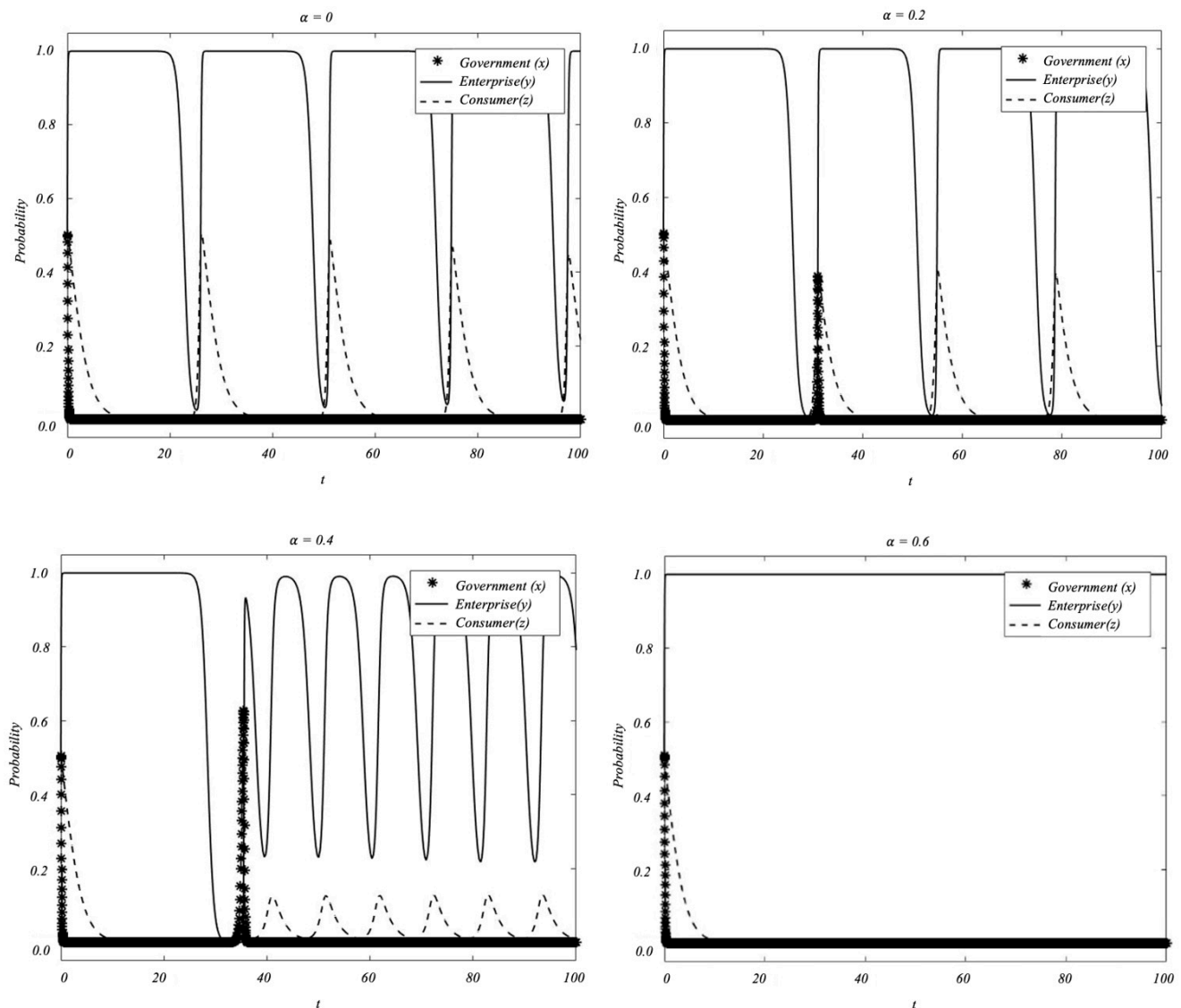


Figure 9. The impact of consumer behavior choices on the evolution of tripartite strategies.

4.2.4. Evolutionary Impact of Varying Traceability Digitalization Level (θ)

Building on the previous parameter settings, the digitalization level of the quality and safety traceability system is denoted by ($\theta = 0, 0.3, 0.5, 0.8$), corresponding to four stages ranging from no adoption of emerging technologies to pilot application, moderate maturity, and high maturity (Figure 10). The numerical results indicate that the system's ability to converge to a stable equilibrium is highly sensitive to the degree of digitalization.

When $\theta = 0$, meaning that the traceability system lacks digital support such as blockchain and big data, the strategies of the government, enterprises, and consumers exhibit strong periodic fluctuations over an extended period. To minimize regulatory costs, the government frequently switches between strict and loose supervision; enterprises oscillate between truthful and falsified traceability strategies; and although consumer verification temporarily increases following exposure of violations, it quickly declines to nearly zero due to high verification costs. As a result, the system fails to form a stable pattern dominated by truthful information sharing. When the digitalization level increases to 0.3, technologies such as blockchain begin to be piloted in agricultural product traceability, enabling partial automation of data recording and verification. While the system still experiences certain fluctuations, both the amplitude and frequency are substantially reduced. Enterprises spend significantly more time adopting the pure strategy of sharing truthful

information, while the duration of strict supervision decreases, suggesting that moderate digitalization mitigates information asymmetry and reduces ex post verification costs, thereby strengthening the incentives for compliant behavior. A major transition occurs when θ rises to 0.5 or above. At this point, the system crosses a critical threshold: regardless of whether $\theta = 0.5$ or $\theta = 0.8$, the three strategies rapidly converge to the same stable equilibrium. Enterprises' probability of sharing truthful information increases quickly and stabilizes at 1; consumers, operating in a transparent and trustworthy traceability environment, gradually reduce verification efforts to zero to save costs; and although the government initially bears substantial investment costs associated with new technologies, improvements in regulatory efficiency and reputational gains ultimately drive it to converge to loose supervision in the long run. Relative to the persistent oscillations under low digitalization, higher digitalization accelerates convergence and yields a system that is substantially more robust to initial conditions.

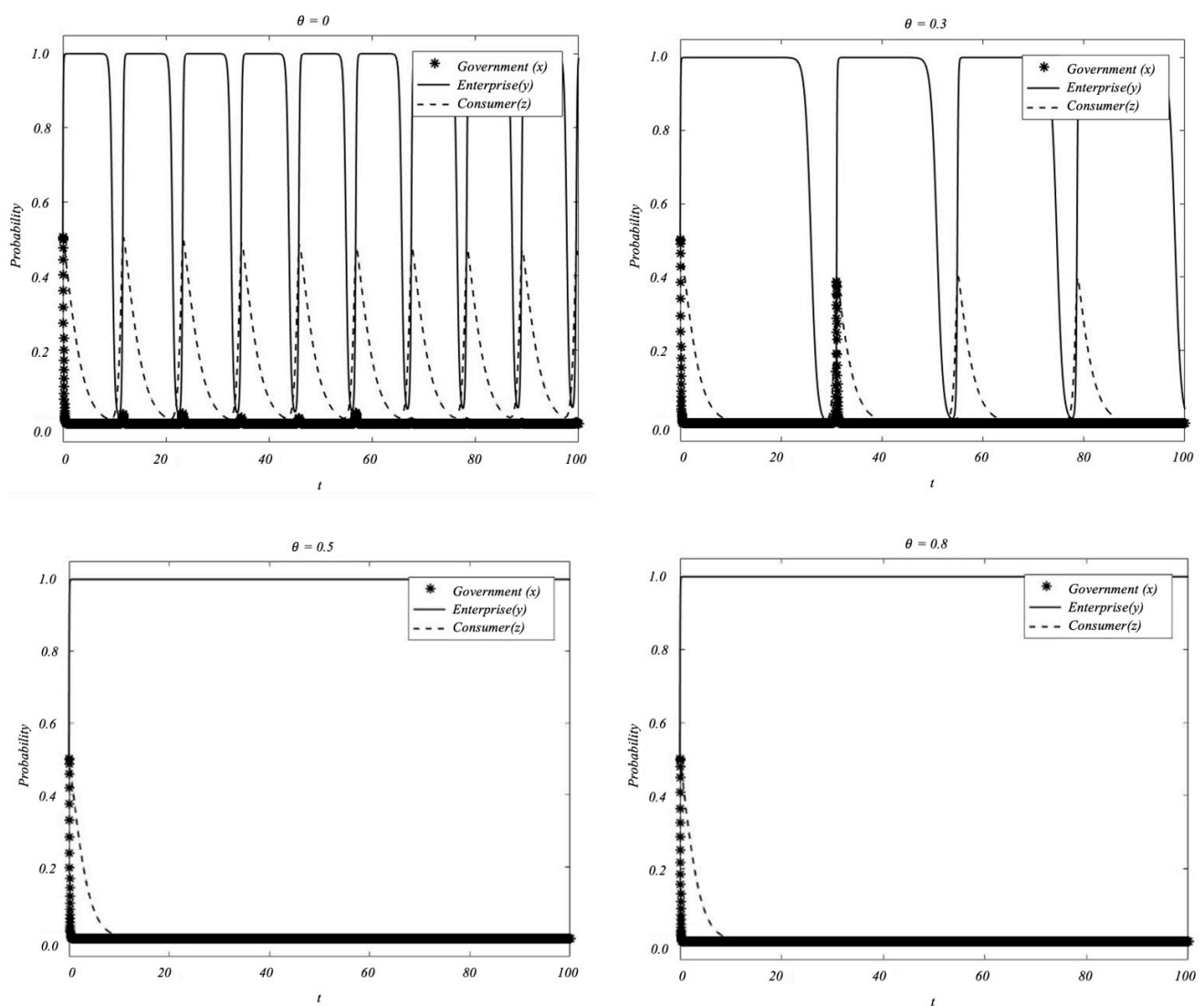


Figure 10. The impact of the digitalization level of the traceability system on the evolution of tripartite strategies.

Although the model assumes that the government bears most of the costs associated with adopting emerging technologies, its expenditures increase with the level of digitalization. Nevertheless, as blockchain and big data mature, they also yield improvements in regulatory efficiency and generate additional reputational benefits for the government.

Consequently, as the digitalization level increases, the government's strategy consistently converges to loosen supervision. This finding underscores the long-term policy implications: under the current big data governance context, government-led promotion of digital technologies such as blockchain in traceability systems helps strengthen incentives for enterprises to share truthful information, fosters a transparent and trustworthy traceability environment, and ultimately contributes to reducing regulatory costs. These results provide theoretical support for the ongoing policy direction that emphasizes digitalizing the traceability system and using technological tools to institutionalize incentives for truthful information disclosure.

5. Conclusions

This study develops an evolutionary game model that incorporates government regulators, traceability enterprises, consumers, and the moderating role of industry associations within a blockchain- and big data-enabled quality and safety traceability framework. Through stability analysis and MATLAB-based simulations, the study examines how regulatory costs, enforcement intensity, consumer participation, association engagement, and technological maturity jointly influence the strategic evolution of key actors.

The results show that when regulatory costs are too low, regulators tend to intervene frequently, suppressing non-compliance in the short term but failing to form stable expectations. Conversely, when regulatory costs are high and penalties insufficient, the marginal effectiveness of strict supervision declines rapidly, leading the system toward a low-quality equilibrium characterized by lenient regulation and weak participation. As digital technologies mature and institutional collaboration deepens, blockchain and big data significantly enhance information credibility, strengthen evidence constraints for enforcement, reduce ex post regulatory costs, and improve consumers' perceived trust. Once digitalization reaches a moderate-to-high level, the system tends to converge toward a desirable equilibrium in which regulators maintain moderate supervision, enterprises consistently disclose truthful traceability information, and consumers directly trust product information. Enterprises' willingness to disclose truthful information is shaped by the joint influence of reward–penalty structures and long-term reputational incentives. Industry associations, while not acting as independent strategic players, indirectly promote compliance by establishing sectoral norms, sharing monitoring costs, and enhancing reputational pressure—thereby expanding the stability region of truthful information sharing and reducing reliance on high-intensity governmental supervision. Consumer engagement in verification and reporting increases when participation processes become simpler and institutional responsiveness improves; however, a decline in consumer involvement combined with persistent regulatory leniency may trigger a “coordination trap” that undermines the credibility of the entire system.

Theoretically, this study highlights the nonlinear linkage between regulatory costs, enforcement intensity, and compliance behavior, clarifying why excessively high regulatory costs may drive systems toward lenient equilibria with weakened incentive effects. By incorporating industry associations as institutional intermediaries into a tri-party evolutionary game, the study enriches existing research that largely focuses on bilateral government–enterprise or enterprise–consumer dynamics and offers a more integrated explanation of how co-regulation and industry self-discipline jointly shape compliance. Moreover, by treating digitalization as a structural variable that affects payoffs and evolutionary pathways, the analysis identifies a dual effect of technological adoption—raising short-term operational costs while enhancing long-term efficiency. This “innovation paradox” offers a fresh perspective for understanding how technology adoption, behavioral adjustment, and institutional design interact within digital traceability governance. Collectively, the theoretical insights contribute to a broader framework for explaining transitions from “high-pressure regulation with low trust” to “digi-

tally enabled, multi-stakeholder co-governance with high trust,” consistent with the principles of transparency and accountability underpinning SDG 12.

Based on these findings, the paper offers the following policy insights to strengthen sustainable traceability governance:

- Strengthen regulatory and incentive mechanisms for sustainable supervision. The simulation results indicate that stable and effective supervision depends on a balanced configuration of regulatory costs, enforcement capacity, and incentive structures. Governments should move toward a digital-first regulatory architecture that records key inspection and enforcement events on blockchain, harmonizes data formats, standardizes information flows, and uses early-warning or rule-based triggers for real-time monitoring. The integration of big data analytics can enhance this system by processing vast amounts of real-time information, enabling predictive analysis and improving the accuracy of monitoring and enforcement decisions. Such arrangements can reduce administrative burdens while improving precision and transparency. At the same time, well-calibrated subsidies and penalties can optimize payoff structures, and reputational instruments—such as “white lists” or public compliance disclosure—can reinforce deterrence without placing excessive strain on public budgets. The overall objective is to design transparent and proportionate incentive schemes that ensure the expected payoff from truthful disclosure exceeds that from falsification, making truthful reporting the dominant rational strategy for firms.
- Encourage active participation of industry associations in co-governance. The analysis shows that higher levels of association participation can stabilize the system even when direct government oversight is limited. As a bridge between public regulation and corporate self-discipline, industry associations should be embedded in formal co-regulation frameworks with clearly defined responsibilities for monitoring, certification, dispute resolution, and recognition of compliant enterprises. By operating digital traceability databases, conducting peer reviews, and promoting best practices, associations can provide normative guidance and reputational incentives that promote sector-wide normalization. This form of institutionalized collaboration not only reduces public enforcement costs but also helps cultivate a culture of trust and responsibility within industries, gradually transforming external supervision into internalized, reputation-based self-regulation.
- Empower consumers and lower participation barriers. An increase in consumers’ reporting probability significantly raises the likelihood that firms choose truthful traceability, but high verification and reporting costs make it difficult to maintain sustained external pressure. Consumer participation is therefore critical for market transparency and social oversight. User-friendly verification and feedback mechanisms—such as QR-based checking, instant feedback channels, and online reporting systems—can substantially strengthen firms’ compliance incentives. Public communication campaigns can raise awareness of the social value of traceability, while robust privacy and data protection measures help build trust in digital participation. When verification is perceived as convenient, safe, and meaningful, consumers can shift from passive recipients to active co-regulators, reinforcing the social foundations of shared responsibility for product quality and safety.
- Enhance technological investment for long-term sustainability. Higher levels of digitalization accelerate convergence toward stable equilibria, enhance regulatory efficiency, and improve corporate transparency. Policymakers should therefore continue to invest in blockchain, big data, IoT, and artificial intelligence applications in the traceability domain, promoting cross-agency data interoperability and standardization. On the demand side, green public procurement and sustainability-linked finance can create market

incentives for digital traceability adoption. At the same time, establishing trust-based governance frameworks—including third-party audits, algorithmic accountability, and transparent performance indicators such as traceability coverage, recall response times, and complaint closure rates—can make governance performance more measurable and verifiable. These measures together can help consolidate a transparent, efficient, and resilient traceability ecosystem that supports sustainable quality governance.

Despite these contributions, the study has several limitations. First, the model abstracts from the heterogeneity of real-world contexts across industries, product categories, and regulatory environments. Future work could extend the framework to multi-level or cross-sectoral settings to more accurately capture differences in compliance behavior and policy outcomes. Second, the analysis focuses on blockchain and big data as enabling technologies; subsequent research could incorporate artificial intelligence, IoT, and privacy-preserving computation to examine their combined impact on information asymmetry and governance efficiency. At the same time, it is important to recognize that large-scale data collection, storage, and processing in IoT- and AI-based systems often depend on energy-intensive data centers and can raise concerns about privacy protection and data security. Future studies could therefore explore how to balance improvements in digitalization and traceability performance with the energy footprint of data infrastructures and the risks associated with data governance, so that digital traceability genuinely contributes to sustainability rather than merely shifting the burden elsewhere. Third, the present analysis relies mainly on evolutionary modeling and numerical simulations, without systematic calibration to real-world data or comprehensive empirical validation. Future research could combine the proposed framework with sector-specific case studies or platform data, estimate key parameters, conduct sensitivity analysis, and use survey methods, experimental economics, or field experiments to test the model's propositions.

Going forward, integrating evolutionary modeling with empirical validation and interdisciplinary approaches will help clarify how technological adoption, behavioral adaptation, and institutional design jointly advance sustainable quality governance. This line of research can provide stronger analytical foundations for promoting transparency, accountability, and trust across global value chains.

Author Contributions: Conceptualization, W.X. and X.D.; methodology, W.X. and M.L.; software, W.X. and M.L.; formal analysis, W.X.; investigation, W.X. and X.B.; resources, W.X. and J.L.; writing—original draft preparation, W.X. and M.L.; writing—review and editing, W.X. and X.B.; visualization, W.X.; supervision, X.D.; project administration, X.D. and J.L.; funding acquisition, J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (Grant No. 72171173).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

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

References

1. Cao, W.; Tao, X. A Study on the Evolutionary Game of the Four-Party Agricultural Product Supply Chain Based on Collaborative Governance and Sustainability. *Sustainability* **2025**, *17*, 1762. [[CrossRef](#)]

2. Bottichio, L.; Keaton, A.; Thomas, D.; Fulton, T.; Tiffany, A.; Frick, A.; Mattioli, M.; Kahler, A.; Murphy, J.; Otto, M.; et al. Shiga Toxin–Producing *Escherichia coli* Infections Associated With Romaine Lettuce—United States, 2018. *Clin. Infect. Dis.* **2020**, *71*, e323–e330. [CrossRef] [PubMed]
3. Kaptchouang Tchatchouang, C.-D.; Fri, J.; De Santi, M.; Brandi, G.; Schiavano, G.F.; Amagliani, G.; Ateba, C.N. Listeriosis Outbreak in South Africa: A Comparative Analysis with Previously Reported Cases Worldwide. *Microorganisms* **2020**, *8*, 135. [CrossRef] [PubMed]
4. Chen, M.; Shen, R. Rural Settlement Development in Western China: Risk, Vulnerability, and Resilience. *Sustainability* **2023**, *15*, 1254. [CrossRef]
5. Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 Establishing a Framework for the Setting of Ecodesign Requirements for Sustainable Products, Amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and Repealing Directive 2009/125/EC. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1781> (accessed on 19 November 2025).
6. FSMA Final Rule on Requirements for Additional Traceability Records for Certain Foods. Available online: <https://www.fda.gov/food/food-safety-modernization-act-fsma/fsma-final-rule-requirements-additional-traceability-records-certain-foods> (accessed on 19 November 2025).
7. The Central Committee of the Communist Party of China and the State Council Issued the “Outline for Building a Quality-Powerful Country”. Available online: https://www.gov.cn/gongbao/content/2023/content_5742204.htm (accessed on 26 February 2025).
8. National Development and Reform Commission. *Implementation Plan on Improving the Security Governance of Data Circulation to Better Promote the Marketization and Valuation of Data Elements*; National Development and Reform Commission: Beijing, China, 2002.
9. Document of the National Certification and Accreditation Administration. Available online: https://www.cnca.gov.cn/zwx/tz/2025/art/2025/art_04711a161872470f9fc155a598277ddc.html (accessed on 19 November 2025).
10. Traceability & Recalls. Available online: <https://www.fao.org/food-safety/food-control-systems/supply-chains-and-consumers/traceability-and-recalls/en/> (accessed on 19 November 2025).
11. Cromwell, J.; Turkson, C.; Dora, M.; Yamoah, F.A. Digital technologies for traceability and transparency in the global fish supply chains: A systematic review and future directions. *Mar. Policy* **2025**, *178*, 106700. [CrossRef]
12. Chen, T.; Ding, K.; Hao, S.; Li, G.; Qu, J. Batch-based traceability for pork: A mobile solution with 2D barcode technology. *Food Control* **2020**, *107*, 106770. [CrossRef]
13. Zhou, C.; Yang, R.; Zhang, G. RFID adoption strategy and the operational performance of a pharmaceutical supply chain: The role of hospital competition. *Comput. Ind. Eng.* **2025**, *206*, 111201. [CrossRef]
14. Bandinelli, R.; Fani, V.; Rinaldi, R. Customer acceptance of NFC technology: An exploratory study in the wine industry. *Int. J. RF Technol. Res. Appl.* **2017**, *8*, 1–16. [CrossRef]
15. Zheng, M.; Zhang, S.; Zhang, Y. Construct Food Safety Traceability System for People’s Health Under the Internet of Things and Big Data. *IEEE Access* **2021**, *9*, 70571–70583. [CrossRef]
16. Jia, L.; Shao, B.; Yang, C.; Bian, G. A Review of Research on Information Traceability Based on Blockchain Technology. *Electronics* **2024**, *13*, 4140. [CrossRef]
17. Feng, H.; Wang, X.; Duan, Y.; Zhang, J.; Zhang, X. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. *J. Clean. Prod.* **2020**, *260*, 121031. [CrossRef]
18. Cheong, B.C. Leveraging Blockchain for Enhanced Transparency and Traceability in Sustainable Supply Chains. *Discov. Anal.* **2025**, *3*, 6. [CrossRef]
19. Nwani, S. Evaluating the Impact of Blockchain Technology on Supply Chain Transparency and Traceability. *GJABR* **2025**, *3*, 1065–1093. [CrossRef]
20. Play the Role of Industry Associations and Explore New Mechanisms for Quality Co-Governance! The Market Supervision Bureau of Foshan City, Guangdong Province Promotes the High-Quality Development of the Manufacturing Industry. Available online: https://www.cqn.com.cn/zj/content/2021-03/04/content_8670259.htm (accessed on 19 November 2025).
21. Verbeke, W.; Viaene, J. Beliefs, attitude and behavior towards fresh meat consumption in Belgium: Empirical evidence from a consumer survey. *Food Qual. Prefer.* **1999**, *10*, 437–445. [CrossRef]
22. Jin, L.W.; Liu, Z.J.; Liu, A.J. Participation behavior of pork seller in traceability system: Empirical analysis of 636 sellers in Beijing, Shanghai and Jinan, China. *Acta Agric. Zhejiangensis* **2021**, *33*, 541–552. [CrossRef]
23. Hu, Q.G.; Tong, L. Analysis on the Export Trade Effect of China’s Agri-products’Quality Safety Traceability System. *J. Int. Trade* **2012**, *7*, 30–36. [CrossRef]
24. Wilson, W.W.; Xavier, H.; Dahl, B.L. Costs and risks of conforming to EU traceability requirements: The case of hard red spring wheat. *Agribusiness* **2008**, *24*, 85–101. [CrossRef]
25. Qiao, J. Analysis of Wholesaler’s Cognition and Behavior Based on Food Safety. *China Bus. Mark.* **2011**, *25*, 76–80. [CrossRef]

26. Guo, J.Y.; Xiao, J. Governing Structure, External Support and Farmer Cooperatives' Traceability Participation of Agricultural Product Quality. *Agric. Econ. Manag.* **2022**, *71*, 93–106. [\[CrossRef\]](#)
27. Jin, Y.; Li, C.; Zheng, M.; Jia, W.; Hu, Q. An Evolutionary Game Analysis of the Aquatic Product Traceability System from a Multi-Actor Perspective. *Water* **2025**, *17*, 1656. [\[CrossRef\]](#)
28. Cao, Y.; Yu, C.Y.; Wan, G.Y. Food company regulation game research under government participation. *Syst. Eng. Theory Pract.* **2017**, *37*, 140–150.
29. Liu, C.Y.; Yu, T.; Ma, Y.H. Game of Government, Enterprise and Consumer Based on Product Quality Regulation Perspective. *Chin. J. Manag. Sci.* **2019**, *27*, 127–135. [\[CrossRef\]](#)
30. Zhu, L.L.; Rong, J.M.; Zhang, S.Y. Three-party Evolutionary Game and Simulation Analysis of Drug Quality Supervision under the Government Reward and Punishment Mechanism. *Chin. J. Manag. Sci.* **2021**, *29*, 55–67. [\[CrossRef\]](#)
31. Song, Y.H.; Shen, N.Z.; Liu, D. Evolutionary game and intelligent simulation of food safety information disclosure oriented to traceability system. *J. Intell. Fuzzy Syst.* **2018**, *35*, 2657–2665. [\[CrossRef\]](#)
32. Wang, L.; Li, Z.N.; Zhou, L.H. The Subject Behavior and Regulatory Policies of Food Traceability Systems—A Study Based on Consumers, Farmers and Enterprises. *J. Dongbei Univ. Financ. Econ.* **2017**, *5*, 46–53. [\[CrossRef\]](#)
33. Tu, J.X. Research on the Willingness to Quality and Safety Supervision in Traceable Agricultural Products Supply Chain. 2020. Available online: https://kns.cnki.net/kcms2/article/abstract?v=LYi8dJWcB0UI7qHPi8suMXqkgW2-X423m0PSo5536wRDouthzKqDj9k-4tJfuzP7Yq-yt03Dh7-4-Xzy0ZhwEHVrk8MMo4cL36OUVXhCjloozaQqgx24-l8loiOS2qzQKOHnHQj_hGuYQvQCtmVXG3Rcn2rxAJAnHmqetfTajhXyyuzo1hE1H7OgQOZwumn&uniplatform=NZKPT&language=CHS (accessed on 19 November 2025).
34. Zheng, Y.; Xu, Y.; Qiu, Z. Blockchain Traceability Adoption in Agricultural Supply Chain Coordination: An Evolutionary Game Analysis. *Agriculture* **2023**, *13*, 184. [\[CrossRef\]](#)
35. Li, C.; Chen, G. Research on Evolutionary Traceability Decision- Making of Quality and Safety Traceability of Stakeholders: Based on the Dual Channel Supply Chain of Agricultural Products. *IEEE Access* **2023**, *11*, 48463–48479. [\[CrossRef\]](#)
36. Li, D.; Mei, X. Evolutionary Game Analysis of Data Sharing among Large and Medium-Sized Enterprises in the Perspective of Platform Empowerment. *Sci. Rep.* **2024**, *14*, 11447. [\[CrossRef\]](#) [\[PubMed\]](#)
37. Zhao, H.; Yang, J. Evolutionary Game Analysis of Stakeholders' Decision-Making Behavior in Agricultural Data Supply Chain. *Front. Phys.* **2024**, *11*, 1321973. [\[CrossRef\]](#)
38. Cao, S.; Xu, H.; Bryceson, K.P. Blockchain Traceability for Sustainability Communication in Food Supply Chains: An Architectural Framework, Design Pathway and Considerations. *Sustainability* **2023**, *15*, 13486. [\[CrossRef\]](#)
39. Agrawal, T.K.; Kumar, V.; Pal, R. Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Comput. Ind. Eng.* **2021**, *154*, 107130–107142. [\[CrossRef\]](#)
40. Liu, Z.; Guo, P. Supply Chain Decision Model Based on Blockchain: A Case Study of Fresh Food E-Commerce Supply Chain Performance Improvement. *Discret. Dyn. Nat. Soc.* **2021**, *2021*, 5795547. [\[CrossRef\]](#)
41. Rimkutė, D. Strategic Silence or Regulatory Talk? Regulatory Agency Responses to Public Allegations amidst the Glyphosate Controversy. *J. Eur. Public Policy* **2020**, *27*, 1636–1656. [\[CrossRef\]](#)
42. Dannenberg, A.; Lumkowsky, M.; Carlton, E.K.; Victor, D.G. Naming and Shaming as a Strategy for Enforcing the Paris Agreement: The Role of Political Institutions and Public Concern. *Proc. Natl. Acad. Sci. USA* **2023**, *120*, e2305075120. [\[CrossRef\]](#) [\[PubMed\]](#)
43. Bovay, J. Food Safety, Reputation, and Regulation. *Appl. Econ. Perspect. Policy* **2023**, *45*, 684–704. [\[CrossRef\]](#)
44. Xue, Q.; Zhan, P.; Jin, Y.; He, H. Reputation, Commitment, and Financial Market Regulation. *Int. Rev. Financ. Anal.* **2024**, *96*, 103667. [\[CrossRef\]](#)
45. Wang, J.; Hu, X.; Zhong, A. Stock Market Reaction to Mandatory ESG Disclosure. *Financ. Res. Lett.* **2023**, *53*, 103402. [\[CrossRef\]](#)
46. Ren, X.Y.; Zheng, Y.X.; Zhou, N. Research on the influencing factors of traceability information sharing of agricultural product supply chain under the background of blockchain. *Int. J. Ind. Eng. Comput.* **2024**, *15*, 965–976. [\[CrossRef\]](#)
47. Zhu, L.L.; Xu, Y.P. Pharmaceutical Enterprises' Drug Quality Moran Process Strategy under Government Rewards and Punishments. *Manag. Rev.* **2025**, *37*, 214–223. [\[CrossRef\]](#)
48. Sun, S.H.; Su, Q. Four-Party Evolutionary Game Analysis of Quality Supervision of Medical Research Reports in Major Epidemic Period. *Chin. J. Manag.* **2020**, *17*, 1391–1401.
49. Ministry of Civil Affairs of the People's Republic of China. *Notice of the General Office of the Ministry of Civil Affairs on Carrying Out a Special Action for National Industry Associations and Chambers of Commerce to Serve High-Quality Development*; Ministry of Civil Affairs of the People's Republic of China: Beijing, China, 2023.
50. Zhang, Y.; Chen, L.; Battino, M. Blockchain: An emerging novel technology to upgrade the current fresh fruit supply chain. *Trends Food Sci. Technol.* **2022**, *124*, 1–12. [\[CrossRef\]](#)

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