


## Article

# The Impact of Blockchain on Enterprises Sharing Real Data Based on Dynamic Evolutionary Game Analysis

Changjuan Zheng <sup>†</sup>, Xu Huang <sup>\*,†</sup>  and Ying Xu

School of Finance and Information, Ningbo University of Finance and Economics, Ningbo 315000, China

\* Correspondence: [huangxu@nbufe.edu.cn](mailto:huangxu@nbufe.edu.cn)

† These authors contributed equally to this work and should be considered co-first authors.

**Abstract:** The use of blockchain technology can ensure that data remains untampered with once it is on the chain. However, it doesn't guarantee the authenticity of data before it enters the chain. In this study, we developed a three-party dynamic evolutionary game model involving core enterprises, small and medium-sized enterprises (SMEs), and financial institutions. Our findings indicate that a blockchain supply chain (BSC) generates more economic benefits than a traditional supply chain (TSC). We then built a dynamic evolutionary game model between core enterprises and SMEs, which revealed that SMEs are influenced by core enterprises and tend to adopt the action strategies of the latter. Additionally, we developed a dynamic evolutionary game model between core enterprises and financial institutions and compared the reward and punishment mechanisms with the synergy payoff mechanism. In the reward and punishment mechanisms, the game is a zero-sum game, where one party's gains come at the expense of the other party. This mechanism has certain limitations and must meet specific conditions to improve the willingness of enterprises to share data. On the other hand, the synergy payoff mechanism enhances the authenticity of shared data by increasing the payoff for participants. When core enterprises play games with SMEs, the probability of core enterprises uploading real data and the distribution ratio of synergy payoff show an inverted U-shape. Similarly, core enterprises and financial institutions have comparable results in allocating synergy payoff. To leverage the synergy payoff mechanism, the distribution proportion of players participating in the synergy payoff should be considered fair. Finally, we validated our findings by simulating the models. If we can use blockchain technology to enhance the mutual trust between enterprises and banks, both banks and enterprises can achieve sustainable development.



**Citation:** Zheng, C.; Huang, X.; Xu, Y. The Impact of Blockchain on Enterprises Sharing Real Data Based on Dynamic Evolutionary Game Analysis. *Sustainability* **2023**, *15*, 9439. <https://doi.org/10.3390/su15129439>

Academic Editor: Assunta Di Vaio

Received: 30 January 2023

Revised: 4 June 2023

Accepted: 8 June 2023

Published: 12 June 2023



**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Keywords:** blockchain; data sharing; dynamic evolutionary game

## 1. Introduction

Within the supply chain, two types of enterprises exist: core enterprises and small and medium-sized enterprises (SMEs). Core enterprises possess high industry status, significant market influence, robust economic strength, and integrity. Consequently, financial institutions, such as banks, identify them as high-quality customers. In contrast, SMEs refer to independent enterprises with fewer than 50 employees, although the definition varies across countries and regions. For most enterprises, the upper limit is around 250 people, while in the United States, SMEs consist of no more than 500 employees. Typically, SMEs have low industry status, weak economic strength, and limited financial transparency, making them high-risk customers for financial institutions such as banks. In the supply chain, SMEs often rely on core enterprises to conduct business and have limited independence [1,2].

The traditional Internet suffers from several shortcomings when it comes to data sharing. Firstly, the dispersion of data across various organizations, coupled with the absence of standardized data formats and protocols, poses challenges for the circulation and sharing of data. Secondly, variations in data sources, collection methods, and processing

stages result in differing data quality among organizations, making it arduous to share data effectively. This issue becomes particularly problematic when attempting to share data between different sources. Thirdly, the sensitive and valuable nature of data necessitates consideration of privacy and security concerns during the sharing process. Any data leak or misuse can lead to severe losses for both organizations and individuals. Lastly, a lack of mutual trust between organizations acts as a deterrent to data sharing. Many organizations are reluctant to share their data with others due to concerns that it may undermine their competitive advantage [3].

To address these challenges and ensure the security and reliability of data, blockchain technology can be employed in the following ways: Firstly, decentralized storage allows for the distribution of data across multiple nodes instead of relying on a central authority, ensuring both decentralization and data security. Secondly, a distributed ledger created using blockchain technology enables multiple participants to record transactions involving shared data. This approach guarantees data transparency and authenticity and prevents tampering and data leakage. Thirdly, smart contracts can be utilized to establish rules and conditions that grant access and usage rights exclusively to authorized users. By automating contract execution and minimizing manual intervention, smart contracts mitigate risks and reduce operational costs. Lastly, encryption algorithms can be employed to encrypt data, ensuring privacy and data security. Access to and decryption of data are restricted to users with appropriate permissions. In summary, blockchain technology offers a more secure, decentralized, and reliable means of sharing data. However, it is important to note that data-sharing solutions leveraging blockchain technology must strike a balance between multiple factors such as cost, efficiency, scalability, and more [4].

Blockchain technology can ensure the quality of shared data, but if the data shared by enterprises itself is false, it is difficult for blockchain technology to effectively play a role. There is little literature on the authenticity of shared data. Blockchain technology has transformed transaction methods and improved financing efficiency [5]. By sharing data in the supply chain, costs can be reduced and the transaction scale can be expanded [6,7]. If the shared data is authentic, blockchain technology can foster trust between enterprises and build a good business environment. However, enterprises do not necessarily upload real data since blockchain technology is not mature. Hack attacks on the blockchain platform may also result in user data leakage, leading to huge losses for enterprises. Therefore, enterprises tend to forge data to hide their real behavior. Thus, improving the quality of uploaded data is vital in practice. In the transaction process, if the information of the enterprise is completely mastered by the other party, the enterprise will be at a disadvantage.

If we can use blockchain technology to enhance the mutual trust between enterprises and banks, both banks and enterprises can achieve sustainable development. Core enterprises, SMEs, and banks share data with each other, reducing financing costs. The enterprise has obtained sufficient funds to expand its scale of reproduction. Banks have also improved their efficiency by providing high-quality services. Therefore, our research on the impact of blockchain technology on data sharing is of great significance for the sustainable development of the financial industry.

We have focused on the above issues and provided a new research perspective for studying data sharing. We build a dynamic evolutionary game model for core enterprises, SMEs, and financial institutions. We analyze the factors that affect enterprises uploading of real data. From the perspective of theoretical modeling and numerical simulation, we have analyzed the impact of the reward and punishment mechanisms and synergy benefits on the authenticity of the enterprise's online data. The results show that SMEs are greatly influenced by core enterprises and often choose to follow the action strategies of the core enterprises. Financial institutions reward enterprises for uploading real data and punish them for uploading false data. However, the effectiveness of the reward and punishment mechanisms depends on certain conditions that need to be met to incentivize enterprises to

upload real data. Improving the synergy payoff and making reasonable distributions can effectively increase the willingness of enterprises to upload real data.

In terms of the advancement of knowledge, our study compared the different impacts of blockchain technology and traditional technology on data sharing. We have found that blockchain technology can reduce the cost of shared data and increase the benefits of shared data, which is beneficial for the promotion of blockchain technology in reality. Our research also points out that the collaborative benefit mechanism is superior to the reward and punishment mechanisms. In order to enhance the willingness of enterprises to share real data, we need to create a better environment to popularize the use of blockchain technology. When collaborative benefits increase, both supply chain enterprises and financial institutions will benefit, and the willingness of enterprises to share real data will increase. Our research has also gained some beneficial insights in the field of allocation. Our research indicates that the distribution ratio of collaborative benefits and willingness to cooperate satisfy the inverted U-shaped form. Our research can calculate the critical point of the distribution ratio, which is conducive to the rational distribution of benefits in reality.

The innovation of this paper is as follows: First, few studies in the literature have studied the authenticity of data shared by enterprises in the context of blockchain. Our research conclusions expand the theoretical scope of the authenticity of shared data. Second, the influence of core enterprises on SMEs is generally ignored in the existing literature's modeling process. We characterize the impact of core enterprises on SMEs as the effect of core enterprises on SMEs' business income, thereby expanding the scope of theoretical research. Third, compared to the previous literature that emphasizes the role of reward and punishment mechanisms, we point out that improving synergy payoff is more effective in promoting enterprises to upload real data. At the same time, we have studied the impact of the distribution proportion of synergy payoff on the equilibrium results, which has significant practical implications. Fourth, we discussed the impact of changes in the distribution ratio on the equilibrium results, highlighting the importance of fairness.

This paper is organized as follows: In Section 2, we reviewed the application of blockchain in data sharing and the research methods of dynamic evolutionary games. In Section 3, we build four dynamic evolutionary game models. We first prove that financial institutions, core enterprises, and SMEs prefer to use blockchain supply chain (BSC) compared with traditional supply chain (TSC). We build a game between core enterprises and SMEs. Theoretical results show that SMEs follow the action strategy of following the core enterprises. Then we build a game between core enterprises and financial institutions to analyze the impact of the two mechanisms on the sharing of real data. In Section 4, we use a numerical simulation to verify the conclusions of Section 3. In Section 5, we conducted a sensitivity analysis for the numerical simulation. In Section 6, we have prepared a corresponding summary and discussion. In Section 7, We have summarized the entire text and pointed out the theoretical significance and practical application of the paper.

## 2. Theoretical Background

### 2.1. Advantages and Disadvantages of Data Sharing

In the supply chain, data sharing promotes overall efficiency by enabling organic integration of information resources [8,9]. For example, in healthcare, sharing patient data among healthcare providers can lead to better coordination of care, reduced medical errors, and improved treatment outcomes. Extensive information integration and data sharing positively affect supply chain performance, such as increased cooperation and reduced inventory [10,11]. Sharing data helps address information asymmetry by providing more comprehensive and accurate information to all stakeholders. This can promote fairness, transparency, and trust in various domains, such as supply chain management and financial transactions. Data sharing facilitates collaboration and knowledge exchange among individuals, organizations, and sectors. It allows for a broader understanding of trends,

patterns, and insights derived from shared data, leading to improved decision-making and innovation. Data sharing can lead to societal benefits by enabling the development of innovative solutions such as smart cities, personalized services, and data-driven policymaking. It can also help address societal challenges such as public health crises or environmental issues.

However, data sharing also has some disadvantages that should be considered. Sharing data can raise concerns about privacy and security. Sensitive or personally identifiable information, if mishandled or accessed by unauthorized parties, can lead to privacy breaches or identity theft. Safeguarding data and ensuring appropriate data protection measures are crucial when sharing information [12]. Shared data may vary in quality, accuracy, and reliability. Inadequate data governance practices, data entry errors, or incomplete datasets can compromise the value and usefulness of shared information. Ensuring data quality and maintaining data standards are essential to mitigate these issues [13]. Sharing proprietary or confidential data may raise concerns about intellectual property rights. Organizations may be hesitant to share valuable data assets for fear of losing a competitive advantage or unauthorized use by others. Balancing the benefits of data sharing with intellectual property protection is a complex challenge [14]. Data sharing often involves compliance with various legal and regulatory frameworks, such as data protection regulations (e.g., GDPR) and industry-specific requirements. Ensuring compliance with these regulations can be complex and resource-intensive, adding complexity to data sharing initiatives. Establishing trust and fostering collaboration among data sharing partners can be challenging. Concerns about data misuse, competition, or differing incentives may hinder the willingness to share data. Building trust, establishing clear data sharing agreements, and addressing governance issues are critical for successful data sharing collaborations [15].

Although data sharing can generate numerous benefits, there are large differences in the income distribution between members of the supply chain [16]. According to rational assumptions, they tend to share information only on the premise of ensuring enterprises' interests. Otherwise, the enthusiasm of enterprises to implement information sharing will weaken, which in turn will lead to a reduction in supply chain revenue [17–20]. Data ownership, data risk, the cost of sharing, and other issues still restrict further improvement of data sharing [21–23]. The sharing of data in different solutions within the supply chain requires additional costs [24]. This is where blockchain technology can help increase data flow between different solutions. Blockchain technology can authorize and quickly access distributed data to avoid a single point of failure and enable real-time data supervision [25]. Therefore, blockchain technology is helpful for data sharing. However, the question of how to improve the quality of data sharing by enterprises in the supply chain remains unanswered.

## *2.2. How Blockchain Technology Affects Data Sharing*

Blockchain technology has several significant effects on data sharing. Blockchain is a decentralized, distributed ledger where data is maintained and verified by multiple participants. This decentralized nature enables more democratic and open data sharing, allowing participants to share data directly with each other without relying on intermediaries or third-party platforms. This eliminates trust issues in traditional data sharing and provides greater transparency and verifiability in data sharing [26]. Blockchain technology also enables the management of data access and usage permissions through smart contracts. Participants can define data ownership and control within smart contracts, specifying access conditions and usage rules. This grants data owners greater control, enhances privacy protection, and safeguards business secrets [27].

Blockchain employs cryptography and consensus algorithms to ensure data security and integrity. Once data is recorded on the blockchain, it is nearly impossible to tamper with or delete. This immutability enhances the credibility of data sharing, particularly in scenarios where data authenticity and tamper resistance are critical, such as supply chain management and intellectual property protection [28]. Traditional data sharing

often involves complex intermediary processes, including data transformation, verification, and authorization. Blockchain technology can simplify these processes by enabling peer-to-peer direct data exchange. Participants can automatically execute data exchange and verification logic through smart contracts, reducing manual intervention and processing time, thus enhancing the efficiency of data sharing [29]. Blockchains can incentivize data sharing through token-based economic models. Participants can earn tokens as rewards for sharing their data, which can be used to access other participants' data or other services. This incentive mechanism encourages data owners to actively engage in data sharing and promotes the development of data ecosystems [30].

It is important to note that while blockchain technology offers potential advantages for data sharing, there are also challenges and limitations. For instance, scalability and performance issues in blockchain still need to be addressed, especially when dealing with large-scale data and high-concurrency transactions. Additionally, data privacy and compliance concerns require attention and resolution. Therefore, the practical application of blockchain in data sharing requires careful consideration of the specific use case and the associated technical and regulatory considerations.

### *2.3. Dynamic Evolutionary Game Applied to Data Sharing*

Data sharing has become increasingly important in various domains, such as healthcare, finance, supply chain management, and social networks [31]. The decision to share data is a complex process influenced by multiple factors, including incentives, trust, and the evolving value of data. Traditional static game theory, which assumes rational actors, may not capture the complexity and dynamics of real-world data sharing scenarios. To address this limitation, researchers have turned to dynamic evolutionary game theory, which provides a more accurate representation of decision-making processes in the context of data sharing [32].

Dynamic evolutionary game theory introduces concepts from biology, such as adaptation and evolution, to study strategic interactions among individuals or organizations over time [33]. Unlike the static game theory assumption of perfect rationality, dynamic evolutionary games account for bounded rationality, recognizing that decision-makers have limited information and cognitive capacities. This framework allows for the study of how individuals or organizations adapt and learn from their own experiences and the behavior of others in a constantly changing environment.

By employing dynamic evolutionary game models, researchers can analyze the strategic decision-making processes in data sharing scenarios [34,35]. These models capture the dynamic nature of data sharing, where participants continually adjust their strategies based on the outcomes of previous interactions. Through this adaptation, the models provide a more realistic depiction of the evolving landscape of data sharing.

Moreover, dynamic evolutionary game theory enables the exploration of trust decision problems in data sharing [36,37]. Trust plays a crucial role in data sharing, as participants must weigh the benefits of sharing data against potential risks and uncertainties. The inclusion of reputation systems, reward-punishment mechanisms, and adaptive strategies in dynamic evolutionary game models allows for a deeper understanding of how trust can be established and maintained in data-sharing networks.

Furthermore, the impact of emerging technologies such as blockchain on data sharing can also be studied using dynamic evolutionary game theory [38]. Blockchain technology provides opportunities to enhance trust, security, and incentivization in data sharing. Dynamic evolutionary game models can shed light on the effects of blockchain technology on data sharing behaviors, exploring how it mitigates default risks, enhances trust, and promotes cooperative behaviors among participants. With the dynamic evolutionary game, the change in the quantity and value of data affects enterprises' decisions to share data. Then, a reward-punishment mechanism is introduced to solve the trust decision problem [39,40]. Using the dynamic evolutionary game model, scholars found that blockchain technology can mitigate the default risk of supply chain finance [41–43].

### 3. Model

Compared with TSC, blockchain technology uses encryption algorithms to ensure the security of data transmission, and the characteristics of smart contracts expand the transaction scale. This part will first use the three-party evolutionary game model to prove that financial institutions, core enterprises, and SMEs prefer to use the BSC. The use of blockchain technology has enabled enterprises and financial institutions to expand their scale and achieve sustainable development. In the context of BSC, we then explore the factors that influence data sharing between the three parties. In the supply chain, core enterprises often occupy the leading position because of their large scale and sufficient funds. Financial institutions, such as banks, tend to cooperate with core enterprises. On the other hand, SMEs are difficult to obtain bank loans for and therefore rely on core enterprises for transactions. On the basis of this observation, we construct a dynamic evolutionary game model between core enterprises and SMEs. On this basis, we study the game theory between core enterprises and financial institutions. Under specific conditions, core enterprises and financial institutions benefit from cooperation and achieve sustainable development.

#### 3.1. BSC vs. TSC in a Three-Party Dynamic Evolutionary Game Model

##### (1) Model Hypotheses

**Hypothesis 1:** The players in this model are core enterprises  $H$ , the SMEs  $J$ , and financial institution  $E$ . The three parties are participants in bounded rationality, and strategy selection gradually evolves and stabilizes to the optimal strategy over time.

**Hypothesis 2:** The strategy space for the core enterprises and SMEs is  $L = \{l_1, l_2\} = \{\text{upload real data, upload false data}\}$ . The probability that the core enterprise chooses action  $l_1$  is  $x$ , and the probability of choosing action  $l_2$  is  $1 - x$ . Similarly,  $y$  and  $1 - y$  are probabilities that SMEs choose action  $l_1$  and  $l_2$ , respectively. The strategy space for the financial institution is  $N = \{n_1, n_2\} = \{\text{BSC, TSC}\}$ . The probability that the financial institution chooses action  $n_1$  is  $v$ , and the probability of choosing action  $n_2$  is  $1 - v$ .

**Hypothesis 3:** In the TSC, the payoffs of core enterprises, SMEs, and financial institutions are  $R_{01}, R_{02}$ , and  $R_{03}$ , respectively. In the BSC, the payoffs of core enterprises, SMEs, and financial institutions are  $R_1, R_2$ , and  $R_3$ , respectively. Compared to TSC, BSC has expanded the transaction scale and improved the payoff of all three parties, so  $R_{01} < R_1, R_{02} < R_2, R_{03} < R_3$ .

**Hypothesis 4:** The number of data shared by core enterprises and SMEs is  $D_1, D_2$ , respectively. Data may be lost during transmission, resulting in poor quality shared data. In the TSC, after transmission is complete, the data shared by the core enterprises and SMEs are  $\rho D_1$  and  $\rho D_2$ . Where,  $\rho$  represents the accuracy of data in the TSC. Blockchain technology improves the accuracy and security of data transmission. Therefore, we assume that after data transmission in the BSC, the data shared by core enterprises and SMEs are still  $D_1$  and  $D_2$ .

**Hypothesis 5:** If both core enterprises and SMEs upload real data, an additional synergy payoff will be generated. The value of the synergy payoff is  $P$  and  $P_0$  in BSC and TSC, respectively. The synergy payoff is proportional to the sum of the uploaded data. Therefore, it is reasonable to suppose  $P = a(D_1 + D_2), P_0 = a(\rho D_1 + \rho D_2), a > 0$ , and  $a$  is the coefficient of the synergy payoff. Core enterprises and SMEs share the synergy payoff. The proportion of core enterprises is  $\lambda$ , the proportion of SMEs is  $1 - \lambda$ , where  $0 < \lambda < 1$ . Because core enterprises and SMEs share real data, the transaction scale expands, and financial institutions obtain additional payoff  $T, T_0$  in the BSC and TSC, respectively. In BSC, the supply chain expands the transaction scale and financial institutions gain more profits. Therefore, we assume that  $T > T_0$ .

**Hypothesis 6:** Uploading real data will bring risks, and the transaction’s counterparty will take the opportunity to lower the price after obtaining the real data. Thus, in the BSC, the risk cost for core enterprises and SMEs uploading real data is supposed as  $C_1, C_2$ , respectively. The cost of core enterprises is higher than that of SMEs, so  $C_1 > C_2$ . Similarly, in the TSC, the risk cost for core enterprises and SMEs uploading real data is supposed as  $C_{01}, C_{02}$ , respectively, where  $C_{01} > C_{02}$ . Blockchain technology improves the security of data transmission and sharing. Therefore, we assume  $C_{01} > C_1, C_{02} > C_2$ .

Based on the above assumptions, the related symbols are further described in Table 1.

**Table 1.** Symbols in a three-party dynamic evolutionary game.

Symbol	Definition
$x$	Probability of core enterprises uploading real data
$y$	Probability of SMEs uploading real data
$v$	Probability of a financial institution choosing blockchain
$\rho$	The accuracy of data transmission in the TSC
$\lambda$	Proportion of core enterprises’ share of synergy payoff
$R_{01}, R_{02}, R_{03}$	Payoffs of core enterprises, SMEs, and financial institutions in TSC
$R_1, R_2, R_3$	Payoffs of core enterprises, SMEs, and financial institutions in BSC
$D_1, D_2$	Number of data shared by core enterprises and SMEs, respectively
$P, P_0$	The value of the synergy payoff in BSC and TSC, respectively
$T, T_0$	When core enterprises and SMEs both upload real data, financial institutions obtain additional benefits from BSC and TSC, respectively
$C_{01}, C_{02}$	In the TSC, the risk costs faced by core enterprises and SMEs when sharing real data
$C_1, C_2$	In the BSC, the risk costs faced by core enterprises and SMEs when sharing real data

(2) Model Construction

From the above analysis, we can obtain the payoff matrix of the dynamic game between the core enterprises, the SMEs, and the financial institution, as shown in Table 2.

**Table 2.** The payoff matrix of the three-party dynamic evolutionary game in BSC vs. TSC.

			Financial Institution	
			BSC	TSC
Core enterprises	Upload real data	SMEs	$R_1 + \lambda P - C_1,$ $R_2 + (1 - \lambda)P - C_2,$ $R_3 + T$	$R_{01} + \lambda P_0 - C_{01},$ $R_{02} + (1 - \lambda)P_0 - C_{02},$ $R_{03} + T_0$
			$R_1 - C_1,$ $R_2,$ $R_3$	$R_{01} - C_{01},$ $R_{02},$ $R_{03}$
	Upload false data	SMEs	$R_1,$ $R_2 - C_2,$ $R_3$	$R_{01},$ $R_{02} - C_{02},$ $R_{03}$
			$R_1,$ $R_2,$ $R_3$	$R_{01},$ $R_{02},$ $R_{03}$

## (3) Model analysis.

In this section, we analyze whether financial institutions choose BSC or TSC, so we calculate and compare the payoff of core enterprises, SMEs, and financial institutions in BSC or TSC, respectively.

We assume that the average payoffs of core enterprises in BSC and TSC are  $K_{11}$  and  $K_{12}$ , respectively. After the calculation, we obtain the following formula:

$$K_{11} = xy(R_1 + \lambda P - C_1) + x(1 - y)(R_1 - C_1) + (1 - x)yR_1 + (1 - x)(1 - y)R_1 \quad (1)$$

$$K_{12} = xy(R_{01} + \lambda P_0 - C_{01}) + x(1 - y)(R_{01} - C_{01}) + (1 - x)yR_{01} + (1 - x)(1 - y)R_{01} \quad (2)$$

The average payoffs of SMEs in BSC and TSC are  $K_{21}$  and  $K_{22}$ , respectively. After the calculation, we obtain the following formula.

$$K_{21} = xy(R_2 + (1 - \lambda)P - C_2) + x(1 - y)R_2 + (1 - x)y(R_2 - C_2) + (1 - x)(1 - y)R_2 \quad (3)$$

$$K_{22} = xy[R_{02} + (1 - \lambda)P_0 - C_{02}] + x(1 - y)R_{02} + (1 - x)y(R_{02} - C_{02}) + (1 - x)(1 - y)R_{02} \quad (4)$$

The average payoffs of financial institutions in BSC and TSC are  $K_{31}$  and  $K_{32}$ , respectively. After the calculation, we obtain the following formula.

$$K_{31} = xy(R_3 + T) + x(1 - y)R_3 + (1 - x)yR_3 + (1 - x)(1 - y)R_3 \quad (5)$$

$$K_{32} = xy(R_{03} + T_0) + x(1 - y)R_{03} + (1 - x)yR_{03} + (1 - x)(1 - y)R_{03} \quad (6)$$

From (1) to (6), we obtain  $K_{11} > K_{12}$ ,  $K_{21} > K_{22}$ ,  $K_{31} > K_{32}$ . Therefore, financial institutions, core enterprises, and SMEs tend to choose BSC. In the subsequent analysis, we calculate and analyze in the context of blockchain by default.

### 3.2. Dynamic Game between Core Enterprises and SMEs in BSC

#### (1) Model Hypotheses

**Hypothesis 1:** The players in this model are core enterprises  $H$  and the SMEs  $J$ , both of which are limited rational agents. The strategy space for the core enterprises and SMEs is  $L = \{l_1, l_2\} = \{\text{upload real data, upload false data}\}$ . The probability that the core enterprise chooses action  $l_1$  is  $x$ , and the probability of choosing action  $l_2$  is  $1 - x$ . Similarly,  $y$  and  $1 - y$  are probabilities that SMEs choose action  $l_1$  and  $l_2$ , respectively.

**Hypothesis 2:** In BSC, the core enterprises and SMEs obtain payoff  $R_1, R_2$  respectively. The number of data shared by core enterprises and SMEs is  $D_1, D_2$ , respectively. If the two agents upload real data, an additional synergy payoff  $P$  is obtained. The synergy payoff is proportional to the sum of the uploaded data. Therefore, it is reasonable to suppose  $P = a(D_1 + D_2)$ ,  $a > 0$ , and  $a$  is the coefficient of the synergy payoff. The core enterprises and the SMEs share the synergy payoff. The proportion of core enterprises is  $\lambda$ , the proportion of SMEs is  $1 - \lambda$ , where  $0 < \lambda < 1$ . Therefore, the synergy payoff obtained by core enterprises and SMEs are  $(1 - \lambda)P$  and  $\lambda P$  respectively.

**Hypothesis 3:** Uploading real data will bring risks, and the transaction's counterparty will take the opportunity to lower the price after obtaining the real data. Thus, the risk cost for the core enterprises and SMEs uploading real data is supposed as  $C_1, C_2$  respectively. The cost of core enterprises is higher than that of SMEs, so  $C_1 > C_2$ . The total risk cost is proportional to the data on the chain, so  $C_1 = b_1 D_1$ ,  $C_2 = b_2 D_2$ ,  $b_1 > 0$ ,  $b_2 > 0$ , where  $b_1, b_2$  is the risk coefficient for uploading data.



**Hypothesis 4:** Core enterprises have a strong influence on SMEs. If an SME uploads false data, the core company will penalize the SME when it is discovered. For example, core enterprises may reduce or even cancel the contracts. The impact of SMEs uploading false data to core enterprises is negligible, but the penalties imposed on SMEs by core enterprises result in SMEs suffering huge losses. Assuming that the core enterprises penalize the SMEs after the SMEs upload false data, the SME's loss is  $M$ , where  $M > 0$ . Meanwhile, we assume that  $C_2 > M$ , since SMEs will lose core business (Table 3).

**Table 3.** Symbols in the dynamic game between core enterprises and SMEs.

Symbol	Definition
$x$	Probability of core enterprises uploading real data
$y$	Probability of SMEs uploading real data
$a$	The coefficient of the synergy payoff
$\lambda$	Proportion of core enterprises' share of synergy payoff
$b_1, b_2$	Risk coefficient of real data uploaded by core enterprises and SMEs
$R_1, R_2$	Payoffs of core enterprises and SMEs in BSC
$D_1, D_2$	Number of data shared by core enterprises and SMEs, respectively
$C_1, C_2$	In the BSC, the risk costs faced by core enterprises and SMEs when sharing real data
$M$	When SMEs upload false data, the penalty value of core enterprises to SMEs
$P$	The value of the synergy payoff in BSC

## (2) Model Construction

From the above analysis, we can obtain the payoff matrix of the dynamic game between the core enterprises and the SMEs, as shown in Table 4.

**Table 4.** Dynamic game payoff matrix between core enterprises and SMEs.

		SMEs	
		Upload Real Data	Upload False Data
Core enterprises	Upload real data	$R_1 + \lambda P - C_1,$ $R_2 + (1 - \lambda)P - C_2$	$R_1 - C_1,$ $R_2 - M$
	Upload false data	$R_1,$ $R_2 - C_2$	$R_1,$ $R_2 - M$

## (3) The replication dynamic equation

In the evolutionary game process, the core enterprises and SMEs continue to transfer stability strategies to the subsequent game process through learning and imitation. When  $x$  and  $y$  are equal to a certain value, both sides have a stable state. When the values of  $x$  and  $y$  change, the game strategy of both sides also changes.

According to Table 4, the expected payoff of the core enterprises  $H$  when adopting the strategies of "uploading real data" and "uploading false data" is  $V_{11}, V_{12}$ , respectively. The average payoff is  $V_1$ . The following information can be obtained as follows:

$$V_{11} = y(R_1 + \lambda P - C_1) + (1 - y)(R_1 - C_1) = \lambda P y + R_1 - C_1 \quad (7)$$

$$V_{12} = y R_1 + (1 - y) R_1 = R_1, \quad (8)$$

$$V_1 = x V_{11} + (1 - x) V_{12} = (\lambda P y - C_1) x + R_1. \quad (9)$$

The replication dynamic equation is a dynamic differential equation formed by simulating the replication dynamic mechanism process of the biological evolutionary game, which is used to describe the frequency of dominant strategies taken by game players. If  $V_{11} > V_1$ , core enterprises choose the action strategy of uploading real data, which can bring a higher payoff than the average payoff. At this time, the proportion  $x$  of core enterprises choosing to upload real data strategy will increase with time. If  $V_{11} < V_1$ , core enterprises choose the action strategy of uploading false data, which can bring a higher than average payoff. At this time, the proportion  $x$  of core enterprises choosing to upload false data strategy will increase with time. The replication dynamic equation of probability  $x$  for core enterprises to adopt the strategy of “uploading real data” is as follows.

$$F_H(x) = \frac{dx}{dt} = x(V_{11} - V_1) = x(1-x)(\lambda Py - C_1). \quad (10)$$

The steady-state value describes the extent to which core enterprises will choose to upload real data through a dynamic evolutionary game. The steady-state values  $x^* = 0$  and  $x^* = 1$  can be solved from  $F_H(x) = 0$ .

Assume that the expected payoff of SMEs  $J$  when adopting the strategy of “uploading real data” and “uploading false data” is respectively  $V_{21}, V_{22}$ . The average payoff is  $V_2$ . After the calculation, we obtain the following formula:

$$V_{21} = x(R_2 + (1-\lambda)P - C_2) + (1-x)(R_2 - C_2) = (1-\lambda)Px + R_2 - C_2, \quad (11)$$

$$V_{22} = x(R_2 - M) + (1-x)(R_2 - M) = R_2 - M, \quad (12)$$

$$V_2 = yV_{21} + (1-y)V_{22} = [(1-\lambda)Px + M - C_2]y + R_2 - M. \quad (13)$$

The replication dynamic equation of probability  $y$  for SMEs to adopt the strategy of “uploading real data” is as follows:

$$F_J(y) = \frac{dy}{dt} = y(V_{21} - V_2) = y(1-y)[(1-\lambda)Px + M - C_2]. \quad (14)$$

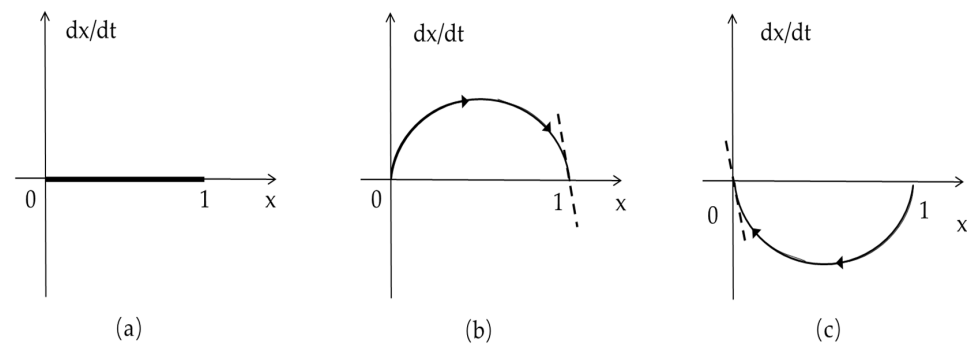
The steady-state value describes the extent to which SMEs will choose to upload real data through a dynamic evolutionary game. The steady-state values  $y^* = 0$  and  $y^* = 1$  can be solved from  $F_J(y) = 0$ .

#### (4) The trend and stability of the core enterprise action strategy

According to the replication dynamic Equation (10), its derivative can be calculated as follows:

$$\frac{dF_H(y)}{dy} = (1-2x)(\lambda Py - C_1) \quad (15)$$

When  $y = \frac{C_1}{\lambda P}$ ,  $\frac{dF_H(x)}{dx} = 0$ , that is,  $x \in [0, 1]$  is always stable. At this time, the replication dynamic equation of the core enterprise is shown in Figure 1a. When SMEs choose the action strategy of uploading real data with the probability of  $\frac{C_1}{\lambda P}$ , there is no difference between the payoff of core enterprises choosing to upload real data or false data. That is,  $x \in [0, 1]$  is the stable state of core enterprises.



**Figure 1.** (a) When  $y = \frac{C_1}{\lambda P}$ , phase diagram of core enterprise replication dynamics. (b) When  $y > \frac{C_1}{\lambda P}$ , phase diagram of core enterprise replication dynamics. (c) When  $y < \frac{C_1}{\lambda P}$ , phase diagram of core enterprise replication dynamics.

When  $y > \frac{C_1}{\lambda P}$ ,  $x^* = 0$  and  $x^* = 1$  are two possible stable points of  $x$ . Because  $\frac{dF_H(1)}{dx} < 0$ ,  $x^* = 1$  is an evolutionary stability strategy. The replication dynamics of the core enterprises are shown in Figure 1b. When the SMEs choose the action strategy of uploading real data with a probability higher than  $\frac{C_1}{\lambda P}$ , core enterprises will gradually change from uploading false data to uploading real data. At this time, uploading real data is the core enterprise’s evolutionary stability strategy.

When  $y < \frac{C_1}{\lambda P}$ ,  $x^* = 0$  and  $x^* = 1$  are two possible stable points of  $x$ . Because  $\frac{dF_H(0)}{dx} < 0$ ,  $x^* = 0$  is an evolutionary stability strategy. The replication dynamics of the core enterprises are shown in Figure 1c. When the SMEs choose the action strategy of uploading real data with a probability lower than  $\frac{C_1}{\lambda P}$ , core enterprises will gradually change from uploading real data to uploading false data. At this time, uploading false data is the core enterprise’s evolutionary stability strategy.

(5) The trend and the stability of the SMEs action strategies

According to the replication dynamic Equation (14), its derivative can be calculated as follows:

$$\frac{dF_J(y)}{dy} = (1 - 2y)[(1 - \lambda)Px + M - C_2]. \tag{16}$$

When  $x = \frac{C_2 - M}{(1 - \lambda)P}$ ,  $\frac{dF_J(y)}{dy} = 0$ , that is,  $y \in [0, 1]$  is always stable. When core enterprises choose the action strategy of uploading real data with the probability of  $\frac{C_2 - M}{(1 - \lambda)P}$ , there is no difference between the payoff of SMEs choosing to upload real data or false data. That is,  $y \in [0, 1]$  is the stable state of SMEs.

When  $x > \frac{C_2 - M}{(1 - \lambda)P}$ ,  $y^* = 0$  and  $y^* = 1$  are two possible stable points of  $y$ . Because  $\frac{dF_J(1)}{dy} < 0$ ,  $y^* = 1$  is an evolutionary stability strategy. When core enterprises choose the action strategy of uploading real data with a probability higher than  $\frac{C_2 - M}{(1 - \lambda)P}$ , SMEs will gradually change from uploading false data to uploading real data. At this time, uploading real data is the evolutionary stability strategy of SMEs.

When  $x < \frac{C_2 - M}{(1 - \lambda)P}$ ,  $y^* = 0$  and  $y^* = 1$  are two possible stable points of  $y$ . Because  $\frac{dF_J(0)}{dy} < 0$ ,  $y^* = 0$  is an evolutionary stability strategy. When core enterprises choose the action strategy of uploading real data with a probability lower than  $\frac{C_2 - M}{(1 - \lambda)P}$ , SMEs will gradually change from uploading real data to uploading false data. At this time, uploading false data is the evolutionary stability strategy of SMEs.

(6) Equilibrium analysis of dynamic evolution

Core enterprises and SMEs have reached a stable state through continuous evolution. According to Equations (10) and (14), let  $F_E(x) = 0$  and  $F_J(y) = 0$  to obtain the five equilibrium points of the replicated dynamic equation,  $O_1(0, 0)$ ,  $I_1(0, 1)$ ,  $H_1(1, 1)$ ,  $G_1(1, 0)$ ,  $E_1(x_1, y_1)$ , where  $x_1 = (C_2 - M)/[(1 - \lambda)P]$ ,  $y_1 = C_1/(\lambda P)$ .

According to the replication dynamic equation of core enterprises and SMEs, the corresponding Jacobian matrix can be obtained as follows:

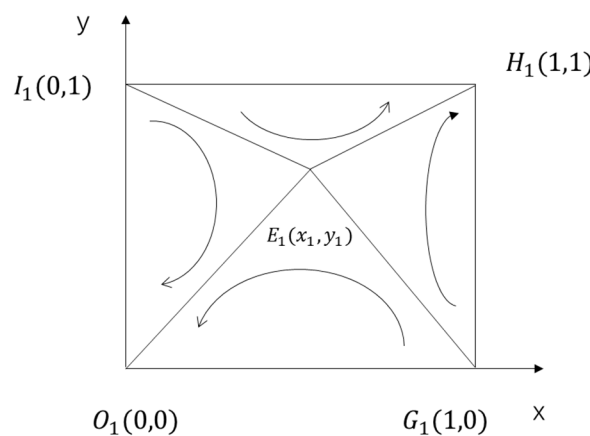
$$J_1 = \begin{pmatrix} \frac{\partial F_H(x)}{\partial x} & \frac{\partial F_H(x)}{\partial y} \\ \frac{\partial F_J(y)}{\partial x} & \frac{\partial F_J(y)}{\partial y} \end{pmatrix}. \tag{17}$$

The dynamic game solution space between core enterprises and SMEs is  $\{(x, y) | 0 \leq x \leq 1, 0 \leq y \leq 1\}$ , thus  $x_1, y_1 \in [0, 1]$ ,  $0 < C_2 - M < (1 - \lambda)P$ ,  $0 < C_1 < \lambda P$ . According to the stability theorem of the differential equation, when the determinant ( $DetJ$ ) of the Jacobian matrix of a local equilibrium point is greater than zero and the trace of the Jacobian matrix ( $TrJ$ ) is less than zero, the local equilibrium point is a stable strategy in an evolutionary game. The steady-state analysis of five local equilibrium points is shown in Table 5.

**Table 5.** Stability analysis of the evolutionary game.

Equilibrium Point	Det ( $J_1$ )	Symbol	Tr( $J_1$ )	Symbol	Equilibrium State
$O_1(0,0)$	$MC_1C_2$	+	$-C_1 - MC_2$	-	ESS
$I_1(0,1)$	$MC_2(\lambda P - C_1)$	+	$\lambda P - C_1 + MC_2$	+	Unstable point
$H_1(1,1)$	$(C_1 - \lambda P)[MC_2 - (1 - \lambda)P]$	+	$C_1 + MC_2 - P$	-	ESS
$G_1(1,0)$	$C_1[(1 - \lambda)P - MC_2]$	+	$C_1 - MC_2 + (1 - \lambda)P$	+	Unstable point
$E_1(x_1, y_1)$	$\lambda(\lambda - 1)P^2x_1(1 - x_1)y_1(1 - y_1)$	+	0		Saddle point

It can be seen in Table 5 that the two stable equilibrium points of the evolutionary game between core enterprises and SMEs are  $O_1(0,0)$  and  $H_1(1,1)$ . SMEs and core enterprises stay consistent in their action strategies and choose to upload real data or false data at the same time.  $I_1(0,1)$  and  $G_1(1,0)$  indicate that the action strategies of the core enterprises and the SMEs are inconsistent and are unstable points.  $E_1(x_1, y_1)$  is a saddle point. The phase diagram of the dynamic evolution of core enterprises and SMEs is shown in Figure 2.



**Figure 2.** Phase diagram of the evolutionary game between core enterprises and SMEs.

$E_1(x_1, y_1)$  is the key point where the replication dynamic curve tends to  $O_1(0,0)$  and  $H_1(1,1)$ . If the initial point of the game between core enterprises and SMEs is near  $E_1$ , a slight disturbance will affect the trend of the replication dynamic curve. The point at which the curve ultimately tends to ultimately depends on the area  $S_1$  of polygon  $O_1I_1E_1G_1$  and the area  $S_2$  of polygon  $I_1H_1G_1E_1$ . If  $S_1 > S_2$ , the copied dynamic curve will tend to  $O_1(0,0)$ . Both core enterprises and SMEs tend to upload the evolution results of false data. If  $S_1 < S_2$ , the replication dynamic curve will tend to  $H_1(1,1)$ . Both core enterprises and SMEs tend to upload the evolution results of real data. Analyze the factors that influence

the tendency of both parties to upload real data. The key is to analyze the factors that affect  $S_2$  changes. After calculation, the  $S_2$  formula is as follows.

$$S_2 = 1 - \frac{1}{2}(x_1 + y_1) = 1 - \frac{1}{2} \cdot \frac{\lambda(C_2 - M) + (1 - \lambda)C_1}{\lambda(1 - \lambda)P}. \quad (18)$$

**Proposition 1.** (i) The higher the synergy payoff between core enterprises and SMEs, the more likely both parties will upload real data. The greater the influence of the core enterprises on the SMEs, the more the parties tend to upload real data. (ii) The higher the risk cost of uploading data by core enterprises and SMEs, the more likely they are to upload false data. (iii) The proportion of real data uploaded by both parties and the distribution of collaboration payoff present an inverted U-shaped result. With the increase in the proportion of collaboration payoff allocated to core enterprises, both parties tend to upload real data. When the proportion of the distribution exceeds a certain threshold, with an increasing proportion of the distribution, both parties tend to upload false data.

(The proof of Proposition 1 is shown in Appendix A.)

It can be found from Proposition 1 that when the synergy payoff increases, the willingness of core enterprises and SMEs to share real data also increases. At the same time, the core enterprises have a strong influence on the SMEs, leading SMEs to adopt the action strategy of following the core enterprises. The risk costs of uploading data affect the authenticity of shared data. Only by taking various measures to reduce risk cost can the authenticity of shared data be effectively improved. The principle of “giving priority to efficiency and giving consideration to fairness” should be followed in the distribution of synergy payoff. Core enterprises play a greater role and should be appropriately inclined toward core enterprises when allocating synergy payoff. The reason is that the core enterprises have larger scale, more data, and greater influence in transactions. However, the principle of fairness should also be followed. When the interests of SMEs are seriously damaged, SMEs will take a non-cooperative attitude. Therefore, the principles of efficiency first and fairness at the same time should be taken into account in the distribution of synergy payoff.

### 3.3. Dynamic Game between Core Enterprises and Financial Institution under the Reward and Punishment Mechanisms in BSC

According to Proposition 1, SMEs adopt the action strategy of following the core enterprises. Therefore, the game between core enterprises and financial institutions becomes more important. If financial institutions can build a reasonable reward and punishment mechanism to encourage core enterprises to upload real data, SMEs will also upload real data, and the quality of shared data will improve.

#### (1) Model Hypotheses

**Hypothesis 1:** The main players in this part are the core enterprises  $H$  and the financial institution  $E$ , both of which are limited in their rationality. The strategy space of the core enterprises is  $L = \{l_1, l_2\} = \{\text{upload real data, upload false data}\}$ . The probability that the core enterprise chooses action  $l_1$  is  $x$ , and the probability of choosing action  $l_2$  is  $1 - x$ . The strategy space of the financial institutions is  $W = \{w_1, w_2\} = \{\text{strict supervision, loose supervision}\}$ . The probability that the core enterprise chooses action  $w_1$  is  $z$ , and the probability of choosing action  $w_2$  is  $1 - z$ .

**Hypothesis 2:** In BSC, core enterprises and financial institutions can obtain  $R_1$  and  $R_3$  in the initial state. Under the financial blockchain platform, the number of online data for core enterprises is  $D_1$ . When financial institutions choose strict supervision, they can find out whether the data shared by the core enterprises are true. If the data for the core company are true, the financial institutions will reward the core company with the amount of  $\alpha D_1$ . Suppose the online data for the core enterprises is false. In that case, the core enterprises will receive punishment  $\beta D_1$ .  $\alpha$  and  $\beta$  are the reward and punishment coefficients of the

core enterprises. Financial institutions will not be able to identify the authenticity of data when they choose loose regulation, so they will not reward and punish enterprises.

**Hypothesis 3:** Enterprises upload real data, which is risky. Assume that the risk cost of uploading real data from core enterprises is  $C_1$ , which is proportional to the total amount of data on-line. Therefore, assume that  $C_1 = b_1D_1$ ,  $b_1 > 0$ , and  $b_1$  is the risk coefficient of core enterprises. When financial institutions adopt strict supervision, it will be more costly. Assuming that the cost of strict supervision is  $C_3$ , and the cost of loose supervision is small, it is set to 0 for convenience. In reality, if data leaks, the core enterprises will suffer a heavy loss, which is much greater than the supervision cost of a financial institution, so it is assumed that  $C_1 > C_3$ .

**Hypothesis 4:** If financial institutions choose strict supervision and ultimately ensure that core enterprises upload real data, their achievements on the blockchain financial platform will be rewarded by the superior institutions with the amount of  $\gamma D_1$ , where  $\gamma$  is the reward coefficient given to the financial institution (Table 6).

**Table 6.** Symbols in a dynamic game between core enterprises and financial institutions.

Symbol	Definition
$x$	Probability of core enterprises uploading real data
$z$	Probability of a financial institution choosing strict supervision
$\alpha$	When core enterprises upload real data, the reward coefficient of the financial institutions for core enterprises
$\beta$	When the core enterprise uploads false data, the penalty coefficient of the financial institution applies to the core enterprise
$\gamma$	Reward coefficient of superior institutions to financial institutions
$b_1$	Risk coefficient of real data uploaded by core enterprises
$R_1, R_3$	Payoffs of core enterprises and financial institutions in BSC, respectively
$D_1$	Number of data shared by core enterprises
$C_1$	In the BSC, the risk costs faced by core enterprises when sharing real data
$C_3$	Cost of a financial institution choosing strict supervision

(2) Model Construction

From the above analysis, we can obtain the dynamic game payoff matrix between the core enterprises and financial institutions, as shown in Table 7:

**Table 7.** Payoff matrix of dynamic games between core enterprises and financial institutions.

		Financial Institution	
		Strict Supervision	Loose Supervision
Core enterprises	Upload real data	$R_1 - C_1 + \alpha D_1,$ $R_3 - C_3 - \alpha D_1 + \gamma D_1$	$R_1 - C_1,$ $R_3$
	Upload false data	$R_1 - \beta D_1,$ $R_3 - C_3 + \beta D_1$	$R_1,$ $R_3$

(3) Model analysis

Similar to the research method in Section 3.2, the following conclusions can be drawn (see Appendix A for a detailed derivation).

**Proposition 2.** (i) *The more rewards the superior institution gives to financial institutions, the more financial institutions tend to be strictly supervised, and the core enterprises will choose to*

upload real data. (ii) The higher the risk cost of uploading data by the core enterprises, the more likely the core enterprises are to upload false data, and the financial institution chooses loose supervision. The higher the supervision cost of the financial institution, the more the financial institution tends to choose loose supervision, and the core enterprises will choose to upload false data.

(The proof of Proposition 2 is shown in Appendix A.)

It can be seen from Proposition 2 that the more financial institutions attach importance to the development of the blockchain financial platform, the more support they give to financial institutions, and the more they can promote financial institutions to choose strict supervision so as to improve the quality of the online data of core enterprises. As SMEs follow the action strategy of core enterprises, they also choose to upload real data in the background of the attention of higher authorities, thus improving the data quality of the blockchain financial platform as a whole. The reasonable and effective use of blockchain and other technologies can effectively promote enterprises to upload real data by improving regulatory efficiency, ensuring the security of blockchain financial platform data, and reducing regulatory and risk costs. The formula of the partial derivative ( $\partial S/\partial\alpha, \partial S/\partial\beta$ ) is too complex to determine the symbol. We analyze it in the simulation part.

#### 3.4. Dynamic Game between Core Enterprises and Financial Institutions under the Synergy Payoff Mechanism in BSC

This part focuses on building new paths and methods to improve the authenticity of enterprise online data. That is, core enterprises upload real data, and financial institutions choose strict supervision to bring synergy payoffs to core enterprises and financial institutions. Strict supervision of financial institutions improves online data quality and reduces financial risks caused by false data. At the same time, the higher the online data quality of the core enterprises, the more widely the blockchain will be promoted, and more enterprises will tend to use the blockchain financial platform. As enterprises upload more real data, it will promote transaction scale and generate higher profits. At the same time, the use of blockchain technology can improve transaction efficiency and reduce transaction costs. The application of blockchain technology benefits both financial institutions and enterprises. That is, the improvement of the quality of shared data will increase the synergy payoff, which will benefit both players.

This part of the model explains how the size and division of the synergy payoff affect the quality of the data on the blockchain financial platform. The hypotheses in this part are basically consistent with those in Section 3.3. This part does not consider the reward or punishment of financial institutions for the core enterprises' uplink data, nor the reward of superior institutions for financial institutions. Assuming that financial institutions are strictly supervised and core enterprises share real data, a synergy payoff  $Q$  will be generated. The core enterprises and financial institutions obtain  $\rho Q$  and  $(1 - \rho)Q$ , where  $0 < \rho < 1$ ,  $\rho$  refers to the distribution proportion obtained by the core enterprises from the synergy payoff (Table 8).

**Table 8.** Symbols in a dynamic game between core enterprises and financial institutions.

Symbol	Definition
$x$	Probability of core enterprises uploading real data
$z$	Probability of a financial institution choosing strict supervision
$\rho$	The distribution proportion obtained by the core enterprises from the synergy payoff
$Q$	Synergy payoff is generated when core enterprises upload real data and financial institutions strictly supervise
$R_1, R_3$	Payoffs of core enterprises and financial institutions in BSC, respectively
$C_1$	In the BSC, the risk costs faced by core enterprises when sharing real data
$C_3$	Cost of a financial institution choosing strict supervision

From the above analysis, we can obtain the dynamic game payoff matrix between the main enterprises and financial institutions, as shown in Table 9. Similar to the research method in Section 3.1, the following conclusions can be drawn (see Appendix A for a detailed derivation).

**Table 9.** Payoff matrix of dynamic games between core enterprises and financial institutions.

		Financial Institution	
		Strict Supervision	Loose Supervision
Core enterprises	Upload real data	$R_1 - C_1 + \rho Q,$ $R_3 - C_3 + (1 - \rho)Q$	$R_1 - C_1,$ $R_3$
	Upload false data	$R_1,$ $R_3 - C_3$	$R_1,$ $R_3$

**Proposition 3.** (i) The greater the synergy payoff created by financial institutions and core enterprises, the more financial institutions tend to be strictly supervised, and core enterprises will choose to upload real data. (ii) With the increase in the proportion of synergy payoff allocated to core enterprises, financial institutions tend to be strictly supervised, and core enterprises tend to upload real data. However, when the distribution ratio exceeds a certain threshold, with an increasing distribution ratio, financial institutions tend to loosen supervision, and core enterprises tend to upload false data.

(The proof of Proposition 3 is shown in Appendix A.)

As seen in Proposition 3, the greater the synergy payoff created by financial institutions and core enterprises, the more it can promote financial institutions to choose strict supervision and core enterprises to choose to upload real data. As SMEs adopt the action strategy of following the core enterprises, improving the synergy payoff will improve the overall quality of shared data. Collaborating and sharing data between enterprises and financial institutions can effectively improve efficiency and promote sustainable development. Financial institutions should use blockchain technology to build a more powerful and complete financial platform that can not only ensure data security and reduce financial risks but also improve transaction scale and reduce transaction costs. The proportion of synergy payoff should be reasonably distributed to improve the enthusiasm of the core enterprises to upload real data. Financial institutions are service institutions, and core enterprises belong to the real economy. The proportion of synergy payoff should be appropriately inclined to core enterprises. In this way, core enterprises can be encouraged to upload real data and increase the scale of transactions. SMEs will follow the core enterprises' strategy. At the same time, we should pay attention to the interests of financial institutions, rationally distribute the synergy payoff, and encourage financial institutions to serve the real economy better.

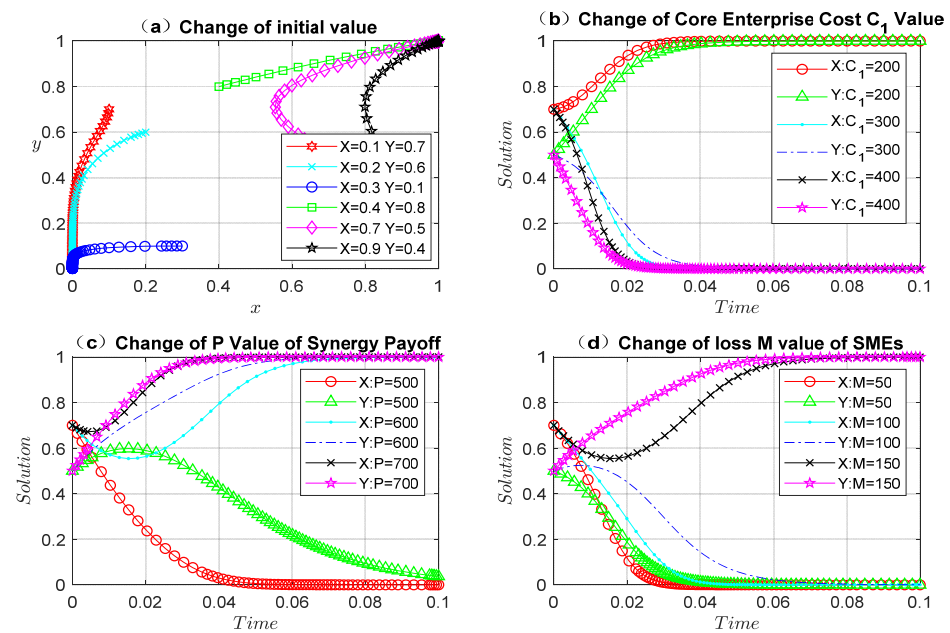
We use the three-party dynamic evolutionary game to analyze the reward and punishment mechanisms and the synergy payoff mechanism. We finally find that the conclusion is the same as Propositions 2 and 3. See Appendix A for a detailed calculation and demonstration steps.

#### 4. Simulation

##### 4.1. Dynamic Game Simulation between Core Enterprises and SMEs

We use MatlabR2019a to write simulation programs. This part verifies the impact of initial value changes on the evolution track of core enterprises and SMEs. We verify the conclusion of Proposition 1 through numerical simulation. The parameters selected for the numerical simulation in this part are as follows:  $D_1 = 600, D_2 = 300, C_1 = 300, C_2 = 200, P = 600, M = 150, a = 2/3, \lambda = 0.7$ . The evolutionary game curves of the core enterprises and SMEs are shown in Figure 3.





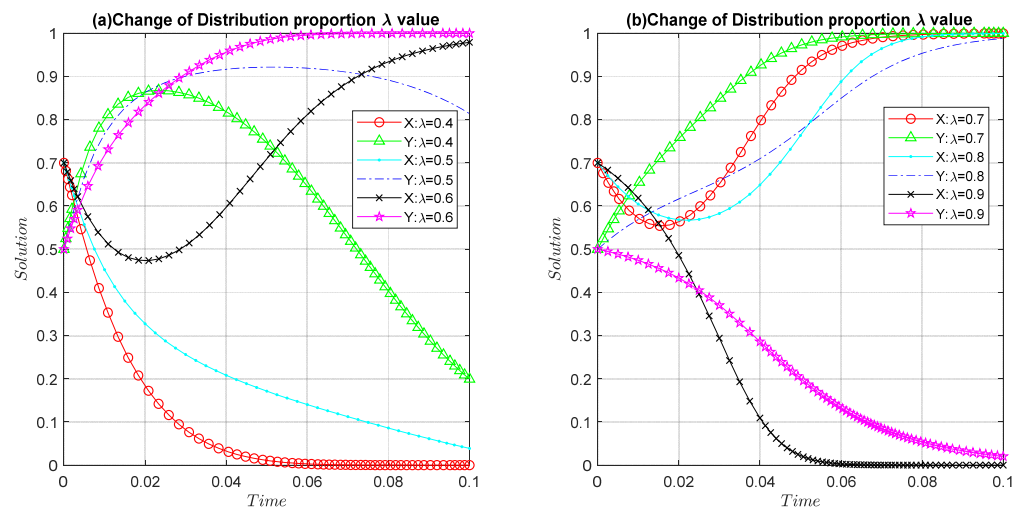
**Figure 3.** Process of dynamic evolution of core enterprises and SMEs.

In Figure 3a, selecting different initial points will result in the curve converging to different stable points  $(0,0)$ ,  $(1,1)$ . The simulation results show that the initial value affects the final results of the evolutionary game.

We discuss the impact of changes in the risk cost  $C_1$  of core enterprises on evolutionary game equilibrium (SME risk cost  $C_2$  has similar evolutionary results, as shown in Figure 3b). Due to  $C_1 < \lambda P = 420$ ,  $C_1$  is taken as 200, 300, and 400, respectively. When the risk cost  $C_1$  of core enterprises is 200, core enterprises and SMEs tend to upload real data. When  $C_1$  increases to 300 or 400, core enterprises and SMEs finally tend to upload false data. The simulation results prove the conclusion of Proposition 1 that the lower the risk cost of core enterprises and SMEs, the more inclined both sides will be to upload real data. The inspiration for reality is that the government should strengthen investment in new infrastructure and maintain the development of the blockchain platform. When the security of the uplink data is guaranteed, the willingness of enterprises to upload real data will increase.

According to Section 3.2,  $P$  needs to meet the conditions  $P > C_1/P$  and  $P > (C_2 - M)/(1 - \lambda)$ , so  $P > 429$ . We take  $P$  as 500, 600, and 700, respectively. Similarly, it can be seen from Figure 3c that the greater the synergy payoff  $P$  between core enterprises and the SMEs, the more it can promote core enterprises and the SMEs to upload real data. Because  $M > C_2 - (1 - \lambda)P = 20$ , so we take  $M$  equal to 50, 100, and 150, respectively. It can be seen in Figure 3d that the greater the influence of the core enterprises on SMEs, the more SMEs tend to follow the action strategies of the core enterprises. The government should create a reasonable business environment and improve the enthusiasm of enterprises to upload real data. At the same time, the government must fully harness the influence of core enterprises to drive economic development.

Figure 4 illustrates that when the proportion of synergy payoff allocated to core enterprises is small (40% and 50%), both core enterprises and SMEs eventually upload false data. When the proportion allocated to core enterprises is high (60%, 70%, and 80%), core enterprises and SMEs will eventually upload real data. However, when the proportion allocated to core enterprises is very high (90%), both core enterprises and SMEs eventually upload false data.



**Figure 4.** Impact of the change in the proportion of the synergy payoff on the dynamic evolutionary game.

In order to promote enterprises to upload real data, the distribution of synergy payoff should be consistent with the status of enterprises. Core enterprises play an important role in the supply chain, and synergy payoff should be allocated to core enterprises in a higher proportion. At the same time, we should also consider fairness, and the proportion allocated to SMEs should not be too low. Otherwise, it will damage the enthusiasm of SMEs and ultimately lead to the breakdown of cooperation. In summary, the allocation of the proportion of synergy payoff should follow the principle of “giving priority to efficiency and giving consideration to fairness”.

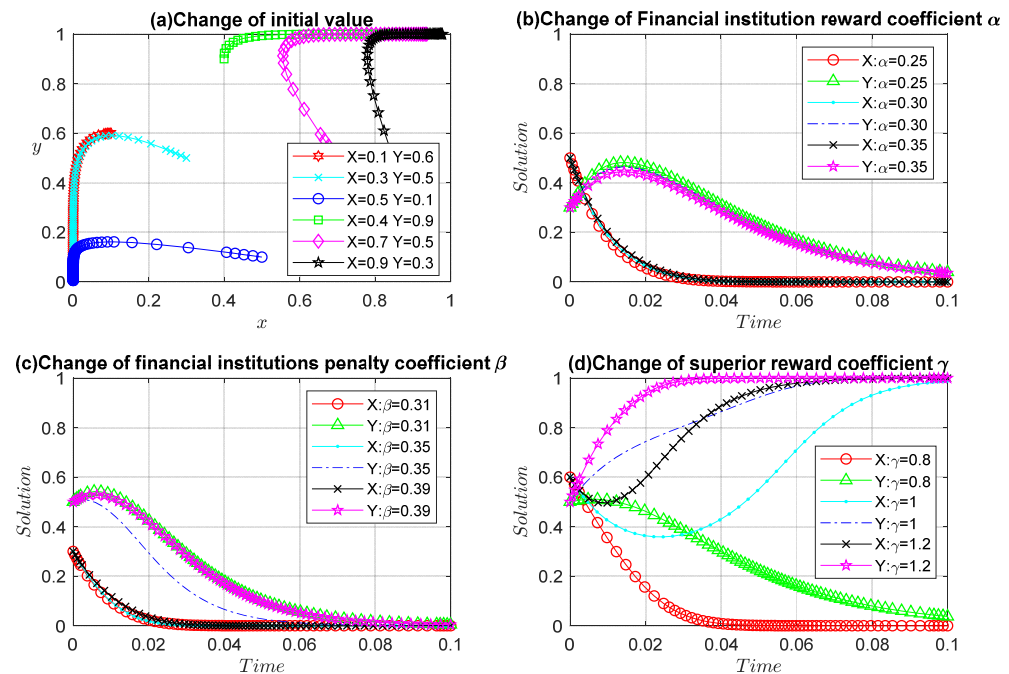
#### 4.2. Dynamic Game Simulation between Core Enterprises and Financial Institutions under the Reward and Punishment Mechanisms

The parameters selected in this part are as follows:  $D_1 = 600$ ,  $C_1 = 300$ ,  $C_3 = 250$ ,  $\alpha = 0.2$ ,  $\beta = 0.35$ ,  $\gamma = 1.2$ . The evolutionary game curve of the core enterprises and financial institutions is shown in Figure 4.

As can be seen in Figure 5a, the selection of different initial points will result in the evolution curve converging to different stable points (0,0) and (1,1). The simulation results show that the initial value affects the final results of the evolutionary game process. According to Section 3.3,  $C_1/D_1 - \beta < \alpha < \min\{\gamma - \beta, \gamma - C_3/D_1\}$ , so  $0.15 < \alpha < 0.7$ . We take  $\alpha$  as 0.25, 0.30, and 0.35. In Figure 5b, when the core enterprises upload real data, the financial institution rewards the core enterprises, which will affect the evolutionary game process. Along with  $\alpha$ , and with the increase in value, the evolution curve of the core enterprises and financial institutions changes upward at the initial stage but eventually converges to 0. That is, the financial enterprises finally choose to loosen supervision, and the core enterprises choose to upload false data. When changing the initial value or other parameter values for the sensitivity analysis, the increase of  $\alpha$  value can promote core enterprises to upload real data in some cases.

According to Section 3.3,  $C_1/D_1 - \alpha < \beta < C_3/D_1$ , so  $0.3 < \beta < 0.5$ . We take  $\beta$  as 0.35, 0.40, and 0.45, respectively. In Figure 5c, when core enterprises upload false data, the financial institution punishes them. The punishment mechanism affects the outcome of the evolutionary game process. With the increase of  $\beta$  value, financial institutions finally choose to loosen supervision, and the core enterprises choose to upload false data. When changing the initial value or other parameter values for sensitivity analysis, the increase of  $\beta$  value can promote core enterprises to upload real data in some cases. The simulation results show that the reward and punishment mechanisms does not always encourage the core enterprises to upload real data. Similarly,  $\gamma > C_3/D_1 + \alpha = 0.8$ , so we take  $\gamma$  as 1.1, 1.2, and 1.3, respectively. In Figure 5d, the reward given by the superior institution to the

financial institution affects the evolutionary game process. The higher the amount awarded by the superior institution, the more the financial institution is inclined to strict supervision and the more core enterprises are inclined to upload real data.



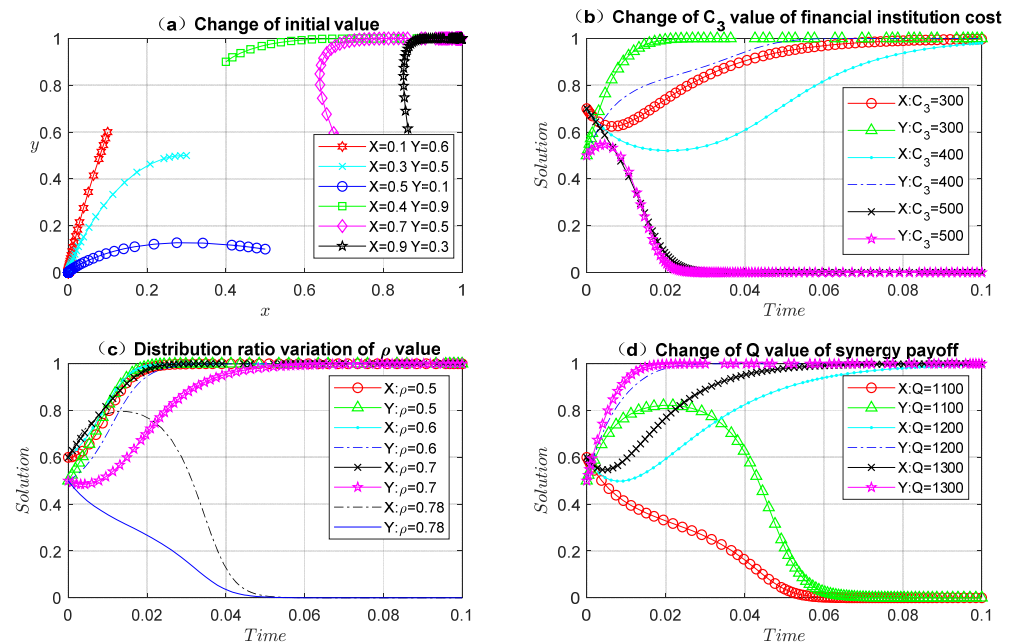
**Figure 5.** Process of dynamic evolution of core enterprises and financial institutions under the reward and punishment mechanisms.

#### 4.3. Simulation of a Dynamic Game between Core Enterprises and Financial Institutions under the Synergy Payoff Mechanism

The simulation results in Section 4.2 show that the reward and punishment mechanisms can only work if they meet certain conditions. This part is devoted to studying the impact of the synergy payoff generated by core enterprises and financial institutions on the dynamic evolutionary game process. The selected parameters are as follows:  $C_1 = 300$ ,  $C_3 = 250$ ,  $\rho = 0.3$ , and  $Q = 1200$ .

In Figure 6a, selecting different initial points will result in the evolution curve converging to different stable points (0, 0) and (1, 1). The simulation results show that the initial value affects the final results of the evolutionary game. According to Section 3.4  $0 < C_3 < (1 - \rho)Q = 840$ . We take  $C_3$  as 300, 400, and 500, respectively. In Figure 6b, we examine the impact of changes in the cost of financial institutions on the evolutionary game process. Optimizing the process and management of financial institutions through blockchain technology, reducing their operating costs, can effectively promote enterprises to upload real data.

Similarly,  $C_1/Q < \rho < 1 - C_3/Q$ , so  $0.25 < \rho < 0.75$ . We take  $\rho$  as 0.3, 0.4, and 0.5, respectively. As shown in Figure 6c, we examine the impact of the change in the proportion of synergy payoff distribution on the evolutionary game process. When selecting different initial points and parameter values for the sensitivity analysis, the impact of the change in the  $\rho$  value on the evolutionary game process is inverted U-shaped. With the rise of  $\rho$ , core enterprises tend to upload real data. When  $\rho$  exceeds a certain threshold, core enterprises tend to upload false data. Financial institutions have similar conclusions. The enlightenment of the above conclusions to reality is that in order to promote the core enterprises to upload real data, the proportion of synergy payoff should be appropriately tilted to the core enterprises. However, the interests of financial institutions must be taken into account, and then financial institution can better serve the real economy.

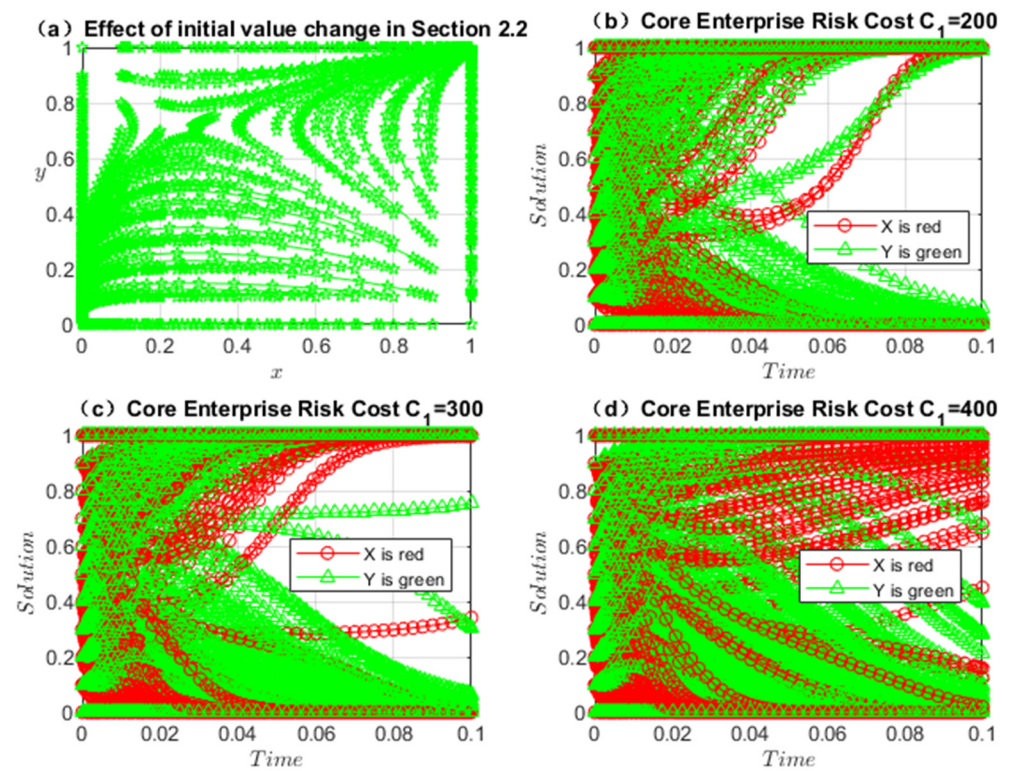


**Figure 6.** Process of dynamic evolution of core enterprises and financial institutions under the synergy payoff mechanism.

In the same way, we can obtain  $Q > \max\{C_1/\rho, C_3/(1-\rho)\}$ , so  $Q > 1000$ . We take  $Q$  as 1100, 1200, and 1300, respectively. Figure 6d shows that the greater the synergy payoff, the more it can promote enterprises to upload real data. The choice of strict supervision by financial institutions can reduce financial risks and improve synergy payoff. The reward and punishment mechanisms can promote enterprises to upload real data under certain conditions, but sometimes it does not work. The reason is that the reward mechanism will reduce the payoff of financial institutions, and the punishment mechanism will reduce the payoff of core enterprises. When the reward and punishment mechanisms increase the economic interests of one player, it will inevitably reduce the economic interests of another player, so it does not always play a role. As long as the synergy payoff is large enough, the synergy payoff mechanism can always encourage enterprises to upload real data. The reward and punishment mechanisms are zero-sum games, while the synergy payoff mechanism is not a zero-sum game. The synergy benefit mechanism can increase the payoffs for both players. Thus, the synergy payoff mechanism is more effective than the reward and punishment mechanisms.

## 5. Sensitivity Analysis

In order to verify the accuracy of the numerical simulation results, we have performed the corresponding sensitivity analysis. For Section 3.2, we have performed a sensitivity analysis on the selection of the initial point and  $C_1$ . Variables  $P$  can use the same method for sensitivity analysis. The parameters selected for the numerical simulation in this part are as follows:  $D_1 = 600$ ,  $D_2 = 300$ ,  $C_1 = 200, 300$  or  $400$ ,  $C_2 = 200$ ,  $P = 600$ ,  $M = 150$ ,  $a = \frac{2}{3}$ , and  $\lambda = 0.7$ . The results of the sensitivity analysis are shown in Figure 7. It can be seen in Figure 7a that different initial points will converge to the two steady-state equilibrium points (0, 0) and (1, 1). It can be seen from Figure 7b–d that the larger the  $C_1$ , the slower the convergence speed of the dynamic evolution curve. Thus, the probability that core enterprises upload real data is inversely proportional to the risk cost  $C_1$ . This conclusion is the same as that of Proposition 1.



**Figure 7.** Sensitivity analysis of the initial point and  $C_1$  in Section 3.2.

For variable  $M$ , we chose another method for sensitivity analysis. The reason is that similar simulation results can be obtained using the method in Figure 7. According to Section 3.2, the greater the  $M$  value, the greater the influence of core enterprises on SMEs. Since  $20 = C_2 - (1 - \lambda)P < M < C_2 = 200$ , we take  $M = 30$  as the initial value, the spacing is 10, and the final value is 190. The results of the sensitivity analysis of the variable  $M$  are shown in Figure 8. When the  $M$  value is small, SMEs converge on the strategy of uploading false data. When the  $M$  value gradually increases, SMEs converge on the strategy of uploading real data. It can also be seen from Figure 8 that SMEs always choose the same action strategy as core enterprises. The above conclusion is the same as Proposition 1.

For the reward and punishment mechanisms, we only conducted a sensitivity analysis of the reward coefficient because the punishment coefficient has similar results. According to Section 3.3  $C_1/D_1 - \beta < \alpha < \min\{\gamma - \beta, \gamma - C_3/D_1\}$ , so  $0.15 < \alpha < 0.7$ . The sensitivity analysis of the reward coefficient is shown in Figure 9a–c. When the reward coefficient is small ( $\alpha = 0.2$ ), core enterprises still tend to upload real data for different initial points. When the reward coefficient is large ( $\alpha = 0.6$ ), the strategy of core enterprises to upload real data does not increase significantly. Therefore, incentive mechanisms do not always work. The same applies to the punishment mechanism.

For the synergy payoff mechanism, we performed a sensitivity analysis for different values of the synergy payoff  $Q$ . According to Section 3.4,  $Q > \max\{C_1/\rho, C_3/(1 - \rho)\} = 100$ , we take  $Q = 1100$  as the initial value, the spacing is 100, and the end value is 2000. The results of the sensitivity analysis of the variable  $Q$  are shown in Figure 9d. The greater the synergy payoff, the greater the probability that core enterprises choose to upload real data, and the faster the convergence speed of copying dynamic curves. The synergy payoff increases the payoff of both players, so the synergy payoff mechanism is better than the reward and punishment mechanisms.

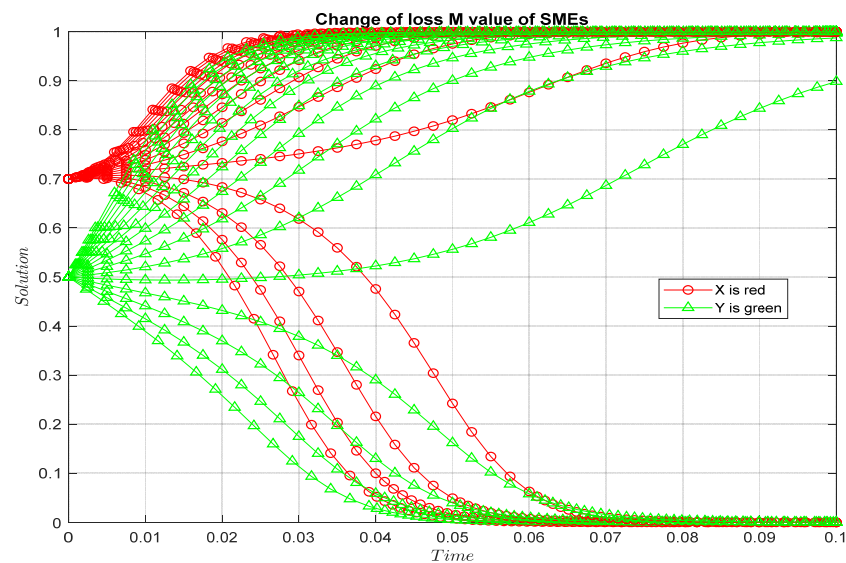


Figure 8. Sensitivity analysis of  $M$  in Section 3.2.

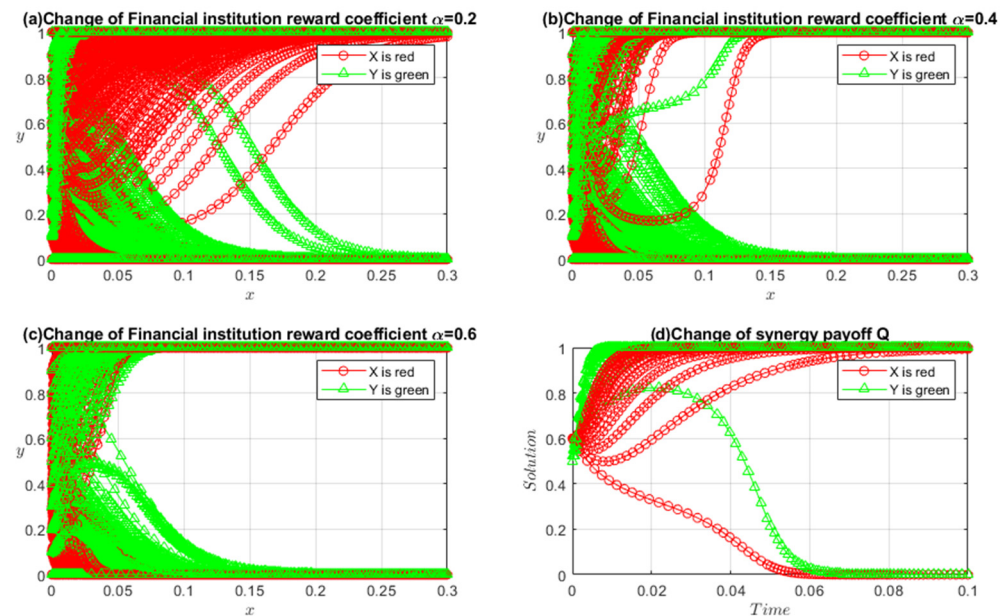


Figure 9. Sensitivity analysis of  $\alpha$  in Section 3.3 and  $Q$  in Section 3.4.

## 6. Discussion of Results

This paper constructs a dynamic evolutionary game model for core enterprises, SMEs, and financial institutions. We compared the blockchain model with the traditional model, and found that the blockchain model reduces costs and improves efficiency. Enterprises and financial institutions are more inclined to use blockchain technology. In reality, SMEs are dependent on core enterprises. SMEs need to obtain orders from core enterprises in order to survive. Without orders from core enterprises, it will be difficult for SMEs to survive. Core enterprises promote SMEs to adopt the same action strategies as core enterprises through their own influence.

In the game between core enterprises and financial institutions, the reward and punishment mechanisms must meet certain conditions to play a role. In the reward and punishment mechanisms, the game is zero-sum. When one player benefits, the other player will suffer. Therefore, in the context of a zero-sum game, how the benefits are distributed will affect the company's decision to share real data. Rewards from superior institutions can also promote the improvement of the quality of the data in the chain.

Compared to the reward and punishment mechanisms, the synergy payoff mechanism can more effectively promote enterprises to upload real data. The synergy payoff mechanism has broken through the category of zero-sum games. Under the reward and punishment mechanism, participants in the game are competitors, and benefiting one party means harming the other party's interests. Under the synergy payoff mechanism, the participants in the game change from a competitive relationship to a cooperative relationship. The more synergy payoffs brought about by cooperation, the more inclined enterprises are to upload real data. Therefore, we need to build a good environment to promote cooperation between enterprises and financial institutions rather than disgusting competition. To promote the uploading of real data by core enterprises and SMEs, it is necessary to reasonably distribute the synergy payoff. With the increased synergy payoff allocated to core enterprises, both parties tend to upload real data. However, both parties tend to upload false data with an increasing allocation proportion if the allocation proportion exceeds a certain threshold. The game between core enterprises and financial institutions on the synergy payoff has similar results.

## 7. Conclusions

### 7.1. Academic Implications

Existing research generally explores the construction of reasonable patterns for sharing data, but neglects the willingness of enterprises to share real data. Our research provides a new perspective for sharing data. We analyzed the factors that constrain companies from sharing real data and found that the cost of sharing real data reduces the willingness of companies to share real data. Our research also found that if blockchain technology can improve the security of shared data and reduce hacker attack losses, it will increase the willingness of enterprises to share data.

Our research also focuses on the impact of a reasonable distribution of benefits on the sharing of real data. We calculated the function formula between the proportion of income distribution and the willingness to share real data. This formula indicates that the willingness to share real data exhibits an inverted U-shaped relationship with the proportion of income distribution. In order to promote cooperation among game players, the distribution of profits must be within a reasonable range. Excessive inclination of profits toward one party may lead to a breakdown of cooperation. Our research points out that focusing solely on the development of blockchain technology is not enough. Blockchain technology is an important tool, and the key to achieving a cooperative relationship depends on expanding profits and the distribution of interests among multiple parties in the game.

### 7.2. Practical Implications

This paper explores how to build a reasonable mechanism to improve the willingness of enterprises to upload real data. In practice, the following measures can be considered to improve the authenticity of the data: (i) Clarify the ownership of data. If the ownership of data cannot be clearly defined, the benefits generated by data sharing will also be unclear. Only after the property rights of the data are determined can the profits generated by the data be determined. Laws and regulations related to data property rights should be established as soon as possible to promote enterprises' willingness to share real data. (ii) Improve the security of blockchain technology. The existing blockchain technology is not yet mature enough. Encryption algorithms and security measures still need to be strengthened. (iii) Establish reasonable incentive measures. Our research results indicate that the unreasonable distribution of the benefits generated by sharing data can lead to companies uploading false data. In order to enhance the willingness of enterprises to share real data, it is necessary to establish a reasonable allocation mechanism. Under a fair distribution mechanism, multiple parties in the game will construct a community of interests, thereby improving the quality of shared data. (iv) Enhance the level of trust between enterprises. Supply chain enterprises form a closed loop that can enhance mutual trust by sharing information. By integrating blockchain and the Internet, an anti-counterfeiting

traceability scheme could be formed to verify the authenticity of the data. Supply chain enterprises and financial institutions sign a letter of commitment and pay a certain deposit to ensure the authenticity of the data.

**Author Contributions:** C.Z. formed the idea of the paper and completed the review of the literature. X.H. constructed a theoretical model and carried out a numerical simulation. Y.X. revised and improved the article and adjusted its structure. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by China's Zhejiang philosophical and social science planning project under Grant No. 21NDJC168YB, Ningbo Natural Science Foundation No. 2023J061, the Recycling and Remanufacturing Network Organization and Its Governance under the Sharing Economy of China under Grant No. 18BGL184, the Financial Structure Governance of Supply Chain Based on Data Federation of China under Grant No. 21BGL088, the Zhejiang Provincial Natural Science Foundation of China under Grant No. LY20G030025, the Youth Fund for Humanities and Social Sciences Research of the Ministry of Education in Year 2022 under Grant No. 22YJC790077, and Major Humanities and Social Sciences Research Projects in Zhejiang higher education institutions under Grant No. 2023QN024.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix A

### Appendix A.1

#### Proof of Proposition 1.

(i) According to Formula (18),  $\frac{\partial S_2}{\partial P} > 0$ ;  $\frac{\partial S_2}{\partial M} > 0$ ;

(ii) According to Formula (18),  $\frac{\partial S_2}{\partial C_1} > 0$ ;  $\frac{\partial S_2}{\partial C_2} > 0$ ;

(iii) According to Formula (18),  $\frac{\partial S_2}{\partial \lambda} = \frac{1}{2P} \cdot \left[ -\frac{C_2 - M}{(1 - \lambda)^2} + \frac{C_1}{\lambda^2} \right] = \frac{(C_1 - C_2 + M)\lambda^2 - 2C_1\lambda + C_1}{2P\lambda^2(1 - \lambda)^2}$ .

Suppose  $f(\lambda) = (C_1 - C_2 + M)\lambda^2 - 2C_1\lambda + C_1$ , then the discriminant is  $\Delta = 4C_1(C_2 - M) > 0$ . Assume  $f(\lambda) = 0$ , According to the root formula, two roots can be obtained as follows:  $0 < \lambda_1 = \frac{C_1 - \sqrt{C_1(C_2 - M)}}{C_1 - C_2 + M} < 1$ ,  $\lambda_2 = \frac{C_1 + \sqrt{C_1(C_2 - M)}}{C_1 - C_2 + M} > 1$ . Thus, when  $\lambda \in (0, \lambda_1)$ ,  $\frac{\partial S_2}{\partial \lambda} > 0$ . When  $\lambda \in (\lambda_1, 1)$ ,  $\frac{\partial S_2}{\partial \lambda} < 0$ . That is, with the current distribution proportion  $\lambda$  in the interval  $(0, \lambda_1)$ , core enterprises and SMEs tend to upload real data with the increase in distribution proportion. Current distribution proportion  $\lambda$  in the interval  $(\lambda_1, 1)$ , core enterprises and SMEs tend to upload false data with the increase in distribution proportion.  $\square$

### Appendix A.2. Section 3.3 Model Analysis and Deduction

The replication dynamic equation of core enterprises and financial institutions is as follows:

$$U_H(x) = \frac{dx}{dt} = x(1 - x)[(\alpha + \beta)D_1z - C_1], \quad (A1)$$

$$U_W(z) = \frac{dz}{dt} = z(1 - z)[(\gamma - \alpha - \beta)D_1x + \beta D_1 - C_3]. \quad (A2)$$

Core enterprises and financial institutions have reached a stable state through continuous evolution. According to Equations (A1) and (A2), let  $U_H(x) = 0$  and  $U_W(z) = 0$  to obtain the five equilibrium points of the copied dynamic equation as  $O_2(0, 0)$ ,  $I_2(0, 1)$ ,  $H_2(1, 1)$ ,  $G_2(1, 0)$ ,  $E_2(x_2, z_2)$ , where  $x_2 = (C_3 - \beta D_1)/[(\gamma - \alpha - \beta)D_1]$ ,  $z_2 = C_1/[(\alpha + \beta)D_1]$ .



According to the replication dynamic equation of core enterprises and SMEs, the corresponding Jacobian matrix can be obtained as follows:

$$J_2 = \begin{pmatrix} \partial U_H(x)/\partial x & \partial U_H(x)/\partial z \\ \partial U_W(z)/\partial x & \partial U_W(z)/\partial z \end{pmatrix}. \tag{A3}$$

The solution space of the dynamic game between core enterprises and financial institutions is  $\{(x, z) | 0 \leq x \leq 1, 0 \leq z \leq 1\}$ ; thus,  $x_2, z_2 \in [0, 1], 0 < C_1 < (\alpha + \beta)D_1, \beta D_1 < C_3 < (\gamma - \alpha)D_1, \gamma > \alpha + \beta$ . The steady-state analysis of five local equilibrium points is shown in Table A1.

**Table A1.** Stability analysis of the evolutionary game.

Equilibrium Point	Det ( $J_1$ )	Symbol	Tr( $J_1$ )	Symbol	Equilibrium State
$O_2(0,0)$	$-C_1(\beta D_1 - C_3)$	+	$\beta D_1 - C_3 - C_1$	-	ESS
$I_2(0,1)$	$[(\alpha + \beta)D_1 - C_1](C_3 - \beta D_1)$	+	$\alpha D_1 - C_3 - C_1$	+	Unstable point
$H_2(1,1)$	$(C_1 - (\alpha + \beta)D_1)[(\alpha - \gamma)D_1 + C_3]$	+	$C_1 + C_3 - (\beta + \gamma)D_1$	-	ESS
$G_2(1,0)$	$C_1[(\gamma - \alpha)D_1 - C_3]$	+	$C_1 + (\gamma - \alpha)D_1 - C_3$	+	Unstable point
$E_2(x_2, y_2)$	$K$	+	0		Saddle point

Note:  $K = (\alpha + \beta)(\gamma - \alpha - \beta)D_1^2 x_2(1 - x_2)z_2(1 - z_2)$ .

Table A1 shows that the two stable equilibrium points of the evolution game between core enterprises and financial institutions are  $O_2(0,0)$  and  $H_2(1,1)$ , that is the stable state is divided into two cases. When financial institutions chooses strict supervision, core enterprises upload real data. When financial institutions choose loose supervision, core enterprises upload false data.  $I_2(0,1)$  and  $G_2(1,0)$  indicate that the action strategies of core enterprises and financial institutions are inconsistent, and they are unstable points.  $E_2(x_2, z_2)$  is a saddle point. Similar to the above analysis, the stable point to which the replication dynamic curve tends ultimately depends on the area  $S_3$  of the polygon  $O_2I_2E_2G_2$  and the area  $S_4$  of the polygon  $I_2H_2G_2E_2$ . If  $S_3 > S_4$ , the replication dynamic curve will tend to  $O_2(0,0)$ , financial institutions will choose loose regulation, and core enterprises will choose to upload false data. If  $S_3 < S_4$ , the replication dynamic curve will tend to  $H_2(1,1)$ , financial institutions will choose strict supervision, and core enterprises will choose to upload real data. After the calculation, the formula  $S_4$  is as follows:

$$S_4 = 1 - \frac{1}{2}(x_2 + z_2) = 1 - \frac{1}{2} \cdot \left[ \frac{C_3 - \beta D_1}{(\gamma - \alpha - \beta)D_1} + \frac{C_1}{(\alpha + \beta)D_1} \right]. \tag{A4}$$

**Proof of Proposition 2.**

- (i) According to Formula (A3),  $(\partial S_4)/\partial \gamma > 0$ .
- (ii) According to Formula (A4),  $\frac{\partial S_4}{\partial C_1} < 0; \frac{\partial S_4}{\partial C_3} < 0$ . □

*Appendix A.3. Section 3.4 Model Analysis and Deduction*

The replication dynamic equation of core enterprises and financial institution is as follows:

$$G_H(x) = \frac{dx}{dt} = x(1 - x)(\rho z Q - C_1), \tag{A5}$$

$$G_W(z) = \frac{dz}{dt} = z(1 - z)[(1 - \rho)z Q - C_3]. \tag{A6}$$

Core enterprises and financial institutions have reached a stable state through continuous evolution. Similar to the above analysis, from Formulas (A5) and (A6), let  $G_H(x) = 0$  and  $G_W(z) = 0$  to obtain the five equilibrium points of the replicated dynamic equation as  $O_3(0,0), I_3(0,1), H_3(1,1), G_3(1,0), E_3(x_3, z_3)$ , where  $x_3 = \frac{C_3}{[(1-\rho)Q]}, z_3 = \frac{C_1}{(\rho Q)}, 0 < C_1 <$

$\rho Q$ , and  $0 < C_3 < (1 - \rho)Q$ . The two stable equilibrium points of the evolution game between core enterprises and financial institution are  $O_3(0, 0)$  and  $H_3(1, 1)$ , that is, the stable state is divided into two cases. When financial institutions choose strict supervision, core enterprises upload real data, while when financial institutions choose loose supervision, core enterprises upload false data.  $I_2(0, 1)$  and  $G_2(1, 0)$  indicate that the action strategies of core enterprises and financial institutions are inconsistent, which are unstable points, and  $E_3(x_3, z_3)$  is a saddle point. How the copied dynamic curve converges depends on the area  $S_5$  of polygon  $O_3I_3E_3G_3$  and the area  $S_6$  of polygon  $I_3H_3G_3E_3$ . After the calculation, the formula  $S_6$  is as follows:

$$S_6 = 1 - \frac{1}{2}(x_3 + z_3) = 1 - \frac{1}{2} \cdot \left[ \frac{C_3}{(1 - \rho)Q} + \frac{C_1}{\rho Q} \right]. \quad (A7)$$

### Proof of Proposition 3.

- (i) According to Formula (A7),  $\frac{\partial S_6}{\partial Q} > 0$ .
- (ii) Let  $g(\rho) = (C_1 - C_3)\rho^2 - 2C_1\rho + C_1$ , and the discriminant is  $\Delta = 4C_1C_3 > 0$ . From the root formula, we can obtain two roots:  $0 < \rho_1 = \frac{C_1 - \sqrt{C_1C_3}}{C_1 - C_3} < 1$ ,  $\rho_2 = \frac{C_1 + \sqrt{C_1C_3}}{C_1 - C_3} > 1$ . Thus, when  $\rho \in (0, \rho_1)$ ,  $\frac{\partial S_6}{\partial \rho} > 0$ ; When  $\rho \in (\rho_1, 1)$ ,  $\frac{\partial S_6}{\partial \rho} < 0$ . That is, the current distribution proportion  $\rho$  in the interval  $(0, \rho_1)$ , with the increase of the distribution proportion, the equilibrium results of financial institutions and core enterprises converge (strict supervision, upload real data). The current distribution proportion  $\rho$  in the interval  $(\rho_1, 1)$ , with the increase of the distribution proportion, the equilibrium results of financial institutions and core enterprises converge (loose supervision, upload false data).  $\square$

### Appendix A.4. Reward and Punishment Mechanisms under a Three-Party Dynamic Evolutionary Game

#### (1) Model Hypotheses

**Hypothesis 1:** The players in this model are core enterprises  $H$ , the SMEs  $J$ , and financial institutions  $E$ . The three parties are the limited rational agents, and the strategy selection gradually evolves and stabilizes to the optimal strategy over time.

**Hypothesis 2:** The strategy space for the core enterprises and SMEs is  $L = \{l_1, l_2\} = \{\text{upload real data, upload false data}\}$ . The probability that the core enterprise chooses action  $l_1$  is  $x$ , and the probability of choosing action  $l_2$  is  $1 - x$ . Similarly,  $y$  and  $1 - y$  are probabilities that SMEs choose action  $l_1$  and  $l_2$ , respectively. The strategy space of the financial institution is  $W = \{w_1, w_2\} = \{\text{strict supervision, loose supervision}\}$ . The probability that the core enterprise chooses action  $w_1$  is  $z$ , and the probability of choosing action  $w_2$  is  $1 - z$ .

**Hypothesis 3:** In the BSC, the payoffs of core enterprises, SMEs, and financial institutions are  $R_1, R_2$  and  $R_3$ , respectively. The number of data shared by core enterprises and SMEs is  $D_1, D_2$ , respectively. If the data of the core company and SMEs are true, the financial institution will reward the core company and SMEs with the amount of  $\alpha D_1, \alpha D_2$ , respectively. Suppose the online data of the core enterprises and SMEs is false. In that case, the core enterprises and SMEs will receive punishment  $\beta D_1, \beta D_2$ , respectively.  $\alpha$  and  $\beta$  are the reward and punishment coefficients of the core enterprises and SMEs. Financial institutions will not be able to identify the authenticity of data when they choose loose regulation, so they will not be rewarded or punished.

**Hypothesis 4:** Uploading real data will bring risks, and the transaction's counterparty will take the opportunity to lower the price after obtaining the real data. Thus, in the BSC, the risk cost for core enterprises and SMEs uploading real data is supposed as  $C_1, C_2$ , respectively. The cost of core enterprises is higher than that of SMEs, so  $C_1 > C_2$ . Assuming

that the cost of strict supervision is  $C_3$ , and the cost of loose supervision is small, it is set to 0 for convenience. In reality, if data leaks, the core enterprises will suffer a heavy loss, which is much greater than the supervision cost of a financial institution, so it is assumed that  $C_1 > C_3$ .

**Hypothesis 5:** If a financial institution chooses strict supervision and ultimately ensures that core enterprises upload real data, the financial institution's achievements on the blockchain financial platform will be rewarded by the superior institutions with the amount of  $\gamma D_1$ , where  $\gamma$  is the reward coefficient given to the financial institution.

**Hypothesis 6:** Core enterprises have a strong influence on SMEs. If an SME uploads false data, the core company will penalize the SME when it is discovered. For example, core enterprises may reduce or even cancel the contracts. The impact of SMEs uploading false data to core enterprises is negligible, but the penalties imposed on SMEs by core enterprises result in SMEs suffering huge losses. Assuming that the core enterprises penalize the SMEs after the SMEs upload false data, the SME's loss is  $M$ , where  $M > 0$ . Meanwhile, we assume that  $C_2 > M$ , since SMEs will lose core business.

**Hypothesis 7:** If a financial institution chooses strict supervision and ultimately ensures that core enterprises and SMEs upload real data, the financial institution's achievements on the blockchain financial platform will be rewarded by the superior institutions with the amount of  $\gamma(D_1 + D_2)$ , where  $\gamma$  is the reward coefficient given to financial institution.

**Table A2.** Symbols under reward and punishment mechanisms in a three-party dynamic evolutionary game.

Symbol	Definition
$x$	Probability of core enterprises uploading real data
$y$	Probability of SMEs uploading real data
$z$	Probability of a financial institution choosing strict supervision
$\alpha$	When core enterprises and SMEs upload real data, the reward coefficient given by financial institutions to enterprises
$\beta$	When core enterprises and SMEs upload false data, the penalty coefficient given by financial institutions to enterprises
$\gamma$	Reward coefficient of superior institutions to financial institutions
$M$	When SMEs upload false data, the penalty value of core enterprises to SMEs
$R_1, R_2, R_3$	Payoffs of core enterprises, SMEs, and financial institutions in BSC
$D_1, D_2$	Number of data shared by core enterprises and SMEs, respectively
$C_1, C_2$	In the BSC, the risk costs faced by core enterprises and SMEs when sharing real data
$C_3$	Cost of a financial institution choosing strict supervision

## (2) Model Construction

From the above analysis, we can obtain the payoff matrix of the dynamic game between the core enterprises, the SMEs, and the financial institution, as shown in Table A3.

**Table A3.** The income matrix of a three-party dynamic evolutionary game under reward and punishment mechanisms.

			Financial Institution		
			Strict Supervision	Loose Supervision	
Core enterprises	Upload real data	SMES	Upload real data	$R_1 + \alpha D_1 - C_1,$ $R_2 + \alpha D_2 - C_2,$ $R_3 - C_3 - \alpha(D_1 + D_2)$ $+ \gamma(D_1 + D_2)$	$R_1 - C_1,$ $R_2 - C_2,$ $R_3$
			Upload false data	$R_1 + \alpha D_1 - C_1,$ $R_2 - \beta D_2 - M,$ $R_3 - C_3 - \alpha D_1 + \beta D_2$	$R_1 - C_1,$ $R_2 - M,$ $R_3$
	Upload false data	SMES	Upload real data	$R_1 - \beta D_1,$ $R_2 + \alpha D_2 - C_2,$ $R_3 - C_3 - \alpha D_2 + \beta D_1$	$R_1,$ $R_2 - C_2,$ $R_3$
			Upload false data	$R_1 - \beta D_1,$ $R_2 - \beta D_2 - M,$ $R_3 - C_3 + \beta(D_1 + D_2)$	$R_1,$ $R_2 - M,$ $R_3$

(3) Model analysis

The expected income of core enterprises uploading real data or false data is  $E_{11}, E_{12}$ . The average expected income of core enterprises is  $E_1$ .

$$E_{11} = yz(R_1 - C_1 + \alpha D_1) + y(1 - z)(R_1 - C_1) + (1 - y)z(R_1 + \alpha D_1 - C_1) + (1 - y)(1 - z)(R_1 - C_1), \tag{A8}$$

$$E_{12} = yz(R_1 - \beta D_1) + y(1 - z)R_1 + (1 - y)z(R_1 - \beta D_1) + (1 - y)(1 - z)R_1, \tag{A9}$$

$$E_1 = xE_{11} + (1 - x)E_{12}. \tag{A10}$$

The dynamic replication equation of probability  $x$  for core enterprises to adopt the strategy of “uploading real data” is as follows:

$$F(x) = \frac{dx}{dt} = x(E_{11} - E_1) = x(1 - x)[(\alpha + \beta)zD_1 - C_1]. \tag{A11}$$

We can calculate the derivative of  $F(x)$  and define the  $G(z)$  function as follows:

$$\frac{dF(x)}{dx} = (1 - 2x)[(\alpha + \beta)zD_1 - C_1], \tag{A12}$$

$$G(z) = (\alpha + \beta)zD_1 - C_1. \tag{A13}$$

According to the stability theorem of differential equations, the core enterprise needs to meet the following conditions when it chooses to upload real data in a stable state:  $F(x) = 0$  and  $\frac{dF(x)}{dx} < 0$ .

Let  $G(z) = 0$  to obtain  $z^* = \frac{C_1}{(\alpha + \beta)D_1}$ .  $G(z)$  is a monotonically increasing function of  $z$ . When  $z < z^*, G(z) < 0$ . At this time,  $x = 0$  is the evolutionary stability strategy (ESS) for core enterprises to upload real data. When  $z > z^*, G(z) > 0$ . At this time,  $x = 1$  is the evolutionary stability strategy (ESS) for core enterprises to upload real data.

The probability of core enterprises choosing to upload real data is  $V_{A1}$ , the formula is as follows:

$$U_1 = 1 - \frac{C_1}{(\alpha + \beta)^2 D_1}, \tag{A14}$$

According to (A14), the following formula can be obtained.

$$\frac{\partial U_1}{\partial C_1} < 0. \tag{A15}$$

It can be seen from (A15) that the probability of core enterprises uploading real data is inversely proportional to the risk cost  $C_1$ . The probability of core enterprises choosing to upload real data is not directly related to variables  $\alpha$  and  $\beta$ . This conclusion is consistent with the conclusion of Proposition 2.

Similarly, we can calculate the replication dynamic equation and the corresponding probability of SMEs choosing to upload real data.

$$F(y) = \frac{dy}{dt} = y(1-y)[(\alpha + \beta)zD_2 - C_2 + M], \quad (\text{A16})$$

$$U_2 = 1 - \frac{C_2 - M}{(\alpha + \beta)^2 D_2}. \quad (\text{A17})$$

According to (A17), the following formula can be obtained:

$$\frac{\partial U_2}{\partial C_2} < 0, \frac{\partial U_2}{\partial M} > 0. \quad (\text{A18})$$

It can be seen from (A18) that the probability of SMEs uploading real data is inversely proportional to the risk cost  $C_2$ , and is directly proportional to the penalty value  $M$  of core enterprises to SMEs. The probability of SMEs choosing to upload real data is not directly related to variables  $\alpha$  and  $\beta$ . This conclusion is consistent with the conclusion of Proposition 2.

Similarly, we can calculate the replication dynamic equation of a financial institution choosing strict supervision and the probability of a financial institution choosing strict supervision.

$$F(z) = \frac{dz}{dt} = z(1-z)[\gamma xy(D_1 + D_2) - (\alpha + \beta)xD_1 - (\alpha + \beta)yD_2 + \beta(D_1 + D_2) - C_3], \quad (\text{A19})$$

$$U_3 = 1 - \frac{C_3 - (\alpha + \beta)^2(D_1 + D_2)}{\gamma(D_1 + D_2)^2} \quad (\text{A20})$$

According to (A20), the following formula can be obtained:

$$\frac{\partial U_3}{\partial C_3} < 0, \frac{\partial U_3}{\partial \gamma} > 0. \quad (\text{A21})$$

It can be seen from (A21) that the probability of a financial institution choosing strict supervision is inversely proportional to the cost of supervision and is directly proportional to the reward coefficient of the superior institutions. This conclusion is consistent with the conclusion of Proposition 2.

#### Appendix A.5. The Synergy Payoff Mechanism under a Three-Party Dynamic Evolutionary Game

##### (1) Model Hypotheses

**Hypothesis 1:** The players in this model are core enterprises  $H$ , the SMEs  $J$ , and financial institutions  $E$ . The three parties are the limited rational agents, and the strategy selection gradually evolves and stabilizes to the optimal strategy over time.

**Hypothesis 2:** The strategy space for the core enterprises and SMEs is  $L = \{l_1, l_2\} = \{\text{upload real data, upload false data}\}$ . The probability that the core enterprise chooses action  $l_1$  is  $x$ , and the probability of choosing action  $l_2$  is  $1 - x$ . Similarly,  $y$  and  $1 - y$  are probabilities that SMEs choose action  $l_1$  and  $l_2$ , respectively. The strategy space of a financial institution is  $W = \{w_1, w_2\} = \{\text{strict supervision, loose supervision}\}$ . The probability that the core enterprises choosing action  $w_1$  is  $z$ , and the probability of choosing action  $w_2$  is  $1 - z$ .

**Hypothesis 3:** In the BSC, the payoffs of core enterprises, SMEs and financial institutions are  $R_1, R_2$ , and  $R_3$ , respectively. The number of data shared by core enterprises and SMEs is  $D_1, D_2$ , respectively.

**Hypothesis 4:** Uploading real data will bring risks, and the transaction's counterparty will take the opportunity to lower the price after obtaining the real data. Thus, in the BSC, the risk cost for core enterprises and SMEs uploading real data is supposed as  $C_1, C_2$ , respectively. The cost of core enterprises is higher than that of SMEs, so  $C_1 > C_2$ . Assuming that the cost of strict supervision is  $C_3$ , and the cost of loose supervision is small, it is set to 0 for convenience. In reality, if data leaks, the core enterprises will suffer a heavy loss, which is much greater than the supervision cost of a financial institution, so it is assumed that  $C_1 > C_3$ .

**Hypothesis 5:** Core enterprises have a strong influence on SMEs. If an SME uploads false data, the core company will penalize the SME when it is discovered. For example, core enterprises may reduce or even cancel the contracts. The impact of SMEs uploading false data to core enterprises is negligible, but the penalties imposed on SMEs by core enterprises result in SMEs suffering huge losses. Assuming that the core enterprises penalize the SMEs after the SMEs upload false data, the SME's loss is  $M$ , where  $M > 0$ . Meanwhile, we assume that  $C_2 > M$ , since SMEs will lose core business.

**Hypothesis 6:** When financial institutions choose to strictly supervise and core enterprises and SMEs choose to upload real data, the cooperation of the three parties will generate a synergy payoff  $B$ . Assume that the proportion of synergy payoff allocated to core enterprises, SMEs and financial institutions is  $\theta_1, \theta_2$ , and  $\theta_3$ . Where  $\theta_1 + \theta_2 + \theta_3 = 1$ ,  $0 < \theta_1, \theta_2, \theta_3 < 1$ . (The difference between Hypothesis 6 in Appendix A.5 and Section 3.4 is that, two parties (financial institutions and core enterprises) distribute synergy payoffs in Section 3.4. Hypothesis 6 in Appendix A.5 is that three parties (financial institutions, core enterprises, and SMEs) jointly distribute synergy payoffs. Therefore, the distribution proportion has been reset.)

**Hypothesis 7:** If the risk cost of core enterprises and SMEs is greater than the synergy payoff obtained, core enterprises and SMEs tend not to upload real data. The same applies to financial institutions. Therefore, we assume that the risk cost is less than the synergy payoff. Where  $C_1 < \theta_1 B, C_2 < \theta_2 B, C_3 < \theta_3 B$ . Based on the above assumptions, related symbols are further described in Table A4.

**Table A4.** Symbols under reward and punishment mechanisms in a three-party dynamic evolutionary game.

Symbol	Definition
$x$	Probability of core enterprises uploading real data
$y$	Probability of SMEs uploading real data
$z$	Probability of a financial institution choosing strict supervision
$\theta_1$	Proportion of synergy payoff allocated to core enterprises
$\theta_2$	Proportion of synergy payoff allocated to SMEs
$\theta_3$	Proportion of synergy payoff allocated to financial institutions
$M$	When SMEs upload false data, the penalty value of core enterprises to SMEs
$R_1, R_2, R_3$	Payoffs of core enterprises, SMEs, and financial institutions in BSC

**Table A4.** Cont.

Symbol	Definition
$D_1, D_2$	Number of data shared by core enterprises and SMEs, respectively
$C_1, C_2$	In the BSC, the risk costs faced by core enterprises and SMEs when sharing real data
$C_3$	Cost of a financial institution choosing strict supervision

(2) Model Construction

From the above analysis, we can obtain the payoff matrix of the dynamic game between the core enterprises, the SMEs, and the financial institutions, as shown in Table A5.

**Table A5.** The income matrix of a three-party dynamic evolutionary game under reward and punishment mechanisms.

			Financial Institution	
			Strict Supervision	Loose Supervision
Core enterprises	Upload real data	SMEs	$R_1 + \theta_1 B - C_1,$ $R_2 + \theta_2 B - C_2,$ $R_3 - C_3 + \theta_3 B$	$R_1 - C_1,$ $R_2 - C_2,$ $R_3$
			$R_1 - C_1,$ $R_2 - M,$ $R_3 - C_3$	$R_1 - C_1,$ $R_2 - M,$ $R_3$
	Upload false data	SMEs	$R_1,$ $R_2 - M,$ $R_3 - C_3$	$R_1,$ $R_2 - C_2,$ $R_3$
			$R_1,$ $R_2 - M,$ $R_3 - C_3$	$R_1,$ $R_2 - M,$ $R_3$

(3) Model analysis

We can calculate the replication dynamic equation and the corresponding probability of core enterprises choosing to upload real data.

$$F(x) = \frac{dx}{dt} = x(1-x)(\theta_1 y z B - C_1), \tag{A22}$$

$$V'_1 = 1 + \frac{C_1}{\theta_1 B} \ln \frac{C_1}{\theta_1 B}. \tag{A23}$$

According to (A23), the following formula can be obtained.

$$\frac{\partial U'_1}{\partial C_1} < 0, \frac{\partial U'_1}{\partial B} > 0. \tag{A24}$$

It can be seen from Formula (A24) that the probability of core enterprises uploading real data is inversely proportional to the risk cost  $C_1$  and is directly proportional to the value of synergy payoff  $B$ . This conclusion is consistent with the conclusion of Proposition 3.

Similarly, we can calculate the replication dynamic equation and the corresponding probability of SMEs choosing to upload real data.

$$F(y) = \frac{dy}{dt} = y(1-y)(\theta_2 x z B + M - C_2), \tag{A25}$$

$$V'_2 = 1 + \frac{C_2 - M}{\theta_2 B} \ln \frac{C_2 - M}{\theta_2 B}. \tag{A26}$$

According to (A26), the following formula can be obtained:

$$\frac{\partial U'_2}{\partial C_2} < 0, \frac{\partial U'_2}{\partial B} > 0, \frac{\partial U'_2}{\partial M} > 0. \quad (\text{A27})$$

It can be seen from (A27) that the probability of SMEs uploading real data is inversely proportional to the risk cost  $C_2$ , and is directly proportional to the value of synergy payoff  $B$ , and the penalty value  $M$  of core enterprises to SMEs. This conclusion is consistent with the conclusion of Proposition 3.

Similarly, we can calculate the replication dynamic equation of a financial institution choosing strict supervision and the probability of a financial institution choosing strict supervision.

$$F(z) = \frac{dz}{dt} = z(1-z)(\theta_3xyB - C_3), \quad (\text{A28})$$

$$U'_3 = 1 + \frac{C_3}{\theta_3B} \ln \frac{C_3}{\theta_3B} \quad (\text{A29})$$

According to (A29), the following formula can be obtained:

$$\frac{\partial U'_3}{\partial C_3} < 0, \frac{\partial U'_3}{\partial B} > 0. \quad (\text{A30})$$

It can be seen from (A30) that the probability of a financial institution choosing strict supervision is inversely proportional to the cost of supervision and is directly proportional to the value of the synergy payoff  $B$ . This conclusion is consistent with the conclusion of Proposition 3.

The research conclusions of the two-party game and the three-party game are the same because SMEs are dependent on the core enterprises to carry out production and sales activities. SMEs lack independence and need more help from the government and core enterprises.

## References

1. Forth, J.; Bewley, H.; Bryson, A. *Small and Medium-Sized Enterprises*; Department of Trade and Industry: London, UK, 2006.
2. Abdulsaleh, A.M.; Worthington, A.C. Small and medium-sized enterprises financing: A review of literature. *Int. J. Bus. Manag.* **2013**, *8*, 36. [[CrossRef](#)]
3. Acemoglu, D.; Makhdoumi, A.; Malekian, A.; Ozdaglar, A. Too much data: Prices and inefficiencies in data markets. *Am. Econ. J. Microecon.* **2022**, *14*, 218–256. [[CrossRef](#)]
4. Li, Z.; Liang, F.; Hu, H. Blockchain-based and value-driven enterprise data governance: A collaborative framework. *Sustainability* **2023**, *15*, 8578. [[CrossRef](#)]
5. Marsal-Llacuna, M.L. Future living framework: Is blockchain the next enabling network? *Technol. Forecast. Soc. Chang.* **2018**, *128*, 226–234. [[CrossRef](#)]
6. Zhou, H.; Benton, W.C., Jr. Supply chain practice and information sharing. *J. Oper. Manag.* **2007**, *25*, 1348–1365. [[CrossRef](#)]
7. Hofman, W.J. Data sharing requirements of supply-And logistics innovations-Towards a maturity model. In Proceedings of the International Conference on Information Systems, Logistics and Supply Chain, Bordeaux, France, 1–4 June 2016.
8. Lee, H.L.; Padmanabhan, V.; Whang, S. Information distortion in a supply chain: The bullwhip effect. *Manag. Sci.* **1997**, *43*, 546–558. [[CrossRef](#)]
9. Lee, H.L.; Padmanabhan, V.; Whang, S. The bullwhip effect in supply chains. *Sloan Manag. Rev.* **1997**, *38*, 93–102. [[CrossRef](#)]
10. Cachon, G.P.; Fisher, M. Supply chain inventory management and the value of shared information. *Manag. Sci.* **2000**, *46*, 1032–1048. [[CrossRef](#)]
11. Schloetzer, J.D. Process integration and information sharing in supply chains. *Account. Rev.* **2012**, *87*, 1005–1032. [[CrossRef](#)]
12. Sarfaraz, A.; Chakraborty, R.K.; Essam, D.L. The implications of blockchain-coordinated information sharing within a supply chain: A simulation study. *Blockchain Res. Appl.* **2023**, *4*, 100–110. [[CrossRef](#)]
13. Behnke, K.; Janssen, M. Boundary conditions for traceability in food supply chains using blockchain technology. *Int. J. Inf. Manag.* **2020**, *52*, 101–112. [[CrossRef](#)]
14. Hughes, L.; Dwivedi, Y.K.; Misra, S.K.; Rana, N.P.; Raghavan, V.; Akella, V. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *Int. J. Inf. Manag.* **2019**, *49*, 114–129. [[CrossRef](#)]



15. Hayrutdinov, S.; Saeed, M.S.R.; Rajapov, A. Coordination of supply chain under blockchain system-based product lifecycle information sharing effort. *J. Adv. Transp.* **2020**, *2020*, 1–10. [[CrossRef](#)]
16. Seidmann, A.; Sunda, R. Sharing logistics information across organizations: Technology, competition and contracting. In *Information Technology and Industrial Competitiveness*; Springer: Boston, MA, USA, 1998; pp. 107–136.
17. Heidl, R.A.; Steensma, H.K.; Phelps, C. Divisive faultlines and the unplanned dissolutions of multipartner alliances. *Organ. Sci.* **2014**, *25*, 1351–1371. [[CrossRef](#)]
18. Du, T.C.; Lai, V.S.; Cheung, W.; Cui, X. Willingness to share information in a supply chain: A partnership-data-process perspective. *Inf. Manag.* **2012**, *49*, 89–98. [[CrossRef](#)]
19. Fawcett, S.E.; Waller, M.A. Mitigating the myopia of dominant logics: On differential performance and strategic supply chain research. *J. Bus. Logist.* **2012**, *33*, 173–180. [[CrossRef](#)]
20. Tran, T.H.; Childerhouse, P.; Deakins, E. Supply Chain information sharing: Challenges and risk mitigation strategies. *J. Manuf. Technol. Manag.* **2016**, *27*, 1102–1126. [[CrossRef](#)]
21. Lee, H.L.; So, K.C.; Tang, C.S. The value of information sharing in a two-level supply chain. *Manag. Sci.* **2000**, *46*, 626–643. [[CrossRef](#)]
22. Liang, F.; Yu, W.; An, D.; Yang, Q.; Fu, X.; Zhao, W. A survey on big data market: Pricing, trading and protection. *IEEE Access* **2018**, *6*, 15132–15154. [[CrossRef](#)]
23. Wang, L.; Guo, S. Blockchain based data trust sharing mechanism in the supply chain. In Proceedings of the International Conference on Security with Intelligent Computing and Big-Data Services, Tokyo, Japan, 17 April 2018; Springer: Cham, Switzerland, 2018; pp. 43–53.
24. Hofman, W.J. A methodological approach for development and deployment of data sharing in complex organizational supply and logistics networks with blockchain technology. *IFAC-Pap. OnLine* **2019**, *52*, 55–60. [[CrossRef](#)]
25. Epiphaniou, G.; Pillai, P.; Bottarelli, M.; Al-Khateeb, H.; Hammoudesh, M.; Maple, C. Electronic regulation of data sharing and processing using smart ledger technologies for supply-chain security. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1059–1073. [[CrossRef](#)]
26. Qian, X.; Papadonikolaki, E. Shifting trust in construction supply chains through blockchain technology. *Eng. Constr. Archit. Manag.* **2021**, *28*, 584–602. [[CrossRef](#)]
27. Xu, X.; He, Y. Blockchain application in modern logistics information sharing: A review and case study analysis. *Prod. Plan. Control.* **2022**, *55*, 1–15. [[CrossRef](#)]
28. Rejeb, A.; Keogh, J.G.; Simske, S.J.; Stafford, T.; Treiblmaier, H. Potentials of blockchain technologies for supply chain collaboration: A conceptual framework. *Int. J. Logist. Manag.* **2021**, *32*, 973–994. [[CrossRef](#)]
29. Lee, D.; Lee, S.H.; Masoud, N.; Krishnan, M.S.; Li, V.C. Integrated digital twin and blockchain framework to support accountable information sharing in construction projects. *Autom. Constr.* **2021**, *127*, 103–114. [[CrossRef](#)]
30. Xu, P.; Lee, J.; Barth, J.R.; Richey, R.G. Blockchain as supply chain technology: Considering transparency and security. *Int. J. Phys. Distrib. Logist. Manag.* **2021**, *51*, 305–324. [[CrossRef](#)]
31. Wang, J.; Zhou, Z.; Botterud, A. An evolutionary game approach to analyzing bidding strategies in electricity markets with elastic demand. *Energy* **2011**, *36*, 3459–3467. [[CrossRef](#)]
32. Wang, J.; Peng, X.; Du, Y.; Wang, F. A tripartite evolutionary game research on information sharing of the subjects of agricultural product supply chain with a farmer cooperative as the core enterprise. *Manag. Decis. Econ.* **2022**, *43*, 159–177. [[CrossRef](#)]
33. Apaloo, J.; Brown, J.S.; Vincent, T.L. Evolutionary game theory: ESS, convergence stability, and NIS. *Evol. Ecol. Res.* **2009**, *11*, 489–515.
34. Encarnação, S.; Santos, F.P.; Santos, F.C.; Blass, V.; Pacheco, J.M.; Portugali, J. Paths to the adoption of electric vehicles: An evolutionary game theoretical approach. *Transp. Res. Part B Methodol.* **2018**, *113*, 24–33. [[CrossRef](#)]
35. Abram, W.C.; Noray, K. Political corruption and public activism: An evolutionary game-theoretic analysis. *Dyn. Games Appl.* **2018**, *8*, 1–21. [[CrossRef](#)]
36. Jiang, Z.Z.; He, N.; Qin, X.; Ip, W.H.; Wu, C.H.; Yung, K.L. Evolutionary game analysis and regulatory strategies for online group-buying based on system dynamics. *Co. Inf. Syst.* **2018**, *12*, 695–713. [[CrossRef](#)]
37. Luo, J.; Ma, B.; Zhao, Y.; Chen, T. Evolution model of health food safety risk based on prospect theory. *J. Healthc. Eng.* **2018**, *10*, 1–13. [[CrossRef](#)]
38. Rong, J.; Zhu, L. Cleaner production quality regulation strategy of pharmaceutical with collusive behavior and patient feedback. *Complexity* **2020**, *125*, 1–15. [[CrossRef](#)]
39. Pan, X.; Ma, J.; Wu, C. Decision game of data sharing in supply chain enterprises considering data value over time. *J. Supercomput.* **2020**, *76*, 3659–3672. [[CrossRef](#)]
40. Chen, Y.; Sun, L. Trust strategy simulation of corporation–NPO cross alliance using evolutionary game theory. *Kybernetes* **2017**, *46*, 450–465. [[CrossRef](#)]
41. Cheng, H.; Li, J.; Lu, J.; Lo, S.L.; Xiang, Z. Incentive-Driven Information Sharing in Leasing Based on a Consortium Blockchain and Evolutionary Game. *J. Theor. Appl. Electron. Commer. Res.* **2023**, *18*, 206–236. [[CrossRef](#)]

42. Sun, R.; He, D.; Su, H. Evolutionary game analysis of blockchain technology preventing supply chain financial risks. *J. Theor. Appl. Electron. Commer. Res.* **2021**, *16*, 2824–2842. [[CrossRef](#)]
43. Zhu, Q.; Zong, R.; Xu, M. Three-Party Stochastic Evolutionary Game Analysis of Supply Chain Finance Based on Blockchain Technology. *Sustainability* **2023**, *15*, 3084. [[CrossRef](#)]

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