RAIRO-Oper. Res. 60 (2026) 1151–1177
https://doi.org/10.1051/ro/2026004

RAIRO Operations Research
www.rairo-ro.org

STUDY ON CHARGING MODEL OF CLOUD MANUFACTURING SUPPLY CHAIN CONSIDERING DATA SECURITY UNDER BLOCKCHAIN TRACEABILITY TECHNOLOGY

Jing Wang*, Mengmeng Liu, Jiaying Fu and Shuang Fan

Abstract. Blockchain traceability technology enhances supply chain transparency and data security in cloud manufacturing supply chain, thereby affecting the choice of charging models. This paper innovatively integrates blockchain traceability technology with cloud data security management to construct a cloud manufacturing supply chain model that includes operators and suppliers. It conducts an in-depth analysis of equilibrium decisions under different charging models across varying levels of blockchain traceability technology, and designs a cost-sharing and revenue-sharing contract to coordinate the interests of all parties in the supply chain. It identifies four important results. First, as the level of blockchain traceability technology transitions from weak to strong, the service price, market demand, and profit levels for all parties in the cloud manufacturing supply chain show significant improvement. Second, the sensitivity coefficient of blockchain traceability technology and the elasticity coefficient of cloud data security positively influence the cloud data security level, blockchain traceability technology level, service price, demand, and profit, whereas the associated cost coefficients exert a negative influence. Third, he combined cost-sharing–revenue-sharing contract exhibits strong robustness and can effectively coordinate the cloud manufacturing supply chain, achieving Pareto improvement. Fourth, the strategic choices of the operator and the supplier are highly dependent on the revenue-sharing ratio. Both excessively high and low ratios lead to preference misalignment, which is further exacerbated by the cost coefficients of blockchain traceability technology and cloud data security management. However, when the ratio lies within a specific intermediate range, both parties consistently favor the revenue-sharing model. Increases in the sensitivity coefficient of blockchain traceability technology and the elasticity coefficient of cloud data security further widen this cooperative range.

Mathematics Subject Classification. 90B06, 91A80.

Received July 8, 2024. Accepted January 6, 2026.

1. Introduction

Cloud manufacturing, as a new industrial model that integrates cloud computing and big data analysis technology, is promoting the development of the manufacturing industry to the direction of networking, service and platform [1]. This transformation has completely reshaped the concept of traditional supply chain and

Keywords. Cloud manufacturing supply chain, blockchain traceability technology, cloud data security, Stackelberg game model, charging model research.

School of Economics and Management, Harbin University of Science and Technology, Harbin 150080, P.R. China.
*Corresponding author: wangjing_ ha@126.com

transformed it into a highly integrated system, covering not only the circulation of material products, but also the provision of value-added services [2], mainly involving demanders, cloud manufacturing platform operators and suppliers [3]. With the acceleration of the process of cloud manufacturing, a large amount of data continues to be uploaded to the cloud operator platform, and data security issues become increasingly prominent [4]. For instance, SolarWinds suffered a supply chain attack with malicious code implanted, impacting U.S. government departments and several Fortune Global 500 companies. The misconfiguration of a third-party cloud service platform outsourced by Toyota led to the exposure of users' sensitive core production data [5]. Competitors imitated its processes to seize market share, damaging its brand reputation. These cases are not isolated. According to the Cloud Security report, up to 24% of operators have experienced cloud security incidents. Not only do the operators themselves suffer losses, but the overall security and stability of the industrial chain are also endangered. Therefore, data security protection is of the utmost urgency. The introduction of blockchain traceability technology may serve as a viable solution, as it ensures real-time transparency of service status and information immutability [6], thereby effectively enhancing cloud data security. By integrating the capabilities of blockchain traceability, a security perimeter spanning the entire lifecycle of data – from generation and transmission to storage – can be established. This enables real-time risk awareness and globally credible traceability of transaction data [7], offering a valuable reference for enhancing data security in cloud manufacturing.

A reasonable charging model is the key to help operators apply blockchain traceability technology, achieve sustainable development, and balance the interests of cloud members. Amazon Web Services (AWS) for example, its contracts require users to prepay fixed long-term fees that are non-cancellable and non-refundable for unused portions. When actual demand falls below projections, low resource utilization exposes users to financial waste, prompting some to migrate toward more flexible pay-as-you-go models [8]. Similarly, Google Cloud's data egress fees substantially increase the cost for users to switch providers or adopt multi-cloud strategies. This has led some customers – faced with opaque pricing and migration barriers – to discontinue service and opt for platforms with greater cost transparency [9]. The above events show that if the charging model is not properly set, enterprises may face problems such as user loss, reduced return on investment, limited innovation, and reduced service quality, all of which will have a negative impact on the long-term sustainable development of enterprises. Therefore, designing a reasonable charging model is crucial to balance the needs of stakeholders, ensure financial stability and maintain market competitiveness. To sum up, the rise of cloud manufacturing not only promotes the modernization transformation of the manufacturing industry, but also brings challenges such as data security and charging models. The use of blockchain traceability technology can improve the transparency and security of data transactions. At the same time, the reasonable design of the charging model is crucial to ensure the harmony of interests of all participants and the sustainable development of the platform, which requires close cooperation and continuous exploration among operators, suppliers and demanders.

Although researchers have explored the charging models in cloud manufacturing supply chain management, cite a few the roles of blockchain traceability technology and cloud data security are often overlooked. Therefore, this study aims to explore the impact of the application of blockchain traceability technology and the security level of cloud data on the charging model and the optimal service price. We try to answer the following questions: (1) What factors influence the levels of blockchain traceability technology and cloud data security in a cloud manufacturing supply chain? (2) How do blockchain traceability technology and cloud data security affect the profits of supply chain members and their choice of charging model? (3) Under what conditions do cloud manufacturing platform operators and suppliers choose the fixed service fee model and revenue-sharing model?

To address the above questions systematically, we construct a two-echelon cloud manufacturing supply chain comprising one cloud manufacturing platform operator and one cloud manufacturing supplier. As the rule-setter and dominant actor in the supply chain, the operator makes decisions first, while the supplier, acting as the follower, responds accordingly [10]. Based on this sequential decision-making structure, we employ a Stackelberg game model to characterize the strategic interaction between the operator and the supplier. Subsequently, under both strong and weak blockchain traceability technology scenarios, we derive the optimal pricing strategies for the fixed service fee model and the revenue-sharing model, both of which incorporate blockchain traceability

technology and consider cloud data security. Then, we analyze the optimal decisions of supply chain members under varying levels of blockchain traceability technology and different charging models. Furthermore, we design a cost sharing-revenue sharing contract for a cloud manufacturing supply chain coordination in the dynamic context.

Section 2 summarizes the existing literature. Section 3 states the problem description and model assumptions. Section 4 present the construction and solution analysis of the models. Section 5 designs the cost sharing – revenue sharing contract. Section 6 conducts a numerical analysis and discussion. Section 7 provides conclusions.

2. Literature review

The literature related to this paper mainly falls into the following three categories: the supply chain management considering data security, application of blockchain traceability technology in supply chain management and supply chain charging model.

One is the supply chain research considering data security. The continuous development of information technology and consumers' concern for privacy protection have pushed data security to the forefront [11, 12]. Numerous data breach incidents indicate that supply chain vulnerabilities have become the weakest link in corporate data protection systems. Supply chain members must establish transparent security mechanisms and contingency plans to ensure consumer information security, thereby preventing erosion of consumer trust and avoiding legal liabilities [13, 14].While privacy-preserving and cryptographic solutions such as homomorphic encryption [15], hash algorithms, and differential privacy [16] – effectively enhance data security within the supply chain, they struggle to address the challenges posed by over-reliance on central nodes, which can lead to information silos and persistent security risks [17]. In contrast, decentralized technologies like blockchain and federated learning help mitigate data security risks across the supply chain. For instance, Tsang *et al.* [18] utilized blockchain to partition the network into multiple shards for data management, while Yao *et al.* [19] employed blockchain to track all transactions on the network, storing transaction data in distributed ledgers maintained across nodes, thereby ensuring data integrity and traceability and enhancing consumer acceptance of cloud services. Additionally, vertical federated learning methods based on compressed sensing reduce communication costs and data leakage risks while preserving model accuracy [20]. Beyond technical solutions, some scholars have also explored the allocation of data security responsibilities and security investment strategies among supply chain members. For example, Yang *et al.* [21] argued that data security responsibilities in cloud services should be shared between the service provider and the user, and developed an incentive mechanism for security investments by both parties. Although the academic community has achieved substantial progress in supply chain data security management, research on the role of specific technologies in motivating security investments by supply chain members remains relatively limited. Moreover, indiscriminately increasing data security levels can raise operational costs for supply chain members and may even reduce overall supply chain efficiency [22]. Therefore, studying the balance between supply chain data security and economic performance is of critical importance.

The second category is supply chain research that considers blockchain traceability technology. In today's business environment, the supply chain is faced with problems such as information asymmetry, which makes it difficult for all links to cooperate, and easy data tampering, which makes it difficult to establish trust. Blockchain technology has become a powerful tool to solve these problems due to its decentralized and immutable characteristics [23, 24]. Block chain is mainly divided into perishable block chain and public block chain. The public block chain is open to everyone, while the perishable block chain has certain access restrictions and is more suitable for cooperative applications among enterprises [25]. The type of block chain studied in this paper belongs to perishable block chain. The adoption of blockchain traceability technology in supply chains is influenced by factors such as consumers' traceability awareness and the associated technological investment costs [26]. The optimal timing for its implementation is determined by the level of consumer privacy concern and technological preference [6]. The introduction of blockchain traceability technology provides a novel approach to enhancing data privacy protection within supply chains [27]. Khan *et al.* [28] have employed methods including text data

encryption, permission-based access control, and hash verification to ensure data security and privacy. Xu *et al.* [29] utilized multi-authority attribute-based encryption and an optimization framework to achieve fine-grained data access control while balancing related factors for privacy preservation. As supply chains become increasingly refined, the role of blockchain traceability technology and its associated data privacy protection mechanisms grows more prominent. For instance, in cross-border e-commerce supply chains, platforms leverage blockchain traceability for product quality verification, which enhances user trust [30]. When integrated into perishable goods supply chains, such as agricultural products, the protected and credible data fundamentally influence market demand and help optimize pricing strategies and economic outcomes for supply chain actors [31,32]. In cloud platforms built for automotive manufacturing supply chains, blockchain-based smart contracts are employed as a traceability solution to ensure the authenticity and transparency of critical data exchanged between upstream and downstream enterprises, thereby improving supply chain coordination efficiency [33]. Furthermore, smart contracts, as the core component of blockchain traceability technology, are reshaping collaboration paradigms in cloud manufacturing supply chains. Even if a particular link is attacked or fails, the overall system can maintain transparent and reliable operations, which strengthens supply chain resilience [34]. Additionally, by leveraging blockchain traceability, abstract "sustainability" metrics can be translated into auditable, verifiable on-chain data points. This increases transparency, reduces energy consumption, and enhances the sustainability of cloud manufacturing supply chains [35]. While the academic community has extensively investigated the role of blockchain traceability technology in protecting supply chain data privacy and its broader impact on supply chains, research within the cloud manufacturing context has predominantly focused on macro-level issues such as its effects on supply chain collaboration, resilience, and sustainability. In contrast, micro-level aspects, including pricing and profit distribution, have received comparatively limited attention.

The third category is the study of the supply chain charging model. Under the membership fee and transaction fee model, based on the two-sided market theory, the optimal pricing strategy of the cloud manufacturing supply chain is analyzed. The optimal pricing strategy is determined by the number of transactions within the platform. The bilateral charging transaction fee model is better when the number of transactions is large, and the bilateral charging membership fee is better when the number of transactions is small [36]. In the registration fee mode, operators can quickly raise a large amount of funds in a short time, avoid bad debts, and use it for investment, making the registration fee pricing significantly better than the transaction fee in the bilateral market competition [37]. Under the two models of fixed service fee and registration fee, considering the impact of users' time sensitivity on the charging model of cloud manufacturing supply chain, the maximum profit of the platform is positively correlated with the cross-network externality coefficient and negatively correlated with the time sensitivity coefficient of the capacity demand side [38]. There are different thresholds of platform value-added service effect under usage charging and subscription charging models. When the service effect is in different threshold ranges, the manufacturer will choose subscription charging model or per-usage charging model [39]. The revenue-sharing model refers to a pricing arrangement in which the service operator collects a predetermined percentage of the transaction value as a service fee. Representative examples include mobile network operators sharing data traffic revenue with third-party service providers for specific internet services [40], and ride-hailing aggregation platforms taking a share of the income generated by transportation service providers [41]. In cloud manufacturing supply chains, members share a portion of the incremental revenue gained from using cloud services with the cloud service provider, often in exchange for reduced subscription fees or enhanced security support [3]. The appropriateness of the revenue-sharing ratio plays a crucial role in shaping supply chain pricing and profitability [41]. The integration of new-generation information technologies into supply chains has reshaped decisions regarding charging model selection, pricing strategies, and optimal profit distribution [42]. Therefore, further research is warranted to determine the optimal charging model, pricing strategy, and resulting profit distribution following the integration of blockchain traceability technology into cloud manufacturing supply chains.

In summary, while existing research has extensively explored data security management in supply chains, the impact of blockchain traceability technology on supply chain data security, revenue, collaboration, and sustainability, as well as the role of charging models in shaping pricing strategies and profitability, it has yet to

fully elucidate the interplay between blockchain traceability technology and cloud data security. Furthermore, the combined influence of these two factors on the selection of charging models, the formulation of pricing strategies, and the resulting profit distribution within cloud manufacturing supply chains remains insufficiently examined. Therefore, this study focuses on key decision variables including optimal service price, blockchain traceability technology level, and cloud data security level in a cloud manufacturing supply chain that implements blockchain traceability technology. It investigates the selection of charging models by the cloud manufacturing platform operator and the supplier, and further designs a Cost-Sharing–Revenue-Sharing Contract to coordinate the supply chain. The fixed service fee model provides stable revenue, facilitating cost planning and user expectation management. The revenue-sharing model aligns the interests of the operator and the supplier, enabling risk-sharing and benefit-sharing. While flexible models, such as pay-as-you-go, offer adaptability, they are often unsuitable for cloud manufacturing supply chains because the value of cloud manufacturing services is difficult to quantify, a difficulty that arises from industry-specific and hard-to-standardize parameters such as machining accuracy and process complexity. Therefore, this study selects the revenue-sharing model and the fixed service fee model as the charging modes for investigation within the cloud manufacturing supply chain context. The contributions of this study are threefold. First, it adopts a novel perspective by simultaneously incorporating blockchain traceability technology and cloud data security into the operational decision-making framework of a cloud manufacturing supply chain. Under different charging models, it explores the optimal levels of blockchain traceability technology and cloud data security that maximize supply chain profit while satisfying data security requirements. Second, the study develops game-theoretic models for the cloud manufacturing supply chain under different charging models and blockchain traceability technology level. It conducts an in-depth analysis of the roles and impacts of the fixed service fee model and the revenue-sharing model, and investigates the optimal charging model selection for both the cloud manufacturing platform operator and the supplier. Third, the study designs a Cost-Sharing–Revenue-Sharing Contract under the fixed service fee model to incentivize cooperation between the operator and the supplier in adopting blockchain traceability technology and enhancing data security. It demonstrates that this contract can achieve coordinated outcomes in a cloud manufacturing supply chain governed by blockchain traceability and data security management. Furthermore, the study identifies how specific factors, including the data security management cost coefficient and the cloud data security elasticity coefficient, influence product/service pricing, optimal profit, and charging model selection under varying levels of blockchain traceability technology within the cloud manufacturing supply chain. The study contributes to the literature by filling a theoretical gap in data security management for cloud manufacturing supply chains, offering decision support for the application of blockchain traceability technology in this specific context, and providing new theoretical support and practical guidance for the coordination management of cloud manufacturing supply chains.

3. Problem description and model assumptions

3.1. Problem description

Consider a cloud manufacturing supply chain system comprising a cloud manufacturing platform operator (F) and a cloud manufacturing supplier (R), integrated with blockchain traceability technology and data security mechanisms. Facing increasingly stringent privacy laws and data security regulations, the cloud manufacturing platform operator provides a certain level of cloud data security services to the supplier and adopts a charging model to collect service fees. For instance, the Salesforce platform charges its enterprise users a fixed periodic subscription fee [43], while AWS deducts a percentage of the supplier's revenue from each transaction as a service compensation [5]. Inspired by these two prevalent practices, we categorize the charging models into the fixed service fee model and the revenue-sharing model. Under the fixed service fee model, the operator charges the supplier a fixed amount w per transaction. Under the revenue-sharing model, the operator collects a ratio ϕ of the supplier's revenue from each transaction. The supplier, in turn, sells the product to consumers at a price p. It should be noted that, in accordance with Article 82 of the General Data Protection Regulation (GDPR) [44], data subjects (*i.e.*, users) have the right to claim compensation for damages resulting from violations of data

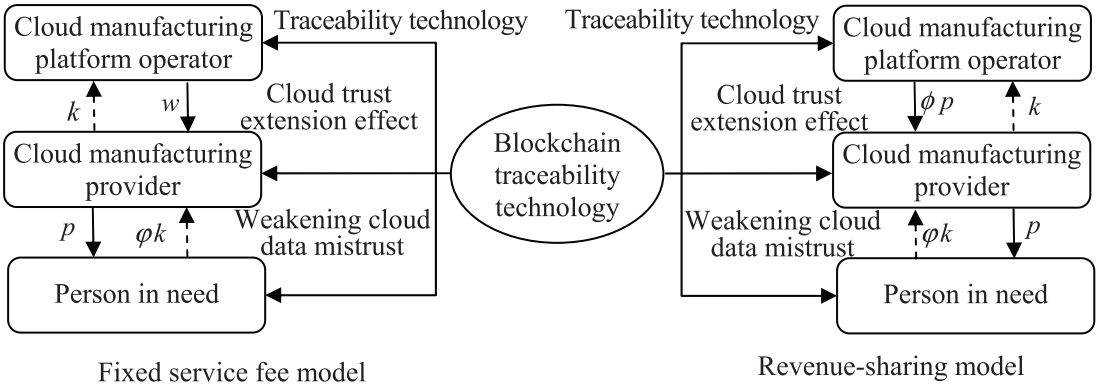

FIGURE 1. The structure of the cloud manufacturing supply chain.

protection regulations. This implies that if the actual cloud data security level provided by the operator fails to meet the promised standard – *i.e.*, a service failure occurs – the supplier may seek corresponding cloud data security compensation k from the operator. In such cases, blockchain traceability technology plays a critical role, not only in attributing liability but also in determining the supplier's liability coefficient φ in the event of potential cloud data security incidents. Should a cloud data security issue arise due to improper operations by the supplier, consumers may claim corresponding cloud data security compensation φk from the supplier. For example, in July 2018, Tencent Cloud experienced a server failure that resulted in the loss of data belonging to Frontier Numerical Control Technology, failing to meet the previously committed cloud data security level. As a result, Tencent Cloud was required to pay corresponding data security compensation [45]. The structure of the cloud manufacturing supply chain is shown in Figure 1.

3.2. Model assumptions

The following assumptions are introduced to inform the model, reflecting the decision-making logic of cloud supply chain participants and ensuring the feasibility of key variables.

(1) Platform operators and suppliers are rational decision makers, and there is a Stackelberg game relationship between them, with operators as leaders and suppliers as followers [46].

(2) The demand function D consists of two components: a market benchmark demand D_0 and a fluctuating demand ΔD, *i.e.*, $D = D_0 + \Delta D$. The market benchmark demand is normalized to $D_0 = 1$ [47]. The fluctuating demand, defined as $\Delta D = \Delta D' + \Delta D''$, is formulated as a nonlinear function of the service price, the cloud data security, and blockchain traceability technology [26, 29]. Here, $\Delta D' = -\alpha p + \beta g$ captures the linear perturbations in demand caused by price and cloud data security level, while $\Delta D'' = \epsilon\delta - \epsilon\delta^2$ captures the inverted U-shaped impact of blockchain traceability technology on demand growth. In the early stages of blockchain traceability technology adoption, an excess "technology dividend" stimulates a rapid surge in market demand. As the technology gradually matures, the growth in demand slows and eventually experiences a gradual decline. Thus, the total demand function can be expressed as $D = 1 - \alpha p + \beta g + \delta - \delta^2$.

(3) To enhance trust among demand-side users, the platform operator has adopted blockchain traceability technology. The investment cost of this technology is denoted as $\frac{1}{2}\theta\delta^2 t^{-\gamma}$ [48]. We assume that the investment cost exhibits a quadratic relationship with the level of the blockchain traceability technology implemented. Furthermore, driven by ongoing technological progress, the investment cost is expected to decrease gradually over time [49].

(4) To further strengthen demand-side confidence in the service, the platform operator can commit to a higher cloud data security level, denoted as g, thereby ensuring data security during transmission, storage, and processing and mitigating the risks of data breaches or tampering. The operator concurrently bears the

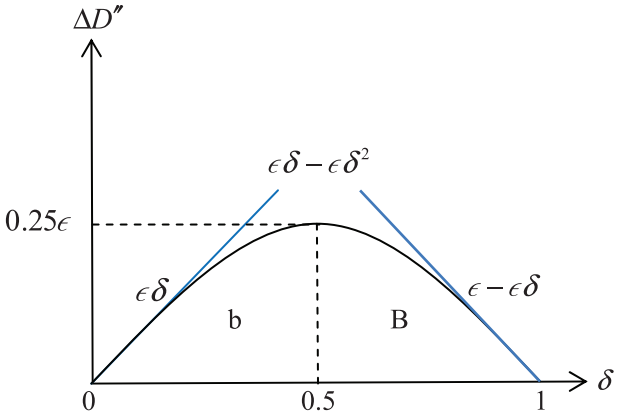

FIGURE 2. Nonlinear fluctuating demand function and its tangent functions.

associated additional costs. It is assumed that the cloud data security cost is a quadratic function of the the level of cloud data security over time t, expressed as $\eta g^2 t^{-\gamma}$ [50]. Blockchain traceability technology enhances the operator's capability to resist data attacks. The more advanced this technology is, the more significantly the cloud data security cost decreases over time [51]. Furthermore, since cloud data security directly influences users' perception of service quality and consequently determines service success or failure, g can be interpreted as the probability of service success [52].

(5) Referring to the assumptions in [26,41], the revenue sharing ratio ϕ is an exogenous variable, and $\phi \in (0,1)$.

(6) Referring to the assumptions in [12, 42], in order to ensure the negative characterization of the Hessian matrix in the text and the economic feasibility of the expression of the correlation function, it is assumed that $-8\alpha\eta\theta + t^{\gamma}(2\epsilon^2\eta + \theta(\beta + k\alpha\varphi)^2) < 0$, $8t^{-\gamma}\alpha\eta - (\beta + k\alpha\varphi)^2 > 0$.

Table 1 lists the main symbols in this paper.

4. MODELING

4.1. Linearization of demand function

To ensure mathematical tractability and enable the efficient derivation of the optimal solution using commercial optimization software, this study employs a piecewise linearization method to approximate the nonlinear fluctuating demand function $\Delta D'' = \epsilon\delta - \epsilon\delta^2$ [53]. As illustrated in Figure 2, the vertex of the $\Delta D''$ function is selected as the breakpoint, dividing $\Delta D''$ into two intervals: weak blockchain traceability technology levels ($0 < \delta \leq 0.5$, Scenario b) and strong blockchain traceability technology levels ($0.5 < \delta < 1$, Scenario B). The original nonlinear function is replaced by linear expressions corresponding to the tangents of the function curve in each interval, as shown in equation (1). The demand function D after piecewise linearization is given by equation (2).

$$\Delta D'' = \begin{cases} \epsilon\delta & (0 < \delta \leq 0.5) \\ \epsilon - \epsilon\delta & (0.5 < \delta < 1) \end{cases} \tag{1}$$

$$D = \begin{cases} 1 - \alpha p + \beta g + \epsilon\delta & (0 < \delta \leq 0.5) \\ 1 - \alpha p + \beta g + \epsilon - \epsilon\delta & (0.5 < \delta < 1)\,. \end{cases} \tag{2}$$

TABLE 1. Main symbols and explanations.

Symbol	Explanations
g	The cloud data security level can be equivalently interpreted as the probability of service success, $g\,(0 < g < 1)$, A higher value of g, closer to 1, indicates a greater cloud data security level and corresponds to a higher probability of service success. Conversely, $1 - g$ defines the probability of service failure.
δ	Blockchain traceability technology level $\delta\,(0 < \delta < 1)$
α	The price sensitivity coefficient of cloud manufacturing services
ϵ	The sensitivity coefficient of blockchain traceability technology $\epsilon\,(0 < \epsilon < 1)$
β	The elasticity coefficient of cloud data security
η	The investment cost coefficient of cloud data security management
θ	The investment cost coefficient of blockchain traceability technology
t	Time
γ	Factors influencing technological progress
p	Price of products or services paid by consumers to suppliers
w	Fixed service fees paid by suppliers to operators
ϕ	Revenue sharing ratio of operators
k	Cloud data security compensation paid by the operator in the event of service failure
φ	The supplier's liability coefficient, *i.e.*, the proportion of compensation provided to the consumer upon service failure
D/D_0	Demand/Market benchmark demand
$\Delta D/\Delta D'/\Delta D''$	Fluctuating demand/Linear fluctuation demand/Nonlinear fluctuation demand
$\pi_F/\pi_R/\pi_T$	Profit of operators/suppliers/cloud manufacturing supply chain

4.2. Fixed service fee model (Model s)

In model s, the order of the game is: the operator of the cloud manufacturing platform decides the level of blockchain traceability technology δ, the level of cloud data security g and the service fee w, and then the supplier decides the service price p charged to the demand side. The profit functions of the operator and the supplier are respectively

$$\pi_F^{\mathrm{s}} = D\left(gw + (1-g)(w-k)\right) - \frac{1}{2}\theta t^{-\gamma}\delta^2 - \eta t^{-\gamma} g^2 \tag{3}$$

$$\pi_R^{\mathrm{s}} = D\left(g(p-w) + (1-g)(p-w+k-\varphi k)\right). \tag{4}$$

4.2.1. Weak blockchain traceability technology level (Scenario b)

First of all, by inverse induction on (4) about the service price p for the first and second order partial derivatives, can be obtained $\frac{\partial \pi_R^{\mathrm{s}}}{\partial p} = 1 - 2p\alpha + w\alpha + g\beta + \delta\epsilon + k\alpha(-1+g+\varphi-g\varphi)$, $\frac{\partial^2 \pi_R^{\mathrm{s}}}{\partial p^2} = -2\alpha < 0$, therefore π_R^{s} is a strictly concave function of p. Therefore, letting its first order derivative equal to 0, we can find the unique optimal response function of the operator regarding p to the supplier's decision as $p^{\mathrm{sb}^*} = \frac{1+w\alpha+g\beta+\delta\epsilon+k\alpha(-1+g+\varphi-g\varphi)}{2\alpha}$, substituting p^{sb^*} into the operator's profit function, the third-order Hessian matrix of π_F^{sb} regarding g, δ, w, is $H^{\mathrm{sb}} = \begin{pmatrix} -\alpha & \frac{1}{2}(\beta + k\alpha(-2+\varphi)) & \frac{\epsilon}{2} \\ \frac{1}{2}(\beta + k\alpha(-2+\varphi)) & -2t^{-\gamma}\eta + k(\beta + k\alpha(-1+\varphi)) & \frac{k\epsilon}{2} \\ \frac{\epsilon}{2} & \frac{k\epsilon}{2} & -t^{-\gamma}\theta \end{pmatrix}$, because $\frac{1}{4}(8t^{-\gamma}\alpha\eta - (\beta + k\alpha\varphi)^2) > 0$, $|H^{sb}| = \frac{1}{4}t^{-2\gamma}(-8\alpha\eta\theta + t^{\gamma}(2\epsilon^2\eta + \theta(\beta + k\alpha\varphi)^2)) < 0$, therefore Hessian matrix is negative definite, $\pi_{\mathrm{F}}^{\mathrm{sb}}$ is a strictly differentiable concave function of g, δ, w, so there is the

unique optimal service fee $w^{sb^*} = \frac{4\eta\theta(1-k\alpha(-2+\varphi))-kt^\gamma\left(2\epsilon^2\eta+(1+\beta)\theta(\beta+k\alpha\varphi)\right)}{8\alpha\eta\theta-t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)}$, the optimal blockchain traceability technology level $\delta^{sb^*} = \frac{2t^\gamma\epsilon\eta(-1+k\alpha\varphi)}{-8\alpha\eta\theta+t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)}$ and the optimal level of cloud data security $g^{sb^*} = \frac{t^\gamma\theta(-1+k\alpha\varphi)(\beta+k\alpha\varphi)}{-8\alpha\eta\theta+t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)}$. Substituting the equilibrium solution of $(w^{sb^*}, g^{sb^*}, \delta^{sb^*})$ into p^{sb^*} can be obtained as: $p^{sb^*} = \frac{-2\eta\theta(3+k\alpha\varphi)+kt^\gamma\varphi\left(2\epsilon^2\eta+(1+\beta)\theta(\beta+k\alpha\varphi)\right)}{-8\alpha\eta\theta+t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)}$, the profit function of the cloud manufacturing platform operator and the cloud manufacturing supplier are, $\pi_F^{sb^*} = \frac{\eta\theta(-1+k\alpha\varphi)^2}{8\alpha\eta\theta-t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)}$, $\pi_R^{sb^*} = \frac{4\alpha\eta^2\theta^2(-1+k\alpha\varphi)^2}{\left(-8\alpha\eta\theta+t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)\right)^2}$, and the demand function is $D^{sb^*} = \frac{2\alpha\eta\theta(-1+k\alpha\varphi)}{-8\alpha\eta\theta+t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)}$.

Property 4.1. The impact of cloud data security elasticity factor and blockchain traceability technology sensitivity factor on supply chain decision making and profitability: (1) $\frac{\partial p^{sb^*}}{\partial\beta} > 0$, $\frac{\partial w^{sb^*}}{\partial\beta} > 0$, $\frac{\partial\delta^{sb^*}}{\partial\beta} > 0$, $\frac{\partial g^{sb^*}}{\partial\beta} > 0$, $\frac{\partial\pi_F^{sb^*}}{\partial\beta} > 0$, $\frac{\partial\pi_R^{sb^*}}{\partial\beta} > 0$, $\frac{\partial D^{sb^*}}{\partial\beta} > 0$; (2) $\frac{\partial p^{sb^*}}{\partial\epsilon} > 0$, $\frac{\partial w^{sb^*}}{\partial\epsilon} > 0$, $\frac{\partial\delta^{sb^*}}{\partial\epsilon} > 0$, $\frac{\partial g^{sb^*}}{\partial\epsilon} > 0$, $\frac{\partial\pi_F^{sb^*}}{\partial\epsilon} > 0$, $\frac{\partial\pi_R^{sb^*}}{\partial\epsilon} > 0$, $\frac{\partial D^{sb^*}}{\partial\epsilon} > 0$.

Proof. Consider $\frac{\partial p^{sb^*}}{\partial\beta}$ as an example.

$\frac{\partial p^{sb^*}}{\partial\beta} = \frac{t^\gamma\theta(-1+k\alpha\varphi)\left(-4\eta\theta(3\beta+k\alpha\varphi)+kt^\gamma\varphi\left(-2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)\right)}{\left(-8\alpha\eta\theta+t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)\right)^2}$, where $(-8\alpha\eta\theta + t^\gamma(2\epsilon^2\eta + \theta(\beta + k\alpha\varphi)^2))^2$ is the square term greater than 0. By the parametric property $-1 + k\alpha\varphi < 0$, $-4\eta\theta(3\beta + k\alpha\varphi) + kt^\gamma\varphi(-2\epsilon^2\eta + \theta(\beta + k\alpha\varphi)^2) < 0$, so $\frac{\partial p^{sb^*}}{\partial\beta} > 0$. Other properties are known by inference. □

Property 4.1 indicates that when the elasticity coefficient of cloud data security and the sensitivity coefficient of blockchain traceability technology increase, the security degree of cloud data, the level of blockchain traceability technology, the demand, the service price, the fixed service fee, and the profit of operators and suppliers will increase accordingly. The increase of elasticity coefficient of data security means that the demanders attach more importance to data privacy and security. The increase in the sensitivity coefficient of blockchain traceability technology indicates that the market is becoming more sensitive to the transparency and traceability of product or service data. In order to meet these needs, operators will not only increase their investment in cloud data security technology, but also improve blockchain traceability technology, thereby improving the overall level of data security and technical transparency. The overall added value of the product or service can be improved, and the market demand will increase significantly. As demand and technology rise in tandem, operators and suppliers can raise their service prices and fixed service charges accordingly. In the end, operators' and suppliers' profits will also be significantly improved, and the cloud manufacturing supply chain will have higher profit opportunities. However, the conclusions of this research model are mainly applicable to cloud manufacturing supply chains with relatively mature technologies and markets. For small manufacturers, especially in the early stages of technology, the earnings boost may not be as significant as for large enterprises due to the high cost of blockchain investment. This is mainly because the high investment cost of early-stage blockchain traceability technology may put pressure on the capital flow of small enterprises, causing them to be unable to recover their investment as quickly as large-scale supply chains, and may even face limitations in the application of the technology. Therefore, in this case, the impact of blockchain traceability technology on the overall performance of the cloud manufacturing supply chain may be more limited.

In practice, Turkey's Paribu exchange has implemented a multi-layered security framework – comprising localized education programs, dynamic cold and hot wallet segregation, and third-party audited proof of reserves – to significantly enhance consumer awareness and trust in blockchain traceability technology and data security [54]. This comprehensive approach has not only strengthened consumer confidence, leading to increased adoption for cryptocurrency transactions platform, but has also created a positive feedback loop, incentivizing the operator to further invest in blockchain and data security enhancements.

Property 4.2. The impact of blockchain traceability technology and cloud data security management cost coefficient on supply chain decision making and profit: (1) $\frac{\partial p^{sb^*}}{\partial \theta} < 0$, $\frac{\partial w^{sb^*}}{\partial \theta} < 0$, $\frac{\partial \delta^{sb^*}}{\partial \theta} < 0$, $\frac{\partial g^{sb^*}}{\partial \theta} < 0$, $\frac{\partial \pi_F^{sb^*}}{\partial \theta} < 0$, $\frac{\partial \pi_R^{sb^*}}{\partial \theta} < 0$, $\frac{\partial D^{sb^*}}{\partial \theta} < 0$; (2) $\frac{\partial p^{sb^*}}{\partial \eta} < 0$, $\frac{\partial w^{sb^*}}{\partial \eta} < 0$, $\frac{\partial \delta^{sb^*}}{\partial \eta} < 0$, $\frac{\partial g^{sb^*}}{\partial \eta} < 0$, $\frac{\partial \pi_F^{sb^*}}{\partial \eta} < 0$, $\frac{\partial \pi_R^{sb^*}}{\partial \eta} < 0$, $\frac{\partial D^{sb^*}}{\partial \eta} < 0$.

Proof. Take $\frac{\partial p^{sb^*}}{\partial \theta} < 0$ as example $\frac{\partial p^{sb^*}}{\partial \theta} = -\frac{2t^\gamma \epsilon^2 \eta(-1+k\alpha\varphi)(-6\eta+kt^\gamma\varphi(\beta+k\alpha\varphi))}{\left(-8\alpha\eta\theta+t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)\right)^2}$, where $(-8\alpha\eta\theta + t^\gamma(2\epsilon^2\eta + \theta(\beta + k\alpha\varphi)^2))^2$ is a quadratic term greater than 0. By the parametric property $-1 + k\alpha\varphi < 0$, $-6\eta + kt^\gamma\varphi(\beta + k\alpha\varphi) > 0$, so $\frac{\partial p^{sb^*}}{\partial \theta} < 0$. Other properties are known by inference from this. □

Property 4.2 indicates that when the cost coefficient of blockchain traceability technology and cloud data security management increases, the security degree of cloud data, the level of blockchain traceability technology, the demand, the service price, the fixed service fee, and the profits of operators and suppliers will decrease accordingly under the fixed service fee model. When the cost coefficient of blockchain traceability technology and the cost coefficient of cloud data security management increase, the cost of the operator in the traceability will increase, and the cost of the operator in maintaining data security will increase. In the face of increasing cost pressure, operators have to make compromises and reduce their investment in data security, which will lead to a decline in the overall cloud data security of the product, which will affect the trust of the demander and ultimately lead to a decrease in market demand. In response to this trend and to remain competitive in the market, vendors may reduce the price of their services, but this will further compress the profit margins of operators and suppliers throughout the cloud manufacturing supply chain. The assumptions of this study are based on the more mature technology and market environment in the cloud manufacturing supply chain. However, for smaller, early-stage suppliers and operators, excessive blockchain traceability technology and cloud data security management costs may adversely affect their profitability models, leading to greater pressure on these enterprises to invest in technology. Therefore, for cloud manufacturing supply chains of different sizes and technology maturity, the increase in costs may have a more significant impact on small enterprises, leading to further compression of their profit room.

In reality, the platform has carried out digital transformation through Inspur Yunzhou Industrial Internet platform, which has effectively reduced costs and enhanced market competitiveness with the help of cloud computing and advanced data security technologies [55]. By integrating cloud services and blockchain traceability technology, the platform not only improves the security and transparency of data, but also provides the platform with flexible resource allocation and real-time monitoring capabilities, helping it maintain a competitive edge by optimizing resource allocation in the face of cost pressure. Through this transformation, the platform is able to maintain technological leadership and ensure a favorable position in a highly competitive environment, thus achieving sustained growth and stable profitability.

4.2.2. Strong blockchain traceability technology level (Scenario B)

The computational procedure and properties for this scenario are consistent with those presented in Section 4.2.1, therefore, the detailed derivation and property analysis are omitted here. The corresponding equilibrium outcomes are summarized in Table 2.

4.3. Revenue-sharing model (Model n)

In the model n, the operator receives a commission fee from the provider as a source of profit. This commission fee is equivalent to a certain percentage of the supplier's revenue, *i.e.*, the revenue share ratio. The order of the game is: the operator decides the level of blockchain traceability technology and the level of cloud data security, and then the supplier decides the service price. The profit functions of the operator and the supplier are:

$$\pi_F^n = \phi pD - (1-g)kD - \frac{1}{2}\theta t^{-\gamma}\delta^2 - \eta t^{-\gamma} g^2 \tag{5}$$

$$\pi_R^n = (1-\phi)pD + k(1-\varphi)(1-g)D. \tag{6}$$

TABLE 2. Equilibrium outcomes under the fixed service fee model in strong blockchain traceability technology level (Scenario B).

Equilibrium outcomes
$w^{\mathrm{sB}^*} = \dfrac{-4\eta\theta\left(1+\epsilon-k\alpha(-2+\varphi)\right)+kt^{\gamma}\left(\beta(1+\beta)\theta+\epsilon(2\epsilon\eta+\beta\theta)+k\alpha(1+\beta+\epsilon)\varphi\right)}{-8\alpha\eta\theta+t^{\gamma}\left(2\epsilon^2\eta+\theta\left(\beta+k\alpha\varphi\right)^2\right)}$
$\delta^{\mathrm{sB}^*} = \dfrac{2t^{\gamma}\epsilon\eta\left(1+\epsilon-k\alpha\varphi\right)}{-8\alpha\eta\theta+t^{\gamma}\left(2\epsilon^2\eta+\theta\left(\beta+k\alpha\varphi\right)^2\right)}$
$g^{\mathrm{sB}^*} = -\dfrac{t^{\gamma}\theta\left(1+\epsilon-k\alpha\varphi\right)\left(\beta+k\alpha\varphi\right)}{-8\alpha\eta\theta+t^{\gamma}\left(2\epsilon^2\eta+\theta\left(\beta+k\alpha\varphi\right)^2\right)}$
$p^{\mathrm{sB}^*} = \dfrac{2kt^{\gamma}\epsilon^2\eta\varphi+kt^{\gamma}\left(1+\beta+\epsilon\right)\theta\varphi\left(\beta+k\alpha\varphi\right)-2\eta\theta\left(3+3\epsilon+k\alpha\varphi\right)}{-8\alpha\eta\theta+t^{\gamma}\left(2\epsilon^2\eta+\theta\left(\beta+k\alpha\varphi\right)^2\right)}$
$D^{\mathrm{sB}^*} = \dfrac{2\alpha\eta\theta\left(-1-\epsilon+k\alpha\varphi\right)}{-8\alpha\eta\theta+t^{\gamma}\left(2\epsilon^2\eta+\theta\left(\beta+k\alpha\varphi\right)^2\right)}$
$\pi_F^{\mathrm{sB}^*} = \dfrac{\eta\theta\left(1+\epsilon-k\alpha\varphi\right)^2}{8\alpha\eta\theta-t^{\gamma}\left(2\epsilon^2\eta+\theta\left(\beta+k\alpha\varphi\right)^2\right)}$
$\pi_R^{\mathrm{sB}^*} = \dfrac{4\alpha\eta^2\theta^2\left(1+\epsilon-k\alpha\varphi\right)^2}{\left(-8\alpha\eta\theta+t^{\gamma}\left(2\epsilon^2\eta+\theta\left(\beta+k\alpha\varphi\right)^2\right)\right)^2}$

4.3.1. Weak blockchain traceability technology level (Scenario b)

From $\frac{\partial^2\pi_R^{\mathrm{n}}}{\partial p^2} = 2\alpha(\phi-1) < 0$, it is known that there exists an optimal service price p such that π_R^{n} is maximum. Let $\frac{\partial\pi_R^{\mathrm{n}}}{\partial p} = 0$, find $p = \frac{1}{2}(\frac{1+g\beta+\delta\epsilon}{\alpha}+\frac{(-1+g)k(-1+\varphi)}{-1+\phi})$. Substituting p into the cloud manufacturing provider's operator profit function π_F^{n}, we obtain π_F^{n} the Hessian matrix with respect to (δ, g), $H^{\mathrm{nb}} = \begin{pmatrix} k\beta-2t^{-\gamma}\eta+\frac{\beta^2\phi}{2\alpha}-\frac{k^2\alpha(-1+\varphi)(-2+\phi+\phi\varphi)}{2(-1+\phi)^2} & \frac{\epsilon(k\alpha+\beta\phi)}{2\alpha} \\ \frac{\epsilon(k\alpha+\beta\phi)}{2\alpha} & -t^{-\gamma}\theta+\frac{\epsilon^2\phi}{2\alpha} \end{pmatrix}$. If $\left|H^{\mathrm{nb}}\right| = \frac{1}{4}t^{-2\gamma}\left(-4kt^{\gamma}\beta\theta+8\eta\theta-\frac{2t^{\gamma}\left(2\epsilon^2\eta+\beta^2\theta\right)\phi}{\alpha}+\frac{k^2t^{\gamma}\left(-t^{\gamma}\epsilon^2(-1+\phi\varphi)^2+2\alpha\theta(-1+\varphi)(-2+\phi+\phi\varphi)\right)}{(-1+\phi)^2}\right) > 0$, H is strictly negative definite, and $\delta^{\mathrm{nb}^*} = -\frac{t^{\gamma}\epsilon\times A}{M+t^{\gamma}(F-2k\alpha(-1+\beta)\theta(-1+\phi)^2+2\beta\theta(-1+\phi)^2\phi)}$ and $g^{\mathrm{nb}^*} = \frac{t^{\gamma}\times F}{M+t^{\gamma}(F-2k\alpha(-1+\beta)\theta(-1+\phi)^2+2\beta\theta(-1+\phi)^2\phi)}$ can be obtained by the first-order condition. Taking g^{nb^*} and δ^{nb^*} back to p and D, $p^{\mathrm{nb}^*} = -\frac{E}{M+t^{\gamma}(F-2k\alpha(-1+\beta)\theta(-1+\phi)^2+2\beta\theta(-1+\phi)^2\phi)}$, $D^{\mathrm{nb}^*} = \frac{\alpha\times C}{M+t^{\gamma}(F-2k\alpha(-1+\beta)\theta(-1+\phi)^2+2\beta\theta(-1+\phi)^2\phi)}$. The profit functions of the cloud manufacturing platform operator and the supplier are $\pi_F^{\mathrm{nb}^*} = -\frac{t^{\gamma}\epsilon^2\theta\times A^2+4k\alpha(-1+\phi)^2\times B\times C+2\alpha\phi\times E\times C+2t^{\gamma}\eta\times F^2}{2(M+t^{\gamma}(F-2k\alpha(-1+\beta)\theta(-1+\phi)^2+2\beta\theta(-1+\phi)^2\phi))^2}$, $\pi_R^{\mathrm{nb}^*} = -\frac{\alpha(-1+\phi)(-C)^2}{(M+t^{\gamma}(F-2k\alpha(-1+\beta)\theta(-1+\phi)^2+2\beta\theta(-1+\phi)^2\phi))^2}$, respectively.

$$
\begin{aligned}
A &= -4\eta(k\alpha-\phi)(-1+\phi)^2+k^2t^{\gamma}\alpha(1+\beta)(-1+\phi\varphi)^2\\
B &= kt^{\gamma}\alpha(1+\beta)\theta-4\alpha\eta\theta+t^{\gamma}(2\epsilon^2\eta+\beta(1+\beta)\theta)\phi\\
C &= -4\eta\theta(-1+\phi)^2-k^2t^{\gamma}\alpha(1+\beta)\theta(-1+\varphi)(-1+\phi\varphi)+k(-1+\phi)(-4\alpha\eta\theta(-1+\varphi)\\
&\quad +t^{\gamma}\left(2\epsilon^2\eta+\beta(1+\beta)\theta\right)(-1+\phi\varphi))\\
E &= 4\eta\theta(-1+\phi)^2+k(-1+\phi)\left(t^{\gamma}\left(2\epsilon^2\eta+\beta(1+\beta)\theta\right)(1+\phi(-2+\varphi))-4\alpha\eta\theta(-1+\varphi)\right)
\end{aligned}
$$

$$+ k^2 t^\gamma \alpha(1+\beta)\theta(-1+\varphi)(-3+\phi(2+\varphi))$$
$$F = 2k\alpha(-1+\beta)\theta(-1+\phi)^2 - 2\beta\theta(-1+\phi)^2\phi + k^2\alpha(t^\gamma\epsilon^2(-1+\phi\varphi)^2 - 2\alpha\theta(-1+\varphi)(-2+\phi+\phi\varphi))$$
$$M = 4kt^\gamma\alpha\beta\theta(-1+\phi)^2 + 2(-1+\phi)^2\left(-4\alpha\eta\theta + t^\gamma\left(2\epsilon^2\eta + \beta^2\theta\right)\phi\right).$$

Property 4.3. The influence of sensitivity coefficient of blockchain traceability technology and elasticity coefficient of cloud data security on supply chain decision and profit. (1) $\frac{\partial p^{\mathrm{nb}^*}}{\partial\beta} > 0$, $\frac{\partial \delta^{\mathrm{nb}^*}}{\partial\beta} > 0$, $\frac{\partial g^{\mathrm{nb}^*}}{\partial\beta} > 0$, $\frac{\partial \pi_F^{\mathrm{nb}^*}}{\partial\beta} > 0$, $\frac{\partial \pi_R^{\mathrm{nb}^*}}{\partial\beta} > 0$, $\frac{\partial D^{\mathrm{nb}^*}}{\partial\beta} > 0$; (2) $\frac{\partial p^{\mathrm{nb}^*}}{\partial\epsilon} > 0$, $\frac{\partial \delta^{\mathrm{nb}^*}}{\partial\epsilon} > 0$, $\frac{\partial g^{\mathrm{nb}^*}}{\partial\epsilon} > 0$, $\frac{\partial \pi_F^{\mathrm{nb}^*}}{\partial\epsilon} > 0$, $\frac{\partial \pi_R^{\mathrm{nb}^*}}{\partial\epsilon} > 0$, $\frac{\partial D^{\mathrm{nb}^*}}{\partial\epsilon} > 0$.

Property 4.3 shows that when the sensitivity coefficient of blockchain traceability technology and the elasticity coefficient of cloud data security increase, the security degree of cloud data, the level of blockchain traceability technology, the demand, the service price, and the profits of operators and suppliers will all increase. The increase of sensitivity coefficient of blockchain traceability technology means that the market attaches more importance to the application of technology, and operators will increase their investment in blockchain traceability technology, so as to improve the security and traceability of services. These technological improvements enhance the customer's trust in the product, and further increase the market demand. As the value of the service increases, the price of the service will reasonably rise, which in turn will drive the growth of the transaction volume, thus increasing the total revenue of the operator and the supplier. For example, the IBM Blockchain and Food Trust is a typical case, which uses blockchain traceability technology to improve the transparency and security of the food supply chain, making every step of the food circulation traceable, thereby enhancing consumers' trust in food safety [56]. This increase in transparency has attracted large retailers such as Walmart to join the platform, driving the application of blockchain traceability technology, enabling reasonable price increases for services, while also driving the growth of transaction volume, further increasing the revenue of operators and suppliers.

Property 4.4. The influence of cost coefficient of blockchain traceability technology and cost coefficient of cloud data security management on supply chain decision and profit. (1) $\frac{\partial p^{\mathrm{nb}^*}}{\partial\theta} < 0$, $\frac{\partial \delta^{\mathrm{nb}^*}}{\partial\theta} < 0$, $\frac{\partial g^{\mathrm{nb}^*}}{\partial\theta} < 0$, $\frac{\partial \pi_F^{\mathrm{nb}^*}}{\partial\theta} < 0$, $\frac{\partial \pi_R^{\mathrm{nb}^*}}{\partial\theta} < 0$, $\frac{\partial D^{\mathrm{nb}^*}}{\partial\theta} < 0$; (2) $\frac{\partial p^{\mathrm{nb}^*}}{\partial\eta} < 0$, $\frac{\partial \delta^{\mathrm{nb}^*}}{\partial\eta} < 0$, $\frac{\partial g^{\mathrm{nb}^*}}{\partial\eta} < 0$, $\frac{\partial \pi_F^{\mathrm{nb}^*}}{\partial\eta} < 0$, $\frac{\partial \pi_R^{\mathrm{nb}^*}}{\partial\eta} < 0$, $\frac{\partial D^{\mathrm{nb}^*}}{\partial\eta} < 0$.

Property 4.4 shows that when the cost factor of blockchain traceability technology and cloud data management increases, data security, blockchain traceability technology level, demand, service prices, and operator and supplier profits will decrease accordingly. An increase in the sensitivity coefficient of blockchain traceability technology usually means an increase in the cost required to maintain blockchain traceability technology, and operators may reduce their investment in data security in order to control expenditures, resulting in a decrease in the security of cloud data. As the level of blockchain traceability technology decreases, demanders' trust in services weakens, leading to a decrease in market demand. Due to the reduction in the value of the service, the price of the service tends to fall, which affects the profit of each transaction. Under the deduction model, although the percentage of the deduction that the operator collects from the supplier remains the same, the actual revenue of the operator will decrease due to the decline in the transaction volume and service price, further squeezing the profit margin of the operator and the supplier. Food delivery platform Uber Eats serves as a typical case exemplifying this scenario [57]. With the rising cost of blockchain traceability technology and data security management, these platforms have had to increase the percentage that merchants take. However, as merchants face higher costs, they often choose to reduce the quality of products and services, and even pass on some of the costs to consumers, leading to customer dissatisfaction, which in turn affects the decline in demand. At the same time, due to the increase in the cost of the platform, the profit margin is compressed, and the platform has to further adjust the price, which may have an adverse impact on the overall competitiveness of the market.

TABLE 3. Equilibrium outcomes under the revenue-sharing model in strong blockchain traceability technology level (Scenario B).

Equilibrium outcomes
$\delta^{\mathrm{nB}^*} = \frac{t^\gamma \epsilon \times G}{N + t^\gamma \left(L - 2k\alpha(-1+\beta-\epsilon)\theta(-1+\phi)^2 + 2\beta(1+\epsilon)\theta(-1+\phi)^2\phi\right)}$
$g^{\mathrm{nB}^*} = \frac{t^\gamma \times L}{N + t^\gamma \left(L - 2k\alpha(-1+\beta-\epsilon)\theta(-1+\phi)^2 + 2\beta(1+\epsilon)\theta(-1+\phi)^2\phi\right)}$
$p^{\mathrm{nB}^*} = -\frac{J}{N + t^\gamma \left(L - 2k\alpha(-1+\beta-\epsilon)\theta(-1+\phi)^2 + 2\beta(1+\epsilon)\theta(-1+\phi)^2\phi\right)}$
$D^{\mathrm{nB}^*} = \frac{\alpha \times K}{N + t^\gamma \left(L - 2k\alpha(-1+\beta-\epsilon)\theta(-1+\phi)^2 + 2\beta(1+\epsilon)\theta(-1+\phi)^2\phi\right)}$
$\pi_F^{\mathrm{nB}^*} = -\frac{t^\gamma \epsilon^2\theta(1-\phi) \times G^2 + 4k\alpha(-1+\phi)^3 \times O \times I - 2\alpha(-1+\phi)\phi \times J \times K + 2t^\gamma\eta(1-\phi) \times L^2}{2(1-\phi)\left(N + t^\gamma \left(L - 2k\alpha(-1+\beta-\epsilon)\theta(-1+\phi)^2 + 2\beta(1+\epsilon)\theta(-1+\phi)^2\phi\right)\right)^2}$
$\pi_R^{\mathrm{nB}^*} = -\frac{\alpha(-1+\phi)\left(-K\right)^2}{\left(N + t^\gamma \left(L - 2k\alpha(-1+\beta-\epsilon)\theta(-1+\phi)^2 + 2\beta(1+\epsilon)\theta(-1+\phi)^2\phi\right)\right)^2}$
$G = 4\eta(-1+\phi)^2(-k\alpha+\phi+\epsilon\phi) + k^2t^\gamma\alpha(1+\beta+\epsilon)(-1+\phi\varphi)^2$
$O = kt^\gamma\alpha(1+\beta+\epsilon)\theta - 4\alpha\eta\theta + t^\gamma\left(2\epsilon^2\eta + \beta(1+\beta+\epsilon)\theta\right)\phi$
$I = 4(1+\epsilon)\eta\theta(-1+\phi)^2 + k^2t^\gamma\alpha(1+\beta+\epsilon)\theta(-1+\varphi)(-1+\phi\varphi) + k(-1+\phi)\left(4\alpha\eta\theta(-1+\varphi) - t^\gamma\left(2\epsilon^2\eta + \beta(1+\beta+\epsilon)\theta\right)(-1+\phi\varphi)\right)$
$J = 4(1+\epsilon)\eta\theta(-1+\phi)^2 + k(-1+\phi)\left(t^\gamma\left(2\epsilon^2\eta + \beta(1+\beta+\epsilon)\theta\right)(1+\phi(-2+\varphi)) - 4\alpha\eta\theta(-1+\varphi)\right) + k^2t^\gamma\alpha(1+\beta+\epsilon)\theta(-1+\varphi)(-3+\phi(2+\varphi))$
$K = -4(1+\epsilon)\eta\theta(-1+\phi)^2 - k^2t^\gamma\alpha(1+\beta+\epsilon)\theta(-1+\varphi)(-1+\phi\varphi) + k(-1+\phi)\left(-4\alpha\eta\theta(-1+\varphi) + t^\gamma\left(2\epsilon^2\eta + \beta(1+\beta+\epsilon)\theta\right)(-1+\phi\varphi)\right)$
$L = 2k\alpha(-1+\beta-\epsilon)\theta(-1+\phi)^2 - 2\beta(1+\epsilon)\theta(-1+\phi)^2\phi + k^2\alpha\left(t^\gamma\epsilon^2(-1+\phi\varphi)^2 - 2\alpha\theta(-1+\varphi)(-2+\phi+\phi\varphi)\right)$
$N = 4kt^\gamma\alpha\beta\theta(-1+\phi)^2 + 2(-1+\phi)^2\left(-4\alpha\eta\theta + t^\gamma\left(2\epsilon^2\eta + \beta^2\theta\right)\phi\right)$

It can be seen that changes in the sensitivity coefficient of blockchain traceability technology and the elasticity coefficient of cloud data security have an important impact on market demand, price and corporate profits. In the face of technology investment and cost pressure, operators need to find the optimal balance between technology investment and cost control to ensure that technology application can promote profit growth, rather than weakening market competitiveness due to rising costs.

4.3.2. Strong blockchain traceability technology level (Scenario B)

The analytical procedure and resultant properties for this scenario align with those established in Section 4.3.1 hence, the detailed solution steps and property discussions are omitted for brevity. The corresponding equilibrium results are presented in Table 3.

TABLE 4. Equilibrium outcomes under the centralized decision-making scenario with strong blockchain traceability technology level (Scenario B).

Equilibrium outcomes
$\delta^{\mathrm{cB}^*} = \dfrac{2t^{\gamma}\epsilon\eta(1+\epsilon-k\alpha\varphi)}{-4\alpha\eta\theta+t^{\gamma}\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)}$
$g^{\mathrm{cB}^*} = \dfrac{t^{\gamma}\theta(1+\epsilon-k\alpha\varphi)(\beta+k\alpha\varphi)}{-4\alpha\eta\theta+t^{\gamma}\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)}$
$p^{\mathrm{cB}^*} = \dfrac{2kt^{\gamma}\epsilon^2\eta\varphi+kt^{\gamma}(1+\beta+\epsilon)\theta\varphi(\beta+k\alpha\varphi)-2\eta\theta(1+\epsilon+k\alpha\varphi)}{-4\alpha\eta\theta+t^{\gamma}\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)}$
$\pi_{\mathrm{T}}^{\mathrm{cB}^*} = \dfrac{\eta\theta\left(1+\epsilon-k\alpha\varphi\right)^2}{4\alpha\eta\theta-t^{\gamma}\left(2\epsilon^2\eta+\theta\left(\beta+k\alpha\varphi\right)^2\right)}$

5. Cost sharing – revenue sharing contract

5.1. Centralized decision-making model (Model c)

Under the centralized decision-making model, both decision-making parties are collectively rational, and both suppliers and operators are viewed as a whole, and both parties make decisions together with the goal of maximizing the profit of the cloud manufacturing supply chain as a whole. At this time, the decision-making variables of the system are also degraded from four to three, the level of cloud data security and blockchain traceability technology, the price of services and system profits as a benchmark for subsequent coordination and optimization, resulting in a decision-making model:

$$\pi_T^c = D\left(gp+(1-g)(p-\varphi k)\right)-\frac{1}{2}\theta t^{-\gamma}\delta^2-\eta t^{-\gamma}g^2. \tag{7}$$

5.1.1. Weak blockchain traceability technology level (Scenario b)

The third-order Hessian matrix $H^{\mathrm{cb}}=\begin{pmatrix}-2\alpha & \beta-k\alpha\varphi & \epsilon\\ \beta-k\alpha\varphi & -2t^{-\gamma}\eta+2k\beta\varphi & -k\epsilon\varphi\\ \epsilon & k\epsilon\varphi & -t^{-\gamma}\theta\end{pmatrix}$ of cloud manufacturing supply chain decisions with respect to p,g,δ has a determinant $\left|H^{\mathrm{cb}}\right|=t^{-2\gamma}(-4\alpha\eta\theta+t^{\gamma}\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right))<0$, with $4\alpha\eta t^{-\gamma}-\left(\beta+k\alpha\varphi\right)^2>0$ and $-2\alpha<0$. As a result, the Hessian matrix of the total profit π_T^c with respect to p,g,δ is strictly negative definite, and the total profit π_T^c with respect to p,g,δ is strictly differentiable concave function. Therefore, there exists a unique optimal service price, optimal cloud data security level, and optimal blockchain traceability technology. The optimal solutions p^*,g^*,δ^* are $p^{\mathrm{cb}^*}=\frac{-2\eta\theta(1+k\alpha\varphi)+kt\varphi(2\epsilon^2\eta+(1+\beta)\theta(\beta+k\alpha\varphi))}{-4\alpha\eta\theta+t^{\gamma}(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2)}$, $g^{\mathrm{cb}^*}=\frac{t^{\gamma}\theta(-1+k\alpha\varphi)(\beta+k\alpha\varphi)}{-4\alpha\eta\theta+t^{\gamma}(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2)}$, $\delta^{\mathrm{cb}^*}=\frac{2t^{\gamma}\varepsilon\eta(-1+k\alpha\varphi)}{-4\alpha\eta\theta+t^{\gamma}(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2)}$, respectively.

At this point, the optimal solutions are substituted into the total profit function, and the total profit of the cloud manufacturing supplier chain in the centralized game is $\pi_{\mathrm{T}}^{\mathrm{cb}^*}=\frac{n\theta(-1+k\alpha\varphi)^2}{4\alpha\eta\theta-t^{\gamma}(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2)}$.

5.1.2. Strong blockchain traceability technology level (Scenario B)

The computational approach for this scenario follows the same methodology as detailed in Section 5.1.1. Therefore, the specific solution procedure is omitted here. The resulting equilibrium outcomes are summarized in Table 4.

5.2. Cost-Sharing–Revenue-Sharing Contract under fixed service fee model (Model sc)

In the model, a combined cost-sharing and benefit-sharing contract $\{x, y, z, w\}$ is introduced to coordinate the supply chain. In this contract, the operator grants a lower service fee to the supplier w. The supplier bears z and y proportions of the operator's costs in improving the level of blockchain traceability technology and data security, respectively, and shares $1-x$ proportions of the revenues to the cloud manufacturing platform operator. The profit functions of both parties are:

$$\pi_F^{\mathrm{sc}} = D\left(gw + (1-g)(w-k)\right) - \frac{1}{2}(1-z)\theta t^{-\gamma}\delta^2 - (1-y)t^{-\gamma}\eta g^2 + (1-x)pD \tag{8}$$

$$\pi_R^{\mathrm{sc}} = D(g(xp-w) + (1-g)(xp-w+k-\varphi k)) - \frac{1}{2}z\theta t^{-\gamma}\delta^2 - y\eta t^{-\gamma}g^2. \tag{9}$$

5.2.1. Weak blockchain traceability technology level (Scenario b)

Proposition 5.1. *When* $w^{\mathrm{scb}^*} = \frac{k(1-\varphi+x\varphi)\left(2t^\gamma\epsilon^2\eta+t^\gamma\beta\theta+t^\gamma\beta^2\theta-4\alpha\eta\theta+kt^\gamma\alpha\theta\varphi+kt^\gamma\alpha\beta\theta\varphi\right)}{2t^\gamma\epsilon^2\eta+t^\gamma\beta^2\theta-4\alpha\eta\theta+2kt^\gamma\alpha\beta\theta\varphi+k^2t^\gamma\alpha^2\theta\varphi^2}$, $z^{\mathrm{scb}^*} = \frac{x}{1+x}$, $y^{\mathrm{scb}^*} = \frac{x}{1+x}$, $x_1 \le x \le x_2$ *are satisfied, a combined cost-sharing and benefit-sharing contract enables supply chain coordination. Where:* $x_1 = \frac{(-4\alpha\eta\theta+Q)\left(\left(48\alpha^2\eta^2\theta^2-12\alpha\eta\theta Q+Q^2\right)+\sqrt{(6400\alpha^4\eta^4\theta^4-2176\alpha^3\eta^3\theta^3Q+304\alpha^2\eta^2\theta^2Q^2-24\alpha\eta\theta Q^3+Q^4)}\right)}{8\alpha\eta\theta(-8\alpha\eta\theta+Q)^2}$, $x_2 = \frac{16\alpha^2\eta^2\theta^2-8\alpha\eta\theta\times Q+Q^2-\sqrt{64\alpha^2\eta^2\theta^2(-8\alpha\eta\theta+Q)(-4\alpha\eta\theta+Q)+(-4\alpha\eta\theta+Q)^4}}{(8\alpha\eta\theta(-8\alpha\eta\theta+Q))}$, $Q = t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)$.

Proof. By backward induction, we can find that $p^{\mathrm{scb}^*} = \frac{x(1+g\beta+\delta\epsilon)+\alpha(w+k(-1+g+\varphi-g\varphi))}{2x\alpha}$, $w^{\mathrm{scb}^*} = \frac{4x^2P+4kP\alpha(1+x-\varphi)+kt^\gamma\left(2(-1+y)\epsilon^2\eta+(-1+z)\beta(1+\beta)\theta\right)(1+(-1+x)\varphi)+k^2t^\gamma(-1+z)\alpha(1+\beta)\theta\varphi(1+(-1+x)\varphi)}{4(1+x)\alpha P+t^\gamma(2(-1+y)\epsilon^2\eta+(-1+z)\theta(\beta+k\alpha\varphi)^2)}$, $P = (-1+y)(-1+z)\eta\theta$, $\delta^{\mathrm{scb}^*} = \frac{2t^\gamma(-1+y)\epsilon\eta(-1+k\alpha\varphi)}{4(1+x)(-1+y)(-1+z)\alpha\eta\theta+t^\gamma(2(-1+y)\epsilon^2\eta+(-1+z)\theta(\beta+k\alpha\eta)^2)}$, and $g^{\mathrm{scb}^*} = \frac{t^\gamma(-1+z)\theta(-1+k\alpha\varphi)(\beta+k\alpha\varphi)}{4(1+x)(-1+y)(-1+z)\alpha\eta\theta+t^\gamma(2(-1+y)\epsilon^2\eta+(-1+z)\theta(\beta+k\alpha\varphi)^2)}$.

When $w^{\mathrm{scb}^*} = \frac{k(1-\varphi+x\varphi)\left(2t^\gamma\epsilon^2\eta+t^\gamma\beta\theta+t^\gamma\beta^2\theta-4\alpha\eta\theta+kt^\gamma\alpha\theta\varphi+kt^\gamma\alpha\beta\theta\varphi\right)}{2t^\gamma\epsilon^2\eta+t^\gamma\beta^2\theta-4\alpha\eta\theta+2kt^\gamma\alpha\beta\theta\varphi+k^2t^\gamma\alpha^2\theta\varphi^2}$, $z^{\mathrm{scb}^*} = \frac{x}{1+x}$, $y^{\mathrm{scb}^*} = \frac{x}{1+x}$, satisfy $p^{\mathrm{scb}^*} = p^{\mathrm{cb}^*}$, $\delta^{\mathrm{scb}^*} = \delta^{\mathrm{cb}^*}$ and $g^{\mathrm{scb}^*} = g^{\mathrm{cb}^*}$. At this time, the profit functions of cloud members are respectively: $\pi_F^{\mathrm{scb}^*} = -\frac{\eta\theta(-1+k\alpha\varphi)^2\left(4\left(-1+x^2\right)\alpha\eta\theta+t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)\right)}{(1+x)\left(-4\alpha\eta\theta+t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)\right)^2}$, $\pi_R^{\mathrm{scb}^*} = \frac{x\eta\theta(-1+k\alpha\varphi)^2\left(4(1+x)\alpha\eta\theta-t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)\right)}{(1+x)\left(-4\alpha\eta\theta+t^\gamma\left(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2\right)\right)^2}$. □

It can be verified that, $\pi_F^{\mathrm{scb}^*} + \pi_R^{\mathrm{scb}^*} = \pi_T^{\mathrm{cb}^*}$, *i.e.*, the cloud manufacturing supply chain can realize the effect of centralized decision making under the combined contract of cost sharing and benefit sharing. In addition, the contract needs to realize the Pareto improvement of the cloud members, when $\boldsymbol{x}$ the following relation is satisfied: $x_1 \le x \le x_2$, with $\pi_F^{\mathrm{scb}} \ge \pi_F^{\mathrm{sb}}$, $\pi_R^{\mathrm{scb}} \ge \pi_R^{\mathrm{sb}}$, which satisfies the individual rationality principle of the coordination contract.

5.2.2. Strong blockchain traceability technology level (Scenario B)

Proposition 5.2. *When* $z^{\mathrm{scB}^*} = \frac{x}{1+x}$, $y^{\mathrm{scB}^*} = \frac{x}{1+x}$, $w^{\mathrm{scB}^*} = \frac{4x^2(1+\epsilon)P+4k\alpha P(1+x-\varphi)+kt^\gamma\left(2(-1+y)\epsilon^2\eta+(-1+z)\beta(1+\beta+\varepsilon)\theta\right)(1+(-1+x)\varphi)+k^2t^\gamma(-1+z)\alpha(1+\beta+\varepsilon)\theta\varphi(1+(-1+x)\varphi)}{4(1+x)\alpha P+t^\gamma(2(-1+y)\epsilon^2\eta+(-1+z)\theta(\beta+k\alpha\varphi)^2)}$, $x_1 \le x \le x_2$ *are satisfied, a combined cost-sharing and benefit-sharing contract enables supply chain coordination. Where:* $x_1 = \frac{(-4\alpha\eta\theta+Q)\left(\left(48\alpha^2\eta^2\theta^2-12\alpha\eta\theta Q+Q^2\right)+\sqrt{(6400\alpha^4\eta^4\theta^4-2176\alpha^3\eta^3\theta^3Q+304\alpha^2\eta^2\theta^2Q^2-24\alpha\eta\theta Q^3+Q^4)}\right)}{8\alpha\eta\theta(-8\alpha\eta\theta+Q)^2}$, $x_2 = \frac{16\alpha^2\eta^2\theta^2-8\alpha\eta\theta\times Q+Q^2-\sqrt{64\alpha^2\eta^2\theta^2(-8\alpha\eta\theta+Q)(-4\alpha\eta\theta+Q)+(-4\alpha\eta\theta+Q)^4}}{(8\alpha\eta\theta(-8\alpha\eta\theta+Q))}$, $Q = t^\gamma(2\epsilon^2\eta+\theta(\beta+k\alpha\varphi)^2)$. *The proof follows the same procedure as established in Section 5.2.1.*

A further comparative analysis of Propositions 5.1 and 5.2 reveals that under both strong and weak blockchain traceability technology scenarios, the cost-sharing and revenue-sharing combined contract $\{x, y, z, w\}$ maintains identical parameters with the notable exception of the service fee w. This indicates that the core mechanism of the contract, specifically the cost-sharing and revenue-sharing ratio $\{x, y, z\}$, exhibits strong robustness across varying levels of blockchain traceability technology.

6. Numerical analysis and discussion

In order to further study the optimal decision results in the above different situations, this part uses Mathematica software to carry out numerical analysis and discussion on the influence of relevant parameters on the preference of the cloud members' charging mode. Without loss of generality under the condition of satisfying the model assumptions, the parameters are selected according to the limited conditions.

6.1. Influence of relevant parameters on decision variables and profits

With the rapid development of cloud computing and blockchain traceability technology, more and more businesses have come to rely on these technologies to enhance their operational efficiency and data security. In practical applications, the charging strategy between cloud service operators and suppliers and the economic principles behind it directly affect the market demand for services, the profit distribution of enterprises and the rate of return on technical input. This study analyzes the market demand of different charging models and blockchain traceability technology levels, and explores the optimal decision and profit distribution scheme of all parties. In this analysis, we further explore the impact of different charging models and blockchain traceability technology levels on market demand by building a mathematical model and making assumptions about several key parameters (such as cloud data security management costs, blockchain traceability technology investment costs, etc.), especially in terms of changes in data security commitments and penalties for service failures. In order to better understand the practical application of these theories, we combined multiple real cases and industry reports to provide a detailed explanation of the parameter settings [44, 58–66]. The following table summarizes the main parameters used in our analysis, the background reasons for their setting and the relevant practical cases, so as to better understand the relationship between market demand, optimal decision making and the profits of all parties. As shown in the Table 5 below.

As shown in Figures 3 and 4, across different charging models and blockchain traceability technology scenarios, an increase in the sensitivity coefficient of blockchain traceability technology and the elasticity coefficient of cloud data security leads to a corresponding rise in demand, service price, operator profit, and supplier profit, which validates Properties 4.1 and 4.3. The underlying logic is that enhanced consumer trust gradually stimulates latent demand, while users become willing to pay a premium for higher credibility and security assurance. Conversely, when the cost coefficients of blockchain traceability technology and cloud data security increase, demand, service price, operator profit, and supplier profit all exhibit a declining trend, confirming Properties 4.2 and 4.4. This occurs because rising costs drive operators to reduce investments in data security and blockchain traceability, resulting in degraded service or product security, diminished trust, lower demand, and suppliers being forced to cut prices to maintain market competitiveness – ultimately compressing overall profitability.

Under the strong blockchain traceability technology scenario, the levels of demand, service price, operator profit, and supplier profit consistently exceed those observed under the weak technology scenario. This clearly demonstrates that advanced blockchain traceability technology, leveraging its immutability and traceability features, significantly enhances transparency across the cloud manufacturing supply chain and elevates the perceived credibility of services. These improvements substantially strengthen consumer confidence in product authenticity and data security, thereby directly stimulating market demand. Furthermore, the expansion of market demand provides suppliers with greater pricing flexibility, which, through coordinated optimization within the cloud manufacturing supply chain, subsequently drives synchronized profit growth for operators. In contrast, weak blockchain traceability technology is less effective in establishing trust, generating demand, and supporting price premiums, resulting in its overall inferior performance.

Further analysis conducted at a sensitivity level of $\phi = 0.3$ reveals distinct impacts of the charging model on system outcomes. Under the fixed service fee model, both the service price and the operator's profit consistently exceed those in the revenue-sharing model. In contrast, the revenue-sharing model leads to higher demand and greater profit for the supplier compared to the fixed-fee approach. The fixed service fee model provides the operator with a stable and predictable revenue stream, which reduces income volatility and helps safeguard profit levels. However, suppliers may perceive the fixed cost as a rigid financial burden, which could dampen

TABLE 5. Analysis of parameter settings.

Elements of analysis	Parameter value	Background and reasons	Reference source
Operator penalty factor in case of service failure k	0.1	Cloud service providers promise in the SLA to offer data security guarantees. If the service fails or data leakage occurs, the operator must compensate the customer.	[58]
Service price sensitivity coefficient α	0.8	The Gartner Cloud Services Market Report and the China Academy of Information and Communications Technology's Cloud Computing Industry White Paper show that the sensitivity of enterprise customers to the price of cloud services is generally 0.7–0.9.	[59]
Pro rata factor of revenue sharing ϕ	0.3	AWS has a 70 per cent (AWS) to 30 per cent (vendor) split with independent software providers.	[60]
Percentage of cloud data security commitment Reimbursements received by demanders φ	0.5	The SLAs (Service Level Agreements) of major cloud providers such as AWS and Aliyun stipulate that the percentage of compensation in the event of a service failure is usually 5–10 per cent of the cost of the service.	[61]
Sensitivity coefficient of blockchain traceability technology ϵ	0.8	Examining IBM Food Trust and similar blockchain initiatives clearly shows how blockchain traceability technologies significantly enhance supply chain transparency, thus driving up demand within supply chain markets.	[62, 63]
Cloud data security elasticity Coefficient β	0.8	AWS and Azure ensure high availability through strategies such as redundant backup and encryption, and this coefficient reflects their recovery capabilities.	[59]
Blockchain traceability technology Investment Cost Factor θ	1	IBM's blockchain platform with Walmart involved a high initial investment, including R&D and global data centre build-outs. Microsoft Azure had a similar investment.	[64]
Cloud data security management cost factor η	1	Cloud service providers must heavily invest in data center security management, especially in global compliance and security measures.	[65]
Times t	1	Standardize the time scale and establish a cycle that carries clear legal and commercial implications.	[44]
Technical Progress Factor γ	0.4	Cloud computing platforms (*e.g.*, AWS, Azure) typically reduce operating costs as technology advances, such as with more efficient hardware and automation.	[66]

their incentive to adopt cloud services and ultimately restrain overall demand expansion. On the other hand, the revenue-sharing model lowers the initial entry barrier for suppliers and aligns the operator's earnings directly with the supplier's sales performance. This alignment helps broaden the market demand base and allows the supplier to maximize total revenue and profit. Nevertheless, in this model, the operator often must relinquish a portion of potential earnings to foster market development.

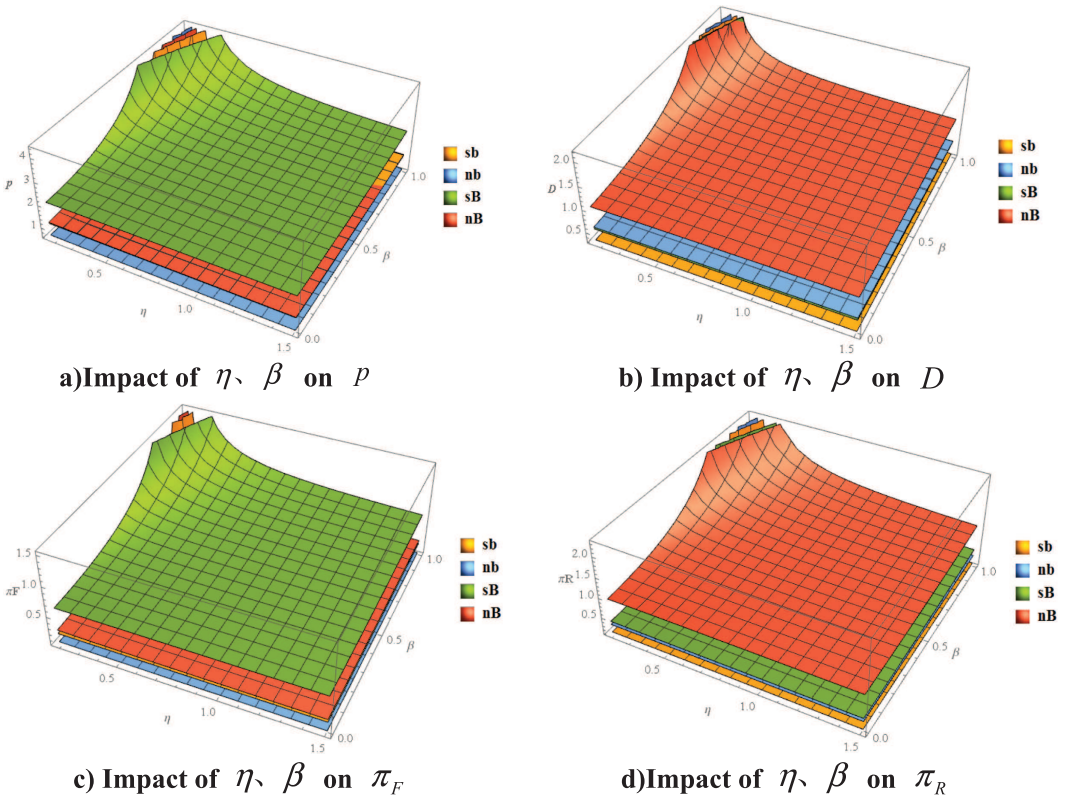

FIGURE 3. The impact of decision variables on η, g.

6.2. The impact of revenue sharing ratio pairs p D π_F π_R

This section focuses on analyzing how revenue sharing ratios affect demand, service price, operator profit, and supplier profit under different blockchain traceability technology levels and charging models, with the aim of examining how cloud members can select the most suitable charging model based on revenue distribution mechanisms.

As observed in Figures 5–8, under the same revenue sharing ratio, the strong blockchain traceability technology scenario consistently yields higher service prices, demand levels, operator profits, and supplier profits compared to the weak technology scenario. The transition from weak to strong blockchain traceability technology leads to a particularly pronounced increase in profits for both operators and suppliers.

Under the revenue-sharing model, an increase in the revenue sharing ratio raises the operator's earnings per transaction. This heightened income incentivizes the operator to invest more in blockchain traceability technology and data security enhancements. These improvements boost consumer trust and market attractiveness, thereby expanding market demand (Fig. 6). As demand grows, the perceived value of the product or service increases, leading to a corresponding rise in service price (Fig. 5). Consequently, the operator experiences significant profit growth (Fig. 7). For the supplier, however, the profit reduction resulting from the higher sharing ratio outweighs the profit gain from demand expansion, ultimately leading to a decline in their overall profit (Fig. 8). To sum up, under the revenue-sharing model, the increase of revenue sharing ratio is a positive signal for operators, which can promote their profit growth and technological progress. However, for suppliers, the profit pressure and market competition may lead them to choose the fixed-fee model to stabilize their revenue and ensure predictability. For instance, in ride-hailing platforms operating in the Helsinki region of Finland, an

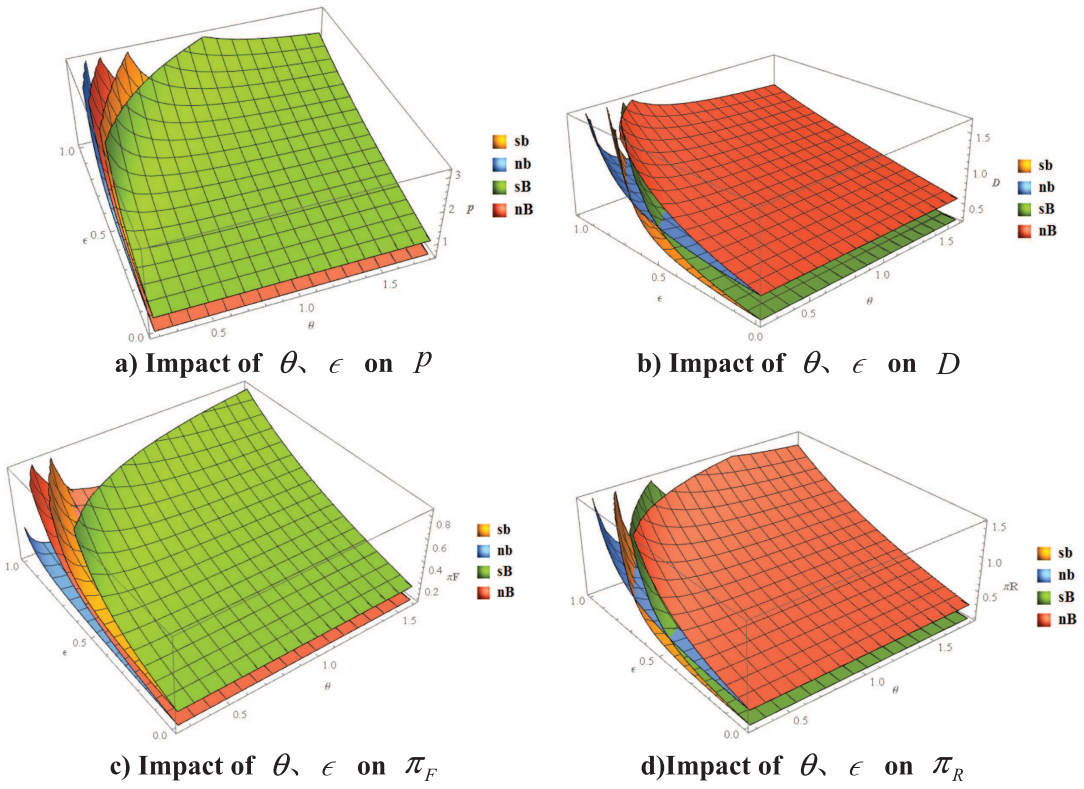

FIGURE 4. The impact of decision variables on θ, ϵ.

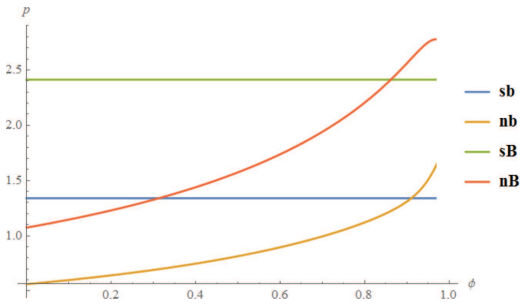

FIGURE 5. Impact of ϕ on P.

increase in the platform's commission rate raises the platform's revenue but simultaneously compresses drivers' income, which may eventually lead to driver attrition. In order to compensate for these losses, drivers may increase their income by increasing their service fees or increasing their working hours. However, the platform increases its investment in technological innovation through these revenues, improving the stability and safety of the platform, thus attracting more passengers and promoting the growth of market demand.

Further analysis of Figures 7 and 8 reveals cloud members' preferences regarding the charging models. At lower revenue sharing ratios, the operator receives only a small portion of the total revenue, while the supplier retains a larger share. As a result, suppliers exhibit a preference for the revenue-sharing model, whereas operators tend

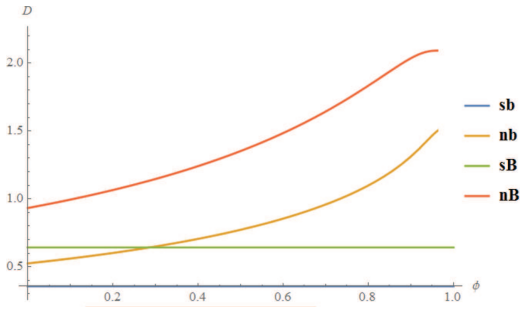

FIGURE 6. Impact of ϕ on D.

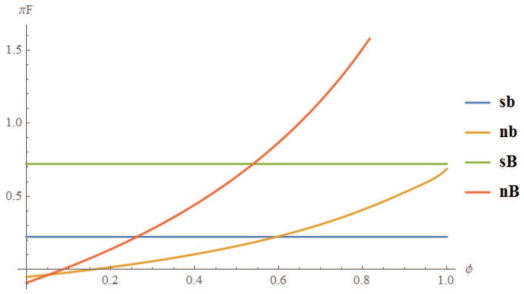

FIGURE 7. Impact of ϕ on π_F.

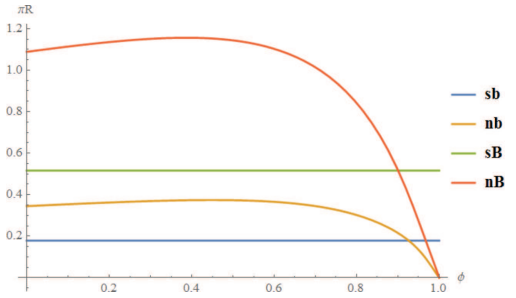

FIGURE 8. Impact of ϕ on π_R.

to favor the fixed service fee model. When the revenue sharing ratio reaches a moderate level, both operators and suppliers show a preference for the revenue-sharing model. This shift occurs because, under this model, the operator obtains a relatively higher share of revenue, which motivates increased investment in blockchain traceability technology and cloud data security. These enhancements attract more demand and expand market size. The resulting demand growth generates a sufficiently positive impact on the operator's net revenue to outweigh the associated investment costs, thereby yielding higher profits than those achievable under the fixed service fee model. Simultaneously, suppliers also prefer the revenue-sharing model at this stage. Although the operator claims a larger portion of revenue, the overall supply chain revenue increases substantially due to market expansion. Consequently, the supplier's profit under the revenue-sharing model remains higher than that under the fixed service fee model. For example, in the case of AWS, an increase in the platform's revenue sharing ratio may compress profits for some suppliers. However, the platform's subsequent investments in data security and

TABLE 6. Charging model selection.

	I ($\phi < \phi_1$)	II ($\phi_1 < \phi < \phi_2$)	III ($\phi > \phi_2$)
Cloud manufacturing platform operator	Fixed service fee model	Revenue-sharing model	Revenue-sharing model
Cloud manufacturing supplier	Revenue-sharing model	Revenue-sharing model	Fixed service fee model

processing capabilities enhance service quality, attract more customers, and stimulate overall demand growth – benefiting the ecosystem as a whole.

At high revenue sharing ratios, operators generally prefer the revenue-sharing model, as it allows them to capture a larger portion of the total revenue. For suppliers, however, the high sharing rate significantly reduces their own revenue share, even if the overall supply chain revenue experiences some growth. Consequently, suppliers tend to favor the fixed service fee model under such conditions, as it provides greater income stability and predictability. A representative example can be observed on content platforms such as YouTube. When the platform increases its revenue sharing ratio, creator earnings may see a nominal rise, but they often face mounting pressure to produce more content to maintain their income levels. This dynamic reflects the delicate balance that platforms and creators must strike to sustain long-term collaboration and common development.

Appropriate adjustment of the revenue sharing ratio plays a critical role in aligning the charging model preferences and coordinated decision-making between the operator and the supplier. Therefore, when determining the revenue sharing ratio in a cloud manufacturing supply chain, it is essential to dynamically adapt the ratio in response to changes in the market environment and technological capabilities. Such flexibility not only contributes to improved service quality and enhanced customer trust, but also helps balance the interests of all parties, thereby promoting long-term stability and sustainable development of the partnership.

6.3. Implications for the choice of fee model

Table 6 illustrates how cloud members select the most suitable charging model based on the revenue sharing ratio. When $\phi < \phi_1$ (*i.e.*, within region I), the operator prefers the fixed service fee model, while the provider prefers the pumping model when $\phi > \phi_2$ (*i.e.*, within region III), the operator prefers the pumping model, while the provider prefers the fixed service model and when $\phi_1 < \phi < \phi_2$ (within region II), both parties will prefer the pumping model.

Figures 9–12 illustrate the impact of key parameters on cloud members' preferences for charging models under different blockchain traceability technology levels. Notably, a strong technology level more significantly weakens the revenue-sharing ratio threshold (ϕ_1) at which the operator prefers the fixed service fee model (*i.e.*, the area of Region I under the strong technology scenario is larger than that under the weak technology scenario). Simultaneously, a strong technology level increases the likelihood that both cloud members jointly prefer the revenue-sharing model ($[\phi_1, \phi_2]$) (*i.e.*, the area of Region II under the strong technology scenario is larger than that under the weak technology scenario). This occurs because the strong blockchain traceability technology effectively ensures transparency and data credibility across the cloud manufacturing supply chain. This assurance substantially reduces the operator's need to rely on the fixed service fee model for revenue stability, making them more inclined to adopt the revenue-sharing model, which better incentivizes ecosystem growth. For suppliers, operating in a credible environment reinforced by strong blockchain traceability technology provides stronger guarantees for data security and transaction fairness. This mitigates their concerns over "rigid costs", making them more willing to adopt the revenue-sharing model, which can maximize both market demand and their own profits. A practical example can be found in the "Three-Body Five-Trust" computing power operation system of Whale Cloud Technology. Here, blockchain traceability technology ensures end-to-end credibility throughout

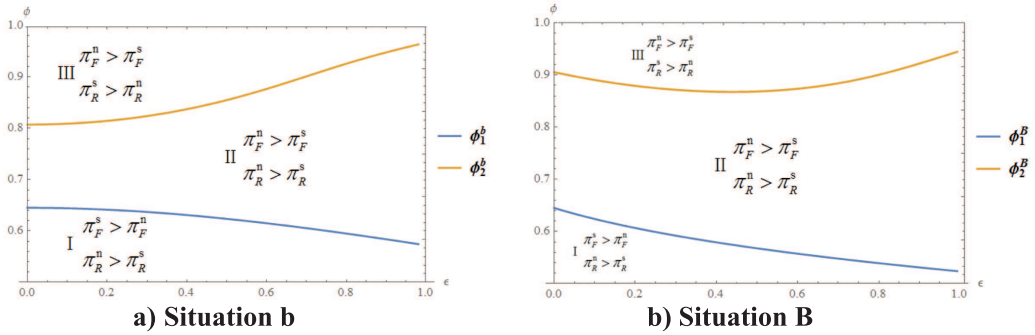

FIGURE 9. The Influence of ϵ on Strategy Selection.

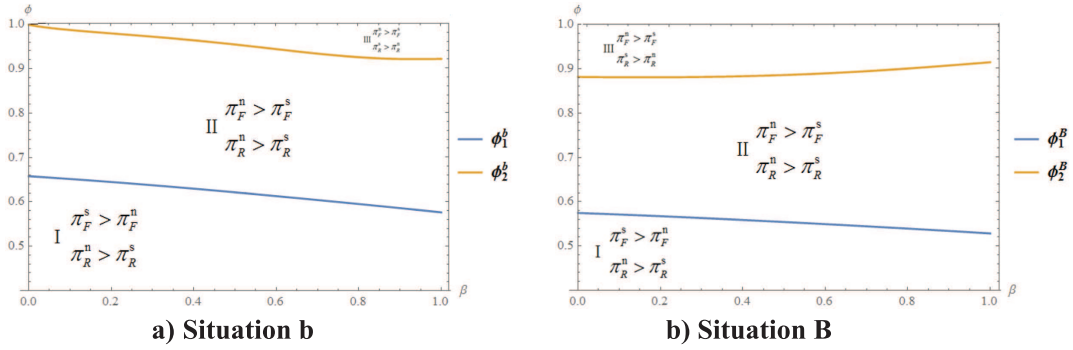

FIGURE 10. The Influence of β on Strategy Selection.

the transaction process, effectively fostering willingness among both supply and demand sides of computing power to collaborate under a revenue-sharing model.

An increase in ϵ and β (Figs. 9 and 10) weakens the revenue sharing ratio threshold at which the operator prefers the fixed service fee model (ϕ_1) (*i.e.*, Region I shrinks) and strengthens the corresponding threshold for the supplier's preference toward the fixed model (ϕ_2) (*i.e.*, Region III gradually shrinks). Consequently, the likelihood that both cloud members jointly prefer the revenue-sharing model increases (*i.e.*, Region II gradually expands). This dynamic arises because, although rising sensitivity to blockchain traceability technology and elasticity of cloud data security improve technology levels, security, demand, and profits under both models, the revenue-sharing model yields more pronounced profit gains for cloud members (*i.e.*, $\frac{\pi_R^{n^*}}{\partial\epsilon} > \frac{\pi_R^{s^*}}{\partial\epsilon}$, $\frac{\pi_F^{n^*}}{\partial\epsilon} > \frac{\pi_F^{s^*}}{\partial\epsilon}$, $\frac{\pi_R^{n^*}}{\partial\beta} > \frac{\pi_R^{s^*}}{\partial\beta}$, $\frac{\pi_F^{n^*}}{\partial\beta} > \frac{\pi_F^{s^*}}{\partial\beta}$). As a result, the range of conditions under which both parties prefer the revenue-sharing model widens. For example, in the fintech sector, as sensitivity to blockchain traceability and cloud data security increases, many financial service platforms (such as PayPal and Square) tend to adopt revenue-sharing models over fixed-fee structures. Growing user demand and heightened data security requirements drive these platforms to enhance transaction security and transparency through blockchain traceability. This, in turn, improves service scalability and stability, incentivizing platforms to invest more in blockchain traceability technology and adopt revenue-sharing arrangements – ultimately strengthening market demand and boosting profitability.

θ increases (Fig. 11), the revenue share ratio thresholds for the operator preference for the fixed service fee model become stronger and the revenue share ratio thresholds for the suppliers preference for the fixed service fee model become weaker (*i.e.*, Regions I and III become progressively larger), and the range of intervals in which both cloud members have the same preference for the revenue-sharing model decreases (Region II becomes

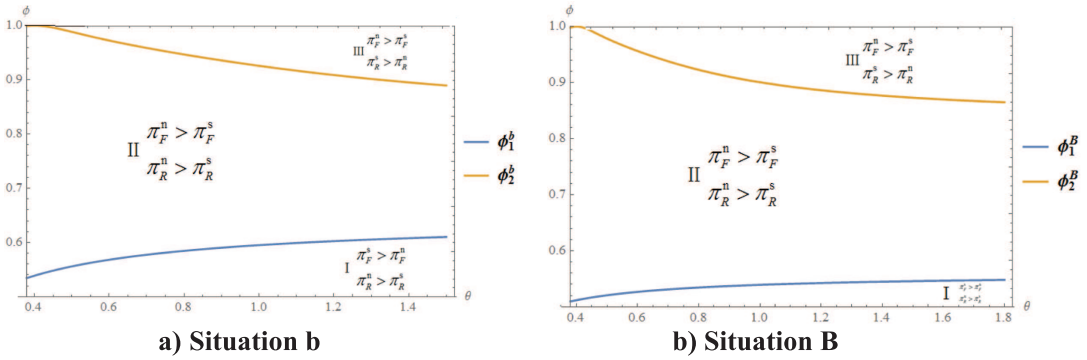

FIGURE 11. The influence of θ on strategy selection.

progressively smaller). This is due to the fact that as the cost factor of blockchain traceability technology increases, the level of blockchain traceability technology and the level of cloud data security decrease in both models, but the demand and profit of the cloud members also decrease. However, the decrease in technology level, demand and profit is more significant under the revenue-sharing model ($\frac{\pi_R^{n*}}{\partial\theta} < \frac{\pi_R^{s*}}{\partial\theta}$, $\frac{\pi_F^{n*}}{\partial\theta} < \frac{\pi_F^{s*}}{\partial\theta}$). For example, e-commerce platforms (such as Amazon and Alibaba) use blockchain traceability technology for supply chain management, but as the cost of the technology increases, the platforms face a declining return on investment in blockchain traceability technology. At this point, platforms may prefer a fixed fee model to maintain a return on technology investment with stable revenues. Suppliers, on the other hand, may also opt for a fixed-fee model to ensure their own revenue stability in the face of rising technology costs, as the decline in profits under the revenue-sharing model is even greater.

The increase of η (Fig. 12) increases the revenue share ratio threshold of the operator's preference for the fixed service fee model (*i.e.*, area I becomes larger) and the revenue share ratio threshold of the supplier's preference for the revenue-sharing model (area III becomes progressively smaller), but decreases the possibility of both parties jointly preferring the revenue-sharing model (area II becomes progressively smaller). This is due to the fact $\left|\frac{\pi_R^{n*}}{\partial\eta} - \frac{\pi_R^{s*}}{\partial\eta}\right| - \left|\frac{\pi_F^{n*}}{\partial\eta} - \frac{\pi_F^{s*}}{\partial\eta}\right| < 0$ that ϕ_1 becomes larger than ϕ_2 becomes smaller, so the range of intervals in which both cloud members prefer the preferred revenue-sharing model increases. For example, SaaS platforms (*e.g.*, Salesforce) face increased operational costs while improving cloud data security management. The platforms may increase their fixed fees to cover the additional security costs, which may lead operators to prefer the fixed fee model. However, some cloud storage providers (*e.g.*, Dropbox or Google Drive) may prefer to continue with a pump-price model despite the rising cost of managing data security, as they need to remain competitive and attract more user demand. As the cost of managing data security increases, the revenue model will continue to adjust based on the cost of sharing profits between platforms and providers, despite increased market demand.

7. CONCLUSIONS

Against the backdrop of intertwined blockchain traceability technology development and data security risks, this study constructs a cloud manufacturing supply chain model comprising an operator and a supplier, with a focus on cloud data security and blockchain traceability. The model analyzes the decisions and coordination between the operator and the supplier under different charging models and varying levels of blockchain traceability technology, and further explores the selection strategy of charging models for cloud manufacturing supply chain members. The research reveals the following key findings. (1) The level of blockchain traceability technology significantly influences the cloud manufacturing supply chain. Under the strong blockchain trace-

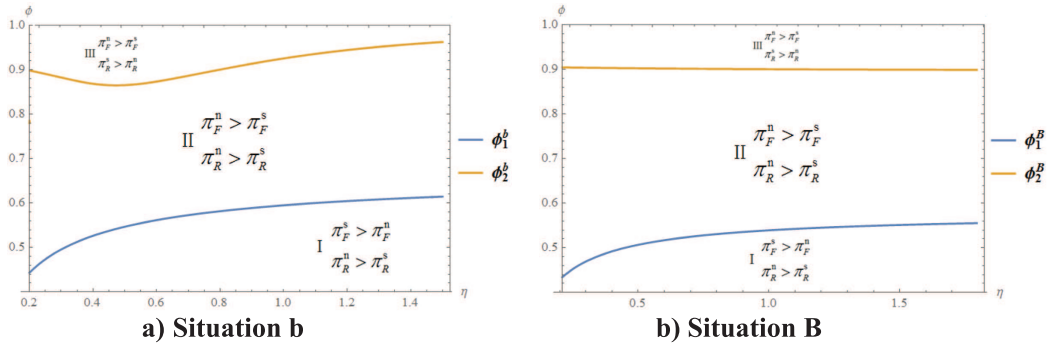

FIGURE 12. The influence of η on strategy selection.

ability technology scenario, the service price, demand, and profits are substantially higher than those under a weak technology scenario. (2) The cloud data security level, blockchain traceability technology level, service price, demand, and profits all increase with higher sensitivity to blockchain traceability technology and greater elasticity of cloud data security. Conversely, an increase in the cost coefficients of blockchain traceability technology and cloud data security management leads to a decline in these decision variables. (3) Under the fixed service fee model, a cost-sharing and revenue-sharing contract can achieve Pareto-optimal profit distribution among cloud manufacturing supply chain members under certain conditions. The core terms of this contract remain unaffected by the strength of blockchain traceability technology, demonstrating strong stability. (4) The selection of charging models by cloud manufacturing supply chain members is jointly influenced by the revenue sharing ratio, sensitivity to blockchain traceability, elasticity of cloud data security, cost coefficient of blockchain traceability technology, and cost coefficient of cloud data security management. At low revenue sharing ratios, the operator prefers the fixed service fee model, while the supplier favors the revenue-sharing model. An increase in the cost coefficients of blockchain traceability technology and cloud data security management strengthens the operator's preference for the fixed model. At high revenue sharing ratios, the operator tends to choose the revenue-sharing model, whereas the supplier leans toward the fixed service fee model. An increase in the cost coefficient of blockchain traceability technology reinforces the supplier's preference for the fixed model, while an increase in the cloud data security management cost coefficient weakens it. At moderate revenue sharing ratios, both parties show a stronger inclination toward the revenue-sharing model. Increases in the sensitivity to blockchain traceability technology and the elasticity of cloud data security further strengthen this shared preference.

Based on the above findings, the following managerial implications are derived. In the operation of a cloud manufacturing supply chain, cloud members should leverage their inherent advantages in data security and blockchain traceability by actively enhancing their technological capabilities and transitioning toward a strong blockchain traceability technology regime as early as possible. Concurrently, close monitoring of shifts in consumer concern for data security and preference for blockchain traceability is essential. Strategies should be adjusted flexibly to adapt to dynamic market demands, thereby delivering greater economic returns to cloud members. Operators should avoid indiscriminately increasing investments in blockchain traceability technology and cloud data security management solely to strengthen technological capability and ensure security. Instead, they must identify an appropriate balance between the two to maximize return on investment and prevent resource waste from overinvestment. Suppliers can appropriately share part of the expenditure on blockchain traceability technology and cloud data security management to promote the sustainable development of the cloud manufacturing supply chain. Furthermore, when selecting a charging model, the revenue-sharing ratio must be carefully considered to prevent instability in cooperation arising from inequitable profit distribution. This study provides a theoretical foundation for selecting charging models and making coordination decisions

in cloud manufacturing supply chains that incorporate data security and blockchain traceability technology. However, certain limitations remain. Future research could further explore cooperation and competition among multiple operators and suppliers within cloud manufacturing supply chains, as well as coordination decision-making in the presence of multiple and heterogeneous preferences.

Funding

This work is supported by the National Social Science Foundation of China (No. 23BGL077) the Key R&D Program (Soft Science Project) of Shandong Province, China (No. 2025RZA0202) the National Natural Science Foundation of China (No. 72474060) and the Humanities and Social Science Fund of Ministry of Education of China (No. 22YJC630133).

Data availability statement

The research data associated with this article are included in the article.

References

[1] B. Hu and L.L. Wang, Enterprise organizational structure change under the environment of Internet of Things. *Manage. World* **36** (2019) 202–210+232+211.

[2] J.X. Nan, L. Zhang, M.J. Zhang and D.F. Li, Two-type game model of multi-person cooperation and technological innovation decision in cloud service supply chain. *Syst. Eng. Theory Pract.* **41** (2021) 1771–1783.

[3] S. Liu, W.Z. Han, Z. Zhang and F.T.S. Chan, An analysis of performance, pricing, and coordination in a supply chain with cloud services: the impact of data security. *Comput. Ind. Eng.* **192** (2024) 110237.

[4] G.P. Jin, Improve the resilience and security level of industrial chain and supply chain. *Econ. Dail. News.* (2020).

[5] Z. Tan, S.P. Parambath, C. Anagnostopoulos, J. Singer and A.K. Marnerides, Advanced persistent threats based on supply chain vulnerabilities: challenges, solutions, and future directions. *IEEE Int. Things J.* **12** (2025) 6371–6395.

[6] J. Yu, X. Cui and C. Zhou, Blockchain adoption and consumer privacy concerns in a platform supply chain with manufacturer competition. *RAIRO-Oper. Res.* **59** (2025) 1935–1958.

[7] Z. Li, X. Liang, Q. Wen and E.A. Wan, The analysis of financial network transaction risk control based on blockchain and edge computing technology. *IEEE Trans. Eng. Manag.* **71** (2024) 5669–5690.

[8] Z. Qu, M. Dawande and G. Janakiraman, Technical noteCloud cost optimization: model, bounds, and asymptotics. *Oper. Res.* **72** (2024) 132150.

[9] Ofcom, Cloud services market study final report. *Ofcom Report* (2023) 1–246.

[10] X. Cao, H. Bo and X. Liu, Effects of different resource-sharing strategies in cloud manufacturing: a Stackelberg game-based approach. *Int. Prod. Res.* **61** (2023) 520–540.

[11] J. Jiang, Z.Y. Gu, J.X. Gao and T.M. Chen, Research on Cloud tenant data security protection Model based on sensitivity level. *Syst. Eng. Theory Pract.* **34** (2014) 2392–2401.

[12] J. Chen, S. Huang and Y.H. Liu, From enabling to enabling: Business Operation Management in the digital environment. *Manage. World* **36** (2020) 117–128.

[13] Q.Q. Zhang, X.L. Han and W.L. Duan, 5G Supply chain security status and standardization suggestions. *Res. Inf. Secur.* **8** (2022) 158–164.

[14] H.R. Nikkhah and V. Grover, Strategizing responses to data breaches: a multi-method study of organizational responsibility and effective communication with stakeholders. *J. Manage. Inf. Syst.* **41** (2024) 1042–1077.

[15] Z. Xu and S. Cao, Multi-source data privacy protection method based on homomorphic encryption and blockchain. *CMES-Comp. Model. Eng. Sci.* **136** (2023) 861–881.

[16] M. Sun, X.N. Ding and Q. Cheng, Federated learning scheme based on differential privacy. *Comput. Sci.* **51** (2024) 912–917.

[17] Y. Cui, V. Gaur and J. Liu, Supply chain transparency and blockchain design. *Manage. Sci.* **70** (2024) 3245–3263.

[18] Y.P. Tsang, Y. Fan, C.K.M. Lee and H.C.W. Lau, Blockchain sharding for e-commerce supply chain performance analytics towards Industry 5.0. *Enterp. Inf. Syst.* **18** (2024) 2311807.

[19] Y.F. Yao, T. Liu and G.X. Tian, Improve the sustainability of supply chain: the role of carbon abatement and blockchain technology. *RAIRO-Oper. Res.* **59** (2025) 115–148.

[20] K. Yang, H.B. Zhu, D. Li, W.B. Zhang, T. Yang and X.B. Tan, Load forecasting method of longitudinal federated learning Park based on compressed sensing. *Electr. Power Inf. Commun. Technol.* **22** (2024) 36–42.

[21] M.W. Yang, V.S. Jacob and R. Srinivasan, Cloud service model's role in provider and user security investment incentives. *Prod. Oper. Manage.* **30** (2020) 419–437.

[22] C.L. Stergiou, E. Bompoli and K.E. Psannis, Security and Privacy Issues in IoT-Based Big Data Cloud Systems in a Digital Twin Scenario. *Appl. Sci.* **13** (2023) 758-758.

[23] J.M. Sun, Z.H. Liu and Y.Z. Jiang, Game study on synergistic effect of building supply chain based on blockchain. *RAIRO-Oper. Res.* **58** (2024) 865–879.

[24] V. Chittipaka, S. Kumar, U. Sivarajah, J.L.H. Bowden and M.M. Baral, Blockchain Technology for Supply Chains operating in emerging markets: an empirical examination of technology-organization-environment (TOE) framework. *Ann. Oper. Res.* **327** (2023) 465–492.

[25] A. Gorkhali, L. Li and A. Shrestha, Blockchain: a literature review. *J. Manag. Anal.* **7** (2020) 321–343.

[26] Z. Fan, X. Wu and B. Cao, Considering the traceability awareness of consumers: Should the supply chain adopt the blockchain technology? *Ann. Oper. Res.* **309** (2020) 837–860.

[27] Y.V.R.S. Viswanadham and K. Jayavel, Design & development of hybrid electric Fish-Harris Hawks optimization-based privacy preservation of data in supply chain network with block chain technology. *Int. J. Inf. Technol. Decis. Mak.* **23** (2024) 1601–1632.

[28] I. Khan, Q.E. Ali, H.J. Hadi, N. Ahmad, G. Ali, Y. Cao and M.A. Alshara, Securing blockchain-based supply chain management: textual data encryption and access control. *Technologies* **12** (2024) 110.

[29] C. Xu, Y. Qu, Y. Xiang, T.H. Luan and L. Gao, An optimized privacy-protected blockchain system for supply chain on internet of things. *IEEE Int. Things* **11** (2024) 9019–9030.

[30] Z. Xiang, M. Wang and Y. Li, Blockchain technology investment decision and ordering strategy of fresh agricultural products retailers. *Front. Eng. Manag. Technol.* **43** (2024) 1–10.

[31] S. Zhao and W. Li, Blockchain-based traceability system adoption decision in the dual-channel perishable goods market under different pricing policies. *Int. J. Prod. Res.* **61** (2023) 4548–4574.

[32] G. Liu, Z. Li and J. Chen, Decision-making in the agricultural product supply chain based on blockchain technology. *Int. J. Simul. Process Modell.* **20** (2023) 71–86.

[33] J. Wei, X. Zhang, Y. Liu and Y. Jiang, Blockchain-based information sharing and supply and demand matching cloud platform for automotive manufacturing supply chain. *Ind. Manag. Data Syst.* **125** (2024) 687–710.

[34] F. Lupi, M.G. Cimino, T. Berlec, F.A. Galatolo, M. Corn, N. Rožman, A. Rossi and M. Lanzetta, Blockchain-based shared additive manufacturing. *Comput. Ind. Eng.* **183** (2023) 109497.

[35] S.A. Radmanesh, A. Haji and O. Fatahi Valilai, Blockchain-based architecture for a sustainable supply chain in cloud architecture. *Sustainability* **15** (2023) 9072.

[36] B. Niu, Z. Mu, B. Cao and J. Gao, Should multinational firms implement blockchain to provide quality verification? *Transp. Res. Part E: Logist. Transp. Rev.* **145** (2021) 102121.

[37] C. Tan, R. Liu and C. Zhao, Research on vaccine supply chain pricing strategy based on blockchain technology. *J. Manag. Eng.* **36** (2022) 205–220.

[38] D. Zhao and S. Chen, Research on pricing strategy of cloud manufacturing platform considering user time sensitivity. *J. Manag.* **18** (2021) 262–269.

[39] X. Pan, Research on value-added service charging model based on Industrial Internet platform. *China Manag. Sci.* **30** (2022) 239–249.

[40] L. Jiang, M.E. Mei and W. Zhong, Impact of percentage on Pricing Strategy of Mobile network operators. *J. Syst. Eng.* **28** (2013) 297–306+386.

[41] H. Li and Q. Xiao, Research on pricing strategy of car-hailing market under aggregation model. *Comput. Eng. Appl.* **58** (14) 236–244.

[42] R. Liu, C. Zhao and C. Tan, Game model and coordination strategy of vaccine supply chain under different charging conditions of blockchain platform. *J. Manag. Sci.* (2024) 1–17.

[43] B.C.M. Neubert, Valuation of a Saas company: a case study of Salesforce.Com. *Innov. Manag. Entrepren. Sustain.* (2018) 166.

[44] European Parliament and Council of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official J. Eur. Union.* **L119** (2016) 1–88.

[45] J.F. Tian and Q. Yang, An arbitrable outsourcing data audit scheme supporting credit reward and punishment and multi-user sharing. *J. Parallel Distrib. Comput.* **178** (2023) 100–111.

[46] Z.Y. Mou, X.X. Yang, K. Li *et al.*, Research on online agricultural support model and financing strategy of smart platform supply chain. *Chin. J. Manage. Sci.* **32** (2024) 170–181.
[47] A. Hervas-Drane and S. Shelegia, Retailer-led marketplaces. *Manag. Sci.* **71** (2025) 9650–9669.
[48] P. Gao, J.J. Nie and J. Xue, Green product R&D innovation and government subsidy strategy considering consumers' privacy concerns under blockchain. *Chin. J. Manage.* **21** (2024) 1097–1106.
[49] X.W. Yan, Z.F. Ping and B.C. Bing, An analysis of strategies for adopting blockchain technology in the fresh product supply chain. *Int. J. Prod. Res.* **61** (2023) 3717–3734.
[50] Z. Liu, C. Y. Ming, X.X. Zheng *et al.*, Research on cooperation mode selection and profit distribution of carbon complementary supply chain under "mandatory + voluntary" mechanism. *Syst. Eng. Theory Pract.* **45** (2025) 2264–2281.
[51] C. Santana and L. Albareda, Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda. *Technol. Forecast. Soc. Change.* **182** (2022) 121806.
[52] W.L. Wang, Q.N. Ren, Y.C. Zhu and T.J. Liu, Cost under the disturbance service quality acceptance decision and coordination of supply chain research. *Manag. Sci. China.* **32** (2024) 176–186.
[53] L.W. Ju, X. Qi, S.B. Yang, B.R. Nie, H.J. Zhu and O.T. Zhang, A hybrid gaming optimization model for rural distributed energy system clusters considering electricity-carbon-biomass peer-to-peer trading. *Syst. Eng. Theory Pract.* (2025) 1–14. (prepublish).
[54] F. Ecer, T. Murat, H. Dinçer and S. Yüksel, A fuzzy BWM and MARCOS integrated framework with Heronian function for evaluating cryptocurrency exchanges: a case study of Türkiye. *Financ. Innov.* **10** (2024) 31.
[55] Ali Research, Platform empowerment: research report on the digital transformation of China's manufacturing industry. (2023) 1–44.
[56] S.K. Singh, M. Jenamani, D. Dasgupta and S. Das, A conceptual model for Indian public distribution system using consortium blockchain with on-chain and off-chain trusted data. *Inf. Technol. Dev.* **27** (2021) 499–523.
[57] H.D. Chung, Y.M. Zhou and C. Choi, When Uber Eats its own business, and its competitors' too: resource exclusivity and oscillation following platform diversification. *Strat. Manag. J.* **46** (2025) 411–435.
[58] V. Nae, R. Prodan and A. Iosup, SLA-based operations of massively multiplayer online games in clouds. *Multimedia Syst.* **20** (2014) 521–544.
[59] H. Ke, X. Wang and A.D. Ralescu, Price and quality decisions in a co-opetitive supply chain considering two-dimensional consumer preferences. *J. Uncertain Syst.* **18** (2025) 2450032.
[60] N. Zhang, X. Yang and J. Wu, Pricing and coordinating of green manufacturing supply chain considering consumers' anticipated regret. *Electron. Commer. Res.* **25** (2025) 4737–4747.
[61] X.L. Zhang, H. Wang, X.Z. Zhao and D.D. Wu, Return decision model of the manufacturer-leading dual-channel supply chain. *Math. Prob. Eng.* **1** (2020) 8864672.
[62] A. Liu and Z. Han, Blockchain-based supply chain management system: framework design for achieving transparency and collaboration. *Int. J. High Speed Electron. Syst.* (2025) 2540241.
[63] C.V. Giada, C.M. Pia, S. Mattia and S. Raffaele, Artificial intelligence in supply chain and operations management: a multiple case study research. *Int. J. Prod. Res.* **62** (2024) 3333–3360.
[64] L. Wang, Initial investment cost of blockchain technology. *Blockch. Bus. Innov.* **4** (2022) 15–25.
[65] F.Z. Chen, Y.F. Wang and Z.H. Deng, Competing on price and guarantee compensation: heeding cloud consumer's quality perception. *Inf. Manag.* **60** (2023) 103884.
[66] Y. Zhou, Y. Zhang, M.I.M. Wahab and M. Goh, Channel leadership and performance for a closed-loop supply chain considering competition. *Transp. Res. Part E-Logist. Transp. Rev.* **175** (2023) 103151.