

RESEARCH ARTICLE

Endogenous Punishment-Driven Distributed Computing Environment for Data Factor Property Right Protection

Chuan Fu^{1,*} and Jian Ye¹¹Institute of Computing Technology, Chinese Academy of Sciences, 100190, Beijing, China*Corresponding author. chuanfu@ict.ac.cn

Received on 21 December 2025; Accepted on 23 September 2026

Abstract

The non-excludability and non-rivalry characteristics of data pose challenges to Coase's property rights theory. Based on Ostrom's Common Pool Resources (CPR) Governance Theory, this study proposes defining the data factor as a six-tuple and designing a computational environment that supports the protection of data factor property rights. This definition integrates the original dataset, transaction entities, commitments, supervision, and punishment into a unified whole, specifically referred to as data factor. Similar to the intellectual property protection system, the six-tuple first endows data factors with excludability in a contractual sense. Secondly, to effectively support such exclusivity, this study proposes a distributed property rights protection computing environment with the capabilities of "supervision-punishment-commitment", adopting the "terminal-pipe-cloud" architectural template. This computing environment better matches the self-organizing nature of data trading activities. We use evolutionary game theory to verify how the new data factor definition promotes the development of trading markets. To provide practical reference, the simulation focuses on two key aspects: market stability under the coexistence of multiple strategies, and the impact of the initial conditions of the institutional environment on participants' strategy choices.

Key words: Data Factor Property Rights Protection, Common Pool Resources Governance, Evolutionary Game, Endogenous Punishment, Network Address Translation(NAT)

1. Introduction

The wealth value of data does not depend on "how much" data one possesses, but on "how to utilize" it. However, the non-excludability and non-rivalry of data[1],[2] pose challenges to the property rights theory advocated by Coase. For instance, how to address the issue that an additional copy halves the data's price, and how to ensure that data is reliable, trustworthy, and usable. The property rights economic theory, which is based on the excludability and rivalry of factors, holds that clear property rights constitute the core prerequisite for ensuring market collaboration and orderly transactions[3]. The ongoing debate over the property rights of data factors precisely indicates that data has not yet fully shed its "pure resource" attribute.

Unlike general factors of production, whose excludability enables owners to sustain prices through use control, data factors are non-excludable. Anyone who gains access can replicate them at zero cost. This drives supply to infinity, prices toward zero, and ultimately severs the link between price and the intrinsic value of the data.

Data open-sourcing is a typical approach to demonstrating the value of data factors and exploring avenues for multi-party collaboration. Among its key components, open-source test datasets[4] serve as critical benchmarks for algorithm validation and model training, furnishing a unified evaluation baseline for technological iteration across diverse domains including artificial intelligence and computer vision[5]. To ensure stable and sustainable supply capacity, we need to prioritize the development dilemmas of open-source datasets[6] as well as the potential incentive mechanisms for them. The Sponsors program rolled out by GitHub, a world-renowned open-source platform, offers valuable implications for the development of the open-source ecosystem. Relevant study[7] have demonstrated that even when a large number of developers do not receive direct sponsorship after joining the program, their enthusiasm for engaging in contributory activities such as code optimization and vulnerability remediation is significantly boosted—and this constitutes the core foundation for them to build reputation and garner trust within the open-source community.

Exploring and refining incentive mechanisms for open data sharing not only serves to fully mobilize the enthusiasm of data contributors, but also accelerates the transformation of data from a general-purpose resource into an economically valuable production factor. In the context of data factors, we argue that—much like peer-to-peer (P2P)[8] systems—distributed environments not only offer the dual advantages of minimizing operational costs and streamlining data access, management, and maintenance for providers, but also, by supporting necessary game-theoretic behaviors, can endow data factors with the core attributes of exclusivity and competitiveness, thereby building a robust computing environment that underpins the protection of data factor property rights.

Elinor Ostrom, the 2009 Nobel laureate in Economics, probed into that whether a common resource (such as a pond) can possess “excludability” depends not only on its inherent natural attributes but also on the costs incurred by the appropriator(s) in attempting to prevent others from using it[9],[10]. To align the computing environment for data factor property rights protection with the requirements of Ostrom’s theory of common-pool resource governance, this study defines data factors in the form of a six-tuple denoted as $\langle P, Q, D, C, \text{punish}, \text{supervisor} \rangle$. Among them: P and Q represent the objectified descriptions of transaction entities; D denotes the transaction data; C stands for the contract signed by P and Q regarding D , which is also an objectified description before the entities of P and Q are determined; “punish” refers to the endogenous punishment or sanction function between entities (This punishment does not require third-party consent or implementation); “supervise” represents the supervision function between entities.

This 6-tuple indicates that when any party involved in the transaction detects a violation related to D , the transaction entities (i.e., P or Q) may impose punishment on the violator in accordance with C , and such punishment or sanctions occur directly between P and Q . The form of the 6-tuple clearly shows that the punitive operations connoted in data factors are intended to protect the interests of specific groups, namely second-tier excludability[10].

Private goods achieve “excludability” in the first-tier sense, whereas club goods and common-pool resources achieve “exclusivity” in the second-tier sense.[10]. Second-tier excludability refers to exclusivity that is realized within a certain scope and based on specific rules or conditions. From the perspective of excludability, the expectation of endogenous punishment can motivate entities involved in sharing to proactively avoid risks and reduce the possibility of data dissemination—similar to how patents are brought under legal protection. On the other hand, the convenience of imposing punishments during transactions destabilizes illegal trading markets[11], which can minimize the number of participants to the greatest extent.

Through the collaboration of “punish” and “supervise”, a mechanism is provided for groups that have already secured access to shared data factors, enabling them to prevent others from using the factors at low cost. The computational environment defined by this six-tuple supports the protection of data factor property rights and is better aligned with the self-organizing nature of data trading activities.

Based on the six-tuple of data factors, this study proposes a distributed property rights protection computing environment that can supervise data factor transaction behaviors, enhance the cooperation level of the transaction market, and features automatic data leakage detection and autonomous contract

breach penalty imposition. The main innovations are as follows:

1. General factors of production possess the attribute of excludability, which enables them to unify both value and price within a single transaction framework. Data factors, however, lack this attribute, causing their price to be gradually eroded during the process of value realization. Addressing the non-excludability characteristic of data—and shifting the analytical object accordingly—we propose a framework that bridges economic theory with technical implementation. By leveraging the incentives embedded in the technical implementation to influence transaction entities, the framework achieves the governance effects prescribed by economic theory, thereby resolving the fundamental contradiction inherent in treating data as a tradable factor. Resolving the non-excludability problem would facilitate the widespread development of data transactions.
2. Based on the CPR Governance Theory, this study proposes a six-tuple framework for describing data factors. Relying on the endogenous punishment mechanisms and customized contracts within the six-tuple, it realizes the excludability(second-tier excludability) and rivalry required for factors, thereby providing support for clarifying the boundaries of property rights.
3. According to the six-tuple of data factors, this study proposes a distributed data factor transaction and supervision system composed of “cloud”, “pipe”, and “terminal”. Specifically: the blockchain serves as the “cloud” to record transaction contracts; a virtual machine-based sandbox is used as the execution environment for data users, allowing data owners to monitor whether the execution process of training programs complies with specifications through the sandbox; by referring to telephone call blocking and utilizing signaling technology[12], we have realized the capability to autonomously punish untrustworthy entities (in a NAT (Network Address Translation) network environment) by blocking and restricting data transmission paths.
Blocking access paths[13],[14] and isolating violators from business cooperative relationships[15],[16] not only reduce their actual operational capabilities but also harm their business reputation through the industry credit transmission mechanism.
4. To verify the role of autonomous punishment in improving the cooperation level of the data transaction market, this study models the autonomous punishment behavior of traders using game theory, based on the prisoner’s dilemma principle. On this basis, we simulate four transaction strategy combinations using the Moran process. The simulation results show that under the constraint of the autonomous punishment mechanism, the probability of individuals choosing the cooperative strategy is much higher than that of choosing other strategies, and the group can benefit from cooperation more quickly. Such simulations can also help policymakers understand the role and value of each external condition in designing the initial system of the trading market.

In terms of the service goal, this system is designed around the theme that data trading requires promoting cooperation among subjects, controlling the dissemination of data among subjects, and supporting subjects in autonomously punishing

each other within a specific relationship, which is essentially different from systems that encourage information sharing. To the best of our knowledge, this is the first paper to define data factors through an extension based on datasets; it is also the first paper to discuss how to construct the excludability attribute of data factors from the perspective of punishment; and it provides, in conjunction with the definition of data factors, the implementation principles of a computing environment that specifically supports factor transactions.

The remainder of this article is structured as follows: First, it introduces the current contradictions in data factor tradings, proposes an extended approach to defining data factors, and briefly describes the innovations of this paper. Second, it introduces the CPR Governance Theory, and based on the six-tuple of data factors, proposes a computing environment supporting the trading market and its implementation mechanism. Third, drawing on simulations of four transaction strategy combinations, it uses evolutionary game theory to explain the important role of the mutual restriction mechanism (supporting autonomous punishment) in enhancing governance capabilities, maintaining the market's cooperation level, and maximizing cooperative benefits. Fourth, it reviews the current research status of data factors and discusses the property rights dilemmas of various schemes. Finally, it presents the conclusions and future work.

2. Data Factor and Property Rights Protection Computing Environment

2.1. Theoretical Basis for Data factor Definition

Ostrom's[9] research focuses on the governance of public goods (e.g., forests, pastures, roads, parking lots)—which also possess non-rivalry and non-excludability. She found that when tackling issues such as free-riding, shirking of responsibilities, and opportunistic behaviors, integrating mechanisms including community rules, supervision, and hierarchical governance can resolve the collective action dilemma, enable effective resource allocation, and achieve economic goals. The development of data factor trading markets also faces collective action dilemmas arising from opportunistic behaviors. Beyond government regulation and privatization models, Ostrom's theory offers a new perspective for defining data factors and constructing relevant trading systems.

Different from property rights economic theory, the governance of common pool resources (CPR)[9] is based on the clear definition of boundaries. The core purpose of clearly defining boundaries is to clarify responsibilities, as well as to fulfill obligations and obtain returns in accordance with these responsibilities. In practice, clearly defining boundaries means that each participant makes explicit commitments to themselves and others. Such commitments do not stem from external imposition but must be self-implemented by the involved parties. The governance solution proposed by Ostrom aims to enable interdependent principals to organize themselves autonomously and achieve sustained collective benefits—even when faced with temptations such as free-riding.

Ostrom argued that commitments and supervision must be strategically nested: effective supervision cannot be achieved solely by relying on external forces; only by integrating supervision and hierarchical sanctions into a complete set of institutional principles and operating them in coordination can strong public institutions be established or reshaped. Supervision is crucial, yet third-party supervision is not the

only approach. When individuals commit to a contingency strategy for abiding by rules—i.e., "I act as others act"—they will be motivated to supervise others to ensure that most people comply with the rules. We argue that supervision and sanctions (i.e., punishment) together constitute effective oversight.

Based on the CPR Governance Theory, this study defines data factors using a six-tuple framework: $\langle P, Q, D, C, \text{punish}, \text{supervise} \rangle$, which essentially serves to define boundaries. The components are defined as follows:

- **P and Q:** Objectified descriptions of transaction entities, i.e., abstract descriptions of the entities' characteristics. All entities that meet the requirements are potential counterparts to these entities (for convenience, P refers to the data owner, and Q refers to the data user).
- **D:** Denotes the transaction data.
- **C:** Represents the contract (i.e., commitment) signed by P and Q regarding D. Before the entities of P and Q are determined, this contract also functions as an objectified description.
- **punish (C, punisher, defaulter):** Represents the punishment or sanction function between entities. The return value of this function is either 0 or 1, where 0 indicates no punishment and 1 indicates the imposition of punishment. The specific form of punishment or sanction shall be determined in accordance with Contract C.
- **supervise (D, C, proctor):** Refers to the inter-entity supervision function. The return value of this function is either 0 or 1, where 0 indicates compliance with relevant agreements and 1 indicates a violation of such agreements. The specific supervision actions and rules are determined in accordance with Data D and Contract C.

This six-tuple implies that when any party involved in the transaction detects a violation related to D, the transaction entity (either P or Q) can impose punishment on the violator in accordance with C, and the punishment or sanction occurs directly between P and Q. The values of "punisher", "defaulter", and "proctor" correspond to the entities represented by P or Q.

When understanding the definition of data factors from the perspective of excludability in property rights economic theory, the expectation of endogenous punishment can motivate entities to proactively avoid risks and abandon the use of relevant datasets. Endogenous punishment first directly leads to losses in expected benefits and prior costs; second, it indirectly affects the entity's business reputation and other ongoing transactions involving the entity. When the total cost of infringement exceeds the benefits of infringement, punishment measures achieve excludability by increasing various costs[17]. Data factors described by the six-tuple can exhibit the excludability required of production factors. On the other hand, the convenience of imposing punishments during transactions destabilizes illegal trading markets[11], which can minimize the number of participants to the greatest extent.

When the dataset is determined, the expression $\langle P, Q, D, C(\emptyset), \text{punish}, \text{supervise} \rangle$ represents the basic data factor released by the data owner. The customized contracts signed by different entities, along with the connections between contracts formed around the same dataset, collectively endow the six-tuple-described data factors with the characteristic of rivalry. Based on the CPR Governance Theory, the six-tuple data factors defined in this study can externally exhibit the characteristics of production factors that are adapted to market transactions.

2.2. Property Rights Protection Computing Environment

To support the trading of six-tuple data factors, this study proposes a distributed property rights protection computing environment for data factor trading, which consists of "cloud", "pipe", and "terminal".

2.2.1. System Structure of the Computing Environment

The six-tuple-based computing environment consists of three components: "cloud", "pipe", and "terminal", as illustrated in Figure 1.

- **Cloud:** The blockchain serves as the "cloud" to record transaction contracts (i.e., C in the six-tuple), which represent commitments.
- **Pipe:** By referring to telephone call blocking and utilizing signaling technology[12], we have realized the capability to independently punish untrustworthy entities (i.e., "punish" in the six-tuple) in a NAT (Network Address Translation) network environment by blocking and restricting data transmission paths.
- **Terminal:** This component is divided into two categories:
 - Terminal systems for data usage (i.e., Q in the six-tuple) are virtual machine-based sandboxes serving as execution environments for data users. Data owners monitor whether the execution process of training programs complies with specifications through the sandbox (i.e., "supervise" in the six-tuple).
 - Terminal systems for data owners (i.e., P in the six-tuple) provide data access environments for data owners and collect information about data users' training data usage.

Both types of terminals access the internet through NAT devices, with data transmission paths between NAT devices established using the SIP protocol.

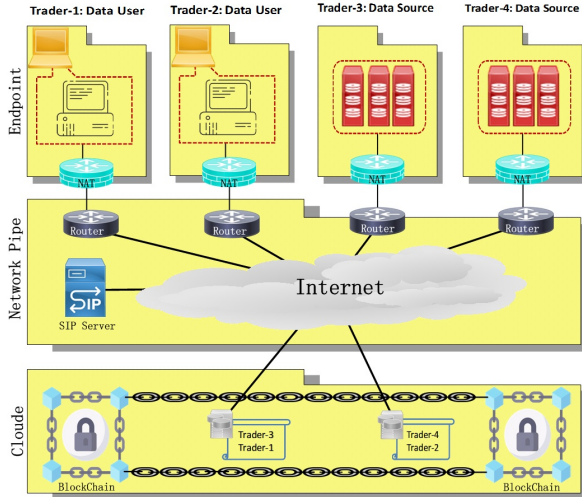


Fig. 1. A computing environment supporting property rights protection.

2.2.2. Commitment and Monitoring

A distributed file system similar to IPFS is used to store contract texts[18],[19]. When a contract text is uploaded, it is

first hashed, and the resulting file hash value is then uploaded to the blockchain for storage. The integration of distributed storage and blockchain technology ensures the tamper-proof nature of the commitments recorded in the contract, providing traceable and reliable guarantees for enforcing punishment in the event of infringement.

The sandbox of the first type of terminal system (for data usage) is capable of tracking the information flow during the training process and restricting the scope of information diffusion. This type of terminal system downloads data from the second type of terminal system (for data owners) and stores the data in a virtual space. Drawing on the privacy-preserving data protection methods for Android systems proposed in References[20],[21],[22], we adopt data contamination marking and attribute-based access control as the core mechanisms for sandbox monitoring of data leakage. These mechanisms can track the original data and the model parameters derived from the original data, and restrict their diffusion scope.

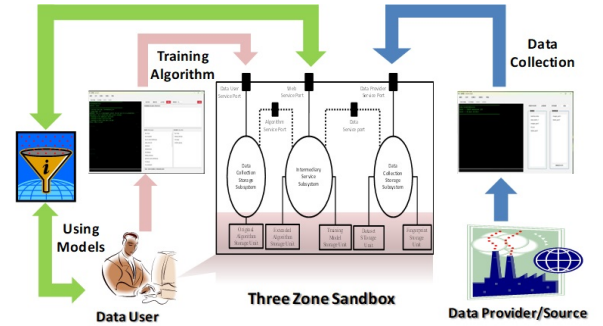


Fig. 2. Three-space sandbox and its interaction process.

Based on the confidentiality and integrity requirements of the security access mode[23], we partition the continuous model training environment into three mutually independent subspaces(zone): the data provider subspace, the data user subspace, and the intermediary service subspace—forming the "three-space sandbox", as illustrated in Figure 2. The data provider subspace stores datasets, the data user subspace stores model training and provides services to the outside.

The access relationships among the three subspaces are determined based on the dataset. The dataset is confirmed as complete by both parties prior to the transaction, and this integrity serves as the foundation for subsequent cooperation. Based on confidentiality requirements, the original data has a higher protection level than the algorithm code; therefore, the data provider subspace is assigned a higher level than the data user subspace. The intermediary service subspace, which performs auditing, has the highest level of privilege.

AI model training follows a fixed data flow: sample reading, preprocessing (normalization/tensor conversion), forward propagation, loss computation, and backpropagation. The training programs provided by data users typically rely on existing third-party libraries. We decompose this workflow across the three subspaces and insert checkpoints at key stages. When the data provider uploads data, the data provider subspace generates a sample fingerprint for each record in the original dataset and stores these fingerprints in a fingerprint table[24]. Upon receiving the algorithm code submitted by the data user, the intermediary service subspace scans the

code using syntactic analysis tools and inserts integrity-checking code before the preprocessing (normalization/tensor conversion) stage. During execution, the integrity-checking code computes the fingerprint of the sample being processed and compares it against the fingerprint table. If no matching record is found, the checking code triggers an alarm. The relative privilege levels among the subspaces ensure that the data user cannot detect the intermediary service's inspection of the algorithm code.

To broaden the coverage of parties participating in data trading, the core purpose of the sandbox is supervision, not absolute protection, and it is designed to simulate the canary in a coal mine. In normal operation, the sandbox achieves mutual isolation between different subjects, as well as mutual isolation between data and the original execution program. When a violation occurs, the data integrity and confidentiality defined by the sandbox will be breached, thereby triggering an alarm to the data provider. This will lead the data provider to initiate punishment. Once a violation is detected, the deterrence comes from the endogenous punishment mechanism—the blocking of signaling and data paths—rather than from the sandbox itself.

2.2.3. Network Environment Supporting Endogenous Punishment

Endogenous punishment serves as the foundation for data factors to possess excludability. Existing studies have applied the PageRank algorithm[15],[16] to evaluate the reputation of nodes in supply networks—nodes in an isolated state within the network fail to obtain favorable evaluations. Therefore, we consider restricting the punished entity's access to the network as a punishment measure[13],[14]. When the data transmission path is blocked, this is equivalent to isolating the defaulter from business cooperative relationships, which directly diminishes their operational capacity and business reputation.

Telecom network operators can compel users with unpaid fees to settle their payments promptly by blocking their calls. As illustrated in Figure 3, based on the SIP protocol and NAT devices, we propose a network environment that not only supports data exchange between transacting parties but also enables the autonomous implementation of punishment. Using NAT (Network Address Translation) devices to provide internet access services to users is a common solution for addressing IP address shortages, and the NAT network environment lays the foundation for us to implement punishment. When a transaction entity accesses the public network via a NAT device using a private address, it requires the assistance of a third-party service deployed on the public network (i.e., a transaction matcher) to communicate with another transaction entity located behind a NAT device. The technical solution for establishing data transmission channels between NAT devices based on the SIP (Session Initiation Protocol) has been widely adopted in the internet. Once the tunnel is established, the two parties can perform data transmission and status synchronization.

As illustrated in Figure 4, when services are provided to transaction entities based on the SIP protocol, the transaction matcher controls the mutual access capabilities of all entities. In the aforementioned network environment, taking the scenario where the first type of terminal detects abnormal behavior as an example, the punishment implementation process is as follows:

1. In accordance with the punishment clauses specified in the contract between the two transaction parties,

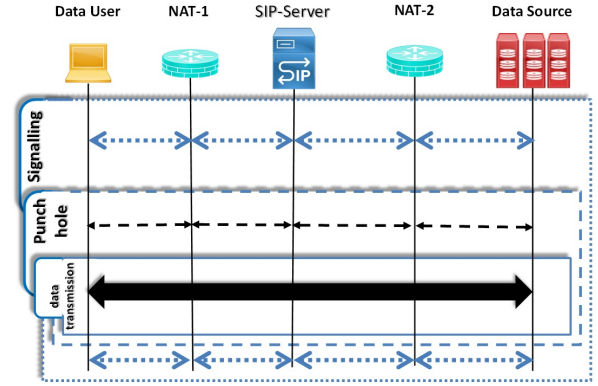


Fig. 3. Process of Establishing Data Paths Between NAT Devices

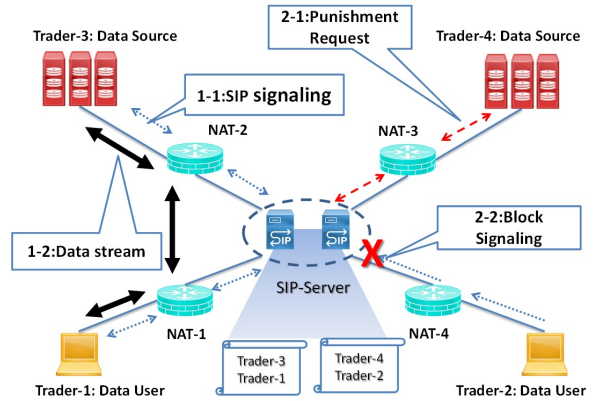


Fig. 4. Process of Implementing Punishment

the transaction matcher can configure an automatic punishment implementation service for the transaction entities.

2. When an entity submits a punishment request, the automatic punishment implementation service is triggered to restrict or block the punished entity from establishing data transmission paths with other entities. The punished entity may also file a reverse punishment request against the initiator of the original punishment request. The transaction matcher will similarly restrict the punishment initiator in accordance with the provisions of the punishment clauses. At this point, the ability of both parties to access other entities in the system will be frozen until the dispute is resolved.
3. During the freezing period, the two parties negotiate to reach a resolution—similar to how PPP (Public-Private-Partnership) models[25] adjust project outputs, modify cost-sharing ratios, or even terminate cooperation through negotiation.
4. After the two transaction parties resolve the dispute, the initiator of the original punishment request submits a revocation request. The transaction matcher then automatically restores both parties' ability to access other entities in the network.

Under normal circumstances, a trader will not initiate a punishment request without cause. From a game-theoretic perspective, this is a lose-lose state and attracts attention from multiple parties. However, it cannot be ruled out that someone

may raise a false alarm or deliberately initiate punishment. Therefore, before implementation, it is necessary to confirm that the sandbox alarm actually occurred. SIP is a protocol with rich tags and complete call-sequence records. Because systems behind different NAT devices need to communicate via the SIP protocol, and SIP has the capability to record sessions in the call server, when a subject submits a punishment request, the call service will check its local records to determine whether the cooperative session exists—that is, whether the alarm message was actually issued by the sandbox. In future work, we will treat security issues in data trading as an independent research problem, and analyze and study security threats from multiple aspects, ranging from system-level attacks to transaction-level attacks.

3. From Endogenous Punishment to Cooperation

To analyze the role of punishment-based restraint mechanisms in enhancing entities' willingness to cooperate, we categorize the strategies available to entities participating in data transactions into four basic types: cooperation, defection, loner, and punishment. In each round of the game, transaction entities can independently choose a strategy based on their own objectives.

- **Cooperation Strategy:** Refers to a strategy where an entity is willing to invest resources (i.e., incur costs) in cooperation and share the resulting benefits.
- **Defection Strategy:** Refers to a strategy where an entity refuses to invest resources (i.e., avoids incurring costs) in cooperation but still seeks to share the benefits.
- **Punishment Strategy:** Refers to a strategy where an entity is willing to invest resources (i.e., incur costs) in cooperation, share the resulting benefits, and proactively punish defectors upon detecting defection—while also bearing the costs associated with the punishment itself.
- **Loner Strategy:** Refers to a strategy where an entity generates value independently using its data, without engaging in cooperation with other entities.

Based on the above strategies, we define four strategy combinations: Cooperation-Defection, Cooperation-Defection-Loner, Cooperation-Defection-Punishment, and Cooperation-Defection-Loner-Punishment. Using the social prisoner's dilemma model as a foundation, we discuss the cooperation tendencies of entities under various combinations by analyzing the fixation probability in evolutionary games. The so-called fixation probability refers to the probability that a strategy spreads from a single mutant individual within a population to eventually dominate the entire population[26],[27].

3.1. Profit Analysis of Transaction Strategies in the Game

In the data transaction market, some entities are responsible for data collection, while others are tasked with data processing. The benefits generated from data are the result of collective efforts. Prior to cooperation, participants cannot observe the strategies adopted by other entities in the market. For the sake of simplicity, we assume that cooperative benefits are evenly distributed among all entities involved in the cooperation.

With reference to Hauert[28], we assume there are M entities participating in data factor tradings in the market, including

X cooperators, Y defectors, Z loners, and W punishers (where $X + Y + Z + W = M$). From a population of M entities, N entities are randomly selected to form a game group for project implementation. δ represents the profit of loners. c represents the cost incurred by cooperators (or punishers). The value created through cooperation is r times the cost c (i.e., r denotes the rate of return). δ provides a reference baseline for cooperative benefits—specifically, it represents the market value that an entity can generate by using a given dataset independently without engaging in cooperation. The value of δ may increase with network effects and decrease accordingly.

β denotes the punishment intensity coefficient with which punishers sanction defectors, or equivalently, the punishment intensity perceived by defectors. $\alpha\beta$ denotes the punishment coefficient with which punishers sanction entities that refuse to participate in punishing defectors, or equivalently, the punishment intensity perceived by those non-participating entities. When terminals communicate via SIP signaling, the call server that provides the service typically also offers a presence service. When a punisher initiates a punishment request, the call server blocks all outgoing connection requests from the punished party, and the punished party's login status is simultaneously set to "dispute frozen." Non-participating entities can query this presence service to obtain the current status of other nodes (e.g., online, dispute frozen, etc.). γ and $\alpha\gamma$ represent the costs borne by punishers for the two aforementioned punishment behaviors, respectively. We assume $N > r > (1 + \delta/c)$ and $\beta > \gamma, 1 > \alpha > 0$. Based on the hypergeometric distribution[29],[30], the average profits corresponding to the above strategies are as follows:

$$\begin{aligned} P_x &= \frac{\binom{Z}{N-1}}{\binom{M-1}{N-1}} \delta + B(Z) - F(Z)c - \frac{W}{M-1} (N-1)G(Y)\alpha\beta \\ P_y &= \frac{\binom{Z}{N-1}}{\binom{M-1}{N-1}} \delta + B(Z) - \frac{W}{M-1} (N-1)\beta \\ P_z &= \delta \\ P_w &= \frac{\binom{Z}{N-1}}{\binom{M-1}{N-1}} \delta + B(Z) - F(Z)c - \frac{Y}{M-1} (N-1)\gamma - \frac{X}{M-1} (N-1)G(Y)\alpha\gamma \end{aligned} \quad (1)$$

where,

$$\begin{aligned} B(Z) &= rc \frac{X+W}{M-Z-1} \left(1 - \frac{1}{N(M-Z)} (M - (Z-N+1)) \frac{\binom{Z}{N-1}}{\binom{M-1}{N-1}} \right) \\ F(Z) &= 1 - \frac{r}{N} \frac{M-N}{M-Z-1} + \frac{\binom{Z}{N-1}}{\binom{M-1}{N-1}} \left(\frac{r}{N} \frac{Z+1}{M-Z-1} + \frac{r(M-Z-2)}{M-Z-1} - 1 \right) \\ G(Y) &= 1 - \frac{M-1}{M-Y-1} \frac{\binom{M-Y-1}{N-1}}{\binom{M-1}{N-1}} \end{aligned} \quad (2)$$

Apart from the scale parameters, all game-related parameters in this paper are illustrative parameters that reflect the economic behavioral characteristics of transacting subjects, rather than parameters of the information system.

3.2. Simulation of Game Behavior Among Data Transaction Entities

To secure higher profits, entities will adjust their strategies based on their opponents' strategies, environmental factors,

Table 1. Game Profits of the Four Strategies

	Cooperation(X)	Defection(Y)	Loner(Z)	Punishment(W)
Cooperation(X)	$(r-1)c$	$\frac{rc}{N} \left[1 + \frac{(X-1)(N-1)}{M-1} \right] - c$	$(r-1)c - \frac{\binom{Z}{N-1}}{\binom{Z}{M-1}} [(r-1)c - \delta]$	$(r-1)c$
Defection(Y)	$\frac{rc}{N} \left[\frac{X(N-1)c}{M-1} \right]$	$\frac{\binom{Y}{N-1}}{\binom{Y}{M-1}} \delta$	$\frac{\binom{Z}{N-1}}{\binom{Z}{M-1}} \delta$	$\frac{W}{M-1} (N-1) (\frac{rc}{N} - \beta)$
Loner(Z)	δ	δ	δ	δ
Punishment(W)	$(r-1)c$	$\frac{rc}{N} (1 + \frac{(W-1)(N-1)}{M-1}) - c - \frac{(M-W)(N-1)}{M-1} \gamma$	$(r-1)c - \frac{\binom{Z}{N-1}}{\binom{Z}{M-1}} [(r-1)c - \delta]$	$(r-1)c$

and game outcomes during repeated games. By integrating environmental influences with individual strategies, we use the Moran process to simulate the four strategy combinations. The specific game structure is presented in Table 1.

In the Moran process, the parameter $\omega \in [0, 1]$ —used to calculate fitness[27]—represents the intensity of natural selection. When ω is close to 0, the external environment in which players operate exerts a greater impact on fitness; when ω is close to 1, the interactions between players have a more significant impact on fitness. Fitness reflects the combined effect of dominance and game dynamics.

In accordance with the requirements of the Moran process, after the population is fully mixed, four types of entities—cooperators, defectors, loners, and punishers—engage in random pairwise games (self-gaming is not considered). For example, when a cooperator interacts with a defector, the profit of the cooperator is $\frac{rc}{N} \left[1 + \frac{(X-1)(N-1)}{M-1} \right] - c$, denoted as P_{XY} . The game profits between other types of entities are presented in Table 1.

Let x, y, z , and w represent the counts of the four types of entities participating in the project, where $N = x + y + z + w$. For convenience, we use the 3D array (x, y, z) to denote a combined state of the four types. Based on the definition of the Moran process, the fitness values corresponding to the four types are as follows:

$$\begin{vmatrix} f_{x,y,z} \\ g_{x,y,z} \\ h_{x,y,z} \\ l_{x,y,z} \end{vmatrix} = (1 - \omega) + \frac{\omega}{N-1} \Pi \quad (3)$$

where,

$$\Pi = \begin{vmatrix} (x-1)P_{XX} & (y)P_{XY} & (z)P_{XZ} & (N-x-y-z)P_{XW} \\ (x)P_{YX} & (y-1)P_{YY} & (z)P_{YZ} & (N-x-y-z)P_{YW} \\ (x)P_{ZX} & (y)P_{ZY} & (z-1)P_{ZZ} & (N-x-y-z)P_{ZW} \\ (x)P_{WX} & (y)P_{WY} & (z)P_{WZ} & (N-x-y-z-1)P_{WW} \end{vmatrix} \mathbf{1}_4 \quad (4)$$

Among them, $f_{x,y,z}$, $g_{x,y,z}$, $h_{x,y,z}$, and $l_{x,y,z}$ represent the fitness of cooperators, defectors, loners, and punishers, respectively. Based on the fitness of each type of entity, we can calculate the transition probability between different entity types. It is assumed that when an entity type transition occurs, only one entity type participates in the transition, and only one individual from this type is involved in the transition. The transition probability is calculated as the product of the proportion of the current entity type in the entire population and the proportion of the target entity type in the entire population under fitness weighting. $\frac{yy}{zz} T_{xx}$ represents the probability that no entity type transition occurs. $\frac{yy+1}{zz+1} T_{xx-1}$ represents the probability that one individual from entity type

x transitions to entity type y ; other similar notations follow the same interpretation. The specific calculation method is as follows:

$$\begin{vmatrix} \frac{yy}{zz} T_{xx} \\ \frac{yy+1}{zz+1} T_{xx-1} \\ \frac{yy}{zz+1} T_{xx-1} \\ \frac{yy}{zz} T_{xx-1} \\ \frac{yy-1}{zz} T_{xx+1} \\ \frac{yy-1}{zz+1} T_{xx} \\ \frac{yy-1}{zz} T_{xx} \\ \frac{yy}{zz-1} T_{xx+1} \\ \frac{yy+1}{zz-1} T_{xx} \\ \frac{yy}{zz-1} T_{xx} \\ \frac{yy}{zz} T_{xx+1} \\ \frac{yy+1}{zz} T_{xx} \\ \frac{yy}{zz+1} T_{xx} \end{vmatrix} = \mu \begin{vmatrix} x & y & z & w \\ y & 0 & 0 & 0 \\ z & 0 & 0 & 0 \\ w & 0 & 0 & 0 \\ 0 & x & 0 & 0 \\ 0 & z & 0 & 0 \\ 0 & w & 0 & 0 \\ 0 & 0 & x & 0 \\ 0 & 0 & y & 0 \\ 0 & 0 & w & 0 \\ 0 & 0 & 0 & x \\ 0 & 0 & 0 & y \\ 0 & 0 & 0 & z \end{vmatrix} \begin{vmatrix} xf_{xyz} \\ yg_{xyz} \\ zh_{xyz} \\ wl_{xyz} \end{vmatrix} \quad (5)$$

where,

$$\mu = \frac{1}{(xf_{x,y,z} + yg_{x,y,z} + zh_{x,y,z} + (N-x-y-z)l_{x,y,z})M} \quad (6)$$

Figure 5 illustrates a potential evolutionary outcome under the fourth game scenario. After multiple rounds of games, cooperators and punishers emerge as the dominant groups within the population.

3.3. Analysis of the Evolutionary Tendency of Transaction Entities

An evolutionarily stable strategy (ESS) refers to a strategy adopted by the majority of a population's members. The benefits this strategy confers on entities cannot be matched by any other strategy. In evolutionary games involving randomness in finite populations, fixation probability is a key indicator for analyzing whether a strategy can qualify as an evolutionarily stable strategy.

To calculate the fixation probability in multi-strategy games, we treat the transition matrix as a process that describes strategy transformation when an independent strategy competes against a set of other strategies. All strategies except the independent one form a "super strategy." We use the calculation method proposed in[27] to compute the fixation probability of this independent strategy. When calculating the fixation probability of other strategies, we sequentially adjust the independent strategy and its corresponding super strategy. When the individual state of the

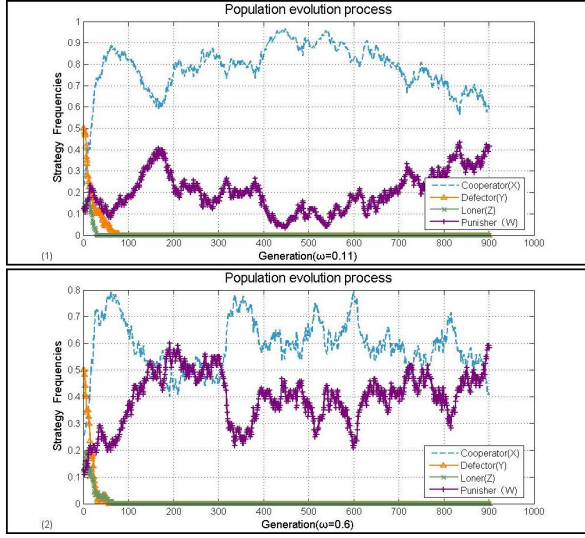


Fig. 5. Population evolution process

independent strategy is 1, it corresponds to multiple individual states of the super strategy; in such cases, we calculate the fixation probability of the independent strategy by taking the average value.

Below, we analyze the cooperation tendencies of entities across the four strategy combinations, based on the relationship between the rate of return r and fixation probability. Figure 6 illustrates the changes in fixation probability for the four combinations when the profit of loners is 0.2. Figure 7 illustrates the changes in fixation probability for the four combinations when the profit of loners is 0.5. Figure 8 illustrates the changes in fixation probability for the four combinations when the profit of loners is 1. The profit of loners serves as the baseline return that individuals in the population can obtain through independent efforts.

The gray plane in each figure represents the reference probability. For example, in the "Cooperator-Defector-Loner-Punisher" scenario, the probability of participants choosing each strategy is 0.25. We consider that when the fixation probability of a particular strategy exceeds the reference plane, this strategy exhibits a selection bias within the population. When all strategies fall below the reference plane, the population has no distinct preferred strategy, and individuals tend to adopt the strategy with a relatively higher fixation probability. The parameters used in the simulations, such as population size, punishment cost, and punishment intensity, are based on references[31][32][33]

Figure 6 to Figure 9 indicate that when individuals select a game strategy, they must comprehensively consider, at minimum, factors such as the return from cooperation, the intensity of natural selection (ω), the profit of loners (δ), and the punishment intensity exerted by punishers.

Figure 6 to Figure 8 demonstrate that, with cooperative profits held constant: as the intensity of external environmental selection (ω) increases, the fixation probability of cooperators rises significantly, while that of defectors decreases significantly; with the intensity of external environmental selection (ω) held constant, as the rate of return (r) increases, the fixation probability of cooperators rises significantly, while that of defectors decreases significantly; when the fixation probability

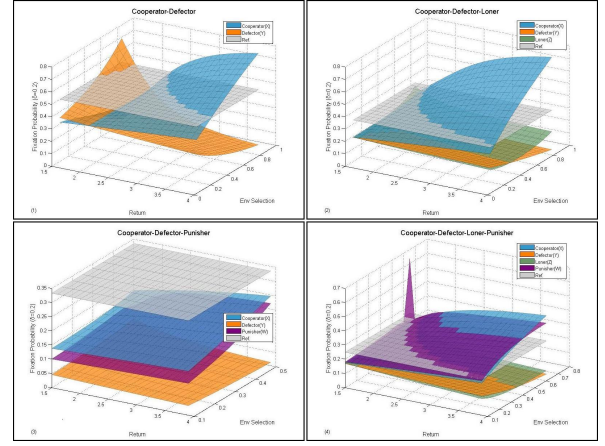


Fig. 6. Fixation Probability ($\delta = 0.2$). $M = 120$ $N = 6$ $c = 1$ $1.5 < r < 3.9$ $0.1 < \omega < 0.85$ $\alpha = 0.1$ $\beta = 1.1$ $\gamma = 0.3$ (1) $X = 60$ $Y = 60$ (2) $X = 40$ $Y = 40$ $Z = 40$ (3) $X = 40$ $Y = 40$ $W = 40$ $0.1 < \omega < 0.5$ (4) $X = 30$ $Y = 30$ $Z = 30$ $W = 30$ $0.1 < \omega < 0.65$

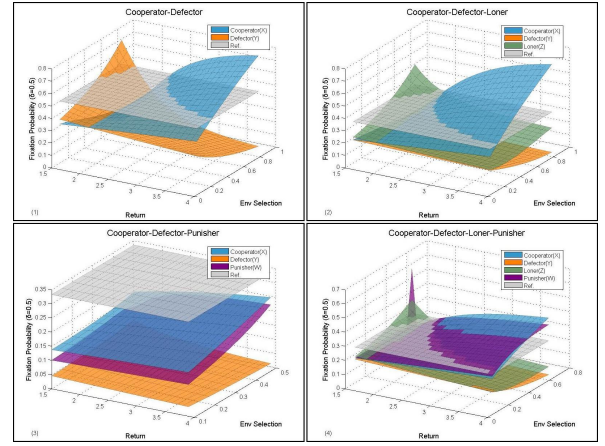


Fig. 7. Fixation Probability ($\delta = 0.5$). $M = 120$ $N = 6$ $c = 1$ $1.5 < r < 3.9$ $0.1 < \omega < 0.85$ $\alpha = 0.1$ $\beta = 1$ $\gamma = 0.3$ (1) $X = 60$ $Y = 60$ (2) $X = 40$ $Y = 40$ $Z = 40$ (3) $X = 40$ $Y = 40$ $W = 40$ $0.1 < \omega < 0.5$ (4) $X = 30$ $Y = 30$ $Z = 30$ $W = 30$ $0.1 < \omega < 0.65$

is lower than the reference probability, it indicates high uncertainty in the strategy selected by individuals.

By comparing (1), (2), and (3) in Figure 6: the presence of loners and punishers leads to a rapid downward trend in the fixation probability of defectors; a comparison between (2) and (3) shows that punishers can more effectively suppress individuals' defection behavior in the environment, however, under the same profit conditions, punishers also inhibit individuals' cooperative behavior; additionally, in the "Cooperator-Defector-Punisher" combination, when the intensity of external environmental selection (ω) is relatively high, punishers will penalize all participants, resulting in abnormal market operation.

A comparison between (2) and (4) shows that when the investment return (r) has increased significantly, the fixation probability of loners in the "Cooperator-Defector-Loner" combination remains relatively high—meaning there is a high probability that individuals will not engage in data transactions with one another; the trend in (4) indicates that, in the fourth strategy combination, the fixation probabilities

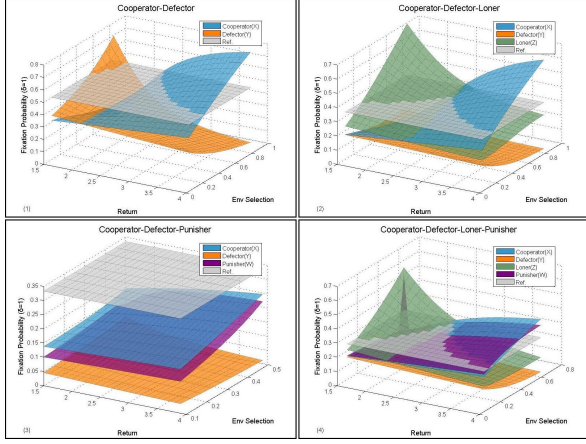


Fig. 8. Fixation Probability ($\delta = 1$) $M = 120$ $N = 6$ $c = 1$ $1.5 \leq r \leq 3.9$ $0.1 \leq \omega < 0.85$ $\alpha = 0.1$ $\beta = 1.1$ $\gamma = 0.3$ (1) $X = 60$ $Y = 60$ (2) $X = 40$ $Y = 40$ $Z = 40$ (3) $X = 40$ $Y = 40$ $W = 40$ $0.1 \leq \omega < 0.5$ (4) $X = 30$ $Y = 30$ $Z = 30$ $W = 30$ $0.1 \leq \omega < 0.65$

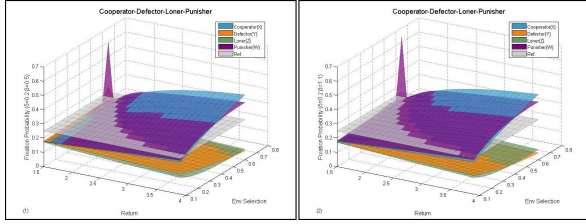


Fig. 9. Fixation Probability ($\delta = 0.2$) $M = 120$ $N = 6$ $X = 30$ $Y = 30$ $Z = 30$ $W = 30$ $0.1 \leq \omega < 0.65$ $c = 1$ $1.5 \leq r \leq 3.9$ $\alpha = 0.1$ $\gamma = 0.3$ $0.1 \leq \omega < 0.85$ $\alpha = 0.1$ $\gamma = 0.3$ (1) $\beta = 0.5$ (2) $\beta = 1.1$

of loners and defectors are significantly lower than those in (2); since punishers are a special type of cooperator, the fixation probability of the population's tendency to cooperate is significantly higher than that in (2); when the fixation probability of cooperators exceeds the reference plane, the rate of return in (4) is lower than that in (2), yet the population can obtain returns through cooperation earlier; both Figure 7 and Figure 8 exhibit this upward trend.

By comparing the fourth strategy combination across Figure 6 to Figure 8, we observe that as the profit of loners (δ) gradually increases, more efficient individual productivity delays group cooperation. Figure 9 illustrates that increasing punishment intensity can effectively suppress the tendency to defect and accelerate the fixation probability of the cooperative tendency to exceed the reference plane.

The above simulation results demonstrate that the incentive mechanism embedded in the technical scheme combining the SIP protocol with the NAT network can achieve the governance effect proposed by Common Pool Resources governance theory—namely, that the majority of individuals in the population adopt cooperative strategies. This study provides a technology-supported institutional system for non-excludable data factors. Only on the basis of traders' stable cooperation can the value of data factors—such as non-rivalry and zero replication cost—be realized.

4. Related Research

We believe that current research on data (factor) transactions can be categorized into three perspectives: value chain research centered on datasets, research on data transaction market construction schemes, and research on governance methods for data factor transaction markets. These studies reflect the process by which data evolves from specific datasets to an abstract concept.

The data value chain originated from enterprises' needs for massive data management[34] and has received widespread attention with the development of big data technologies[35]. In industry-specific research—such as in supply chains[36], finance[37], agriculture[38], and healthcare[39]—people have further recognized the new value that the data value chain brings to industries.

When data transactions need to be conducted across organizations and countries[40], constructing transaction environments has become a new research hotspot. Transaction environments have evolved from cloud-based environments[41] to distributed transaction environments[42]. Studies[42],[43],[44] have explored how to use blockchain technology to address security and credibility issues in data transactions within distributed environments. Research[45],[46] aims to promote cross-border data flow and transactions through more reasonable profit distribution mechanisms.

Research on transaction environment construction schemes has also stimulated in-depth exploration of governance mechanisms for data factor tradings. Governance mechanisms are divided into two types: governance centered on organizing units or departments, and governance based on polycentric governance theory. Governments[47],[48], internet platforms[49], and data intermediaries[50] all play organizing roles. In the "platform society"[49], a large amount of data is controlled by a few large technology platforms, making platforms a natural dominant model for data governance. By applying evolutionary game theory, the value of regulators in open data governance is elaborated[51]. Attention needs to be paid to balancing differences between individuals, and between individuals and policymakers[52].

On the other hand, data stored dispersedly among numerous interconnected entities forms a "datasphere"[53]. In environments where governments, markets, societies, and non-governmental organizations coexist, studies[54] have discussed how to use polycentric governance theory[55],[56] to promote coordination and cooperation among different entities and establish a more efficient market. While polycentric governance theory is increasingly accepted as a governance concept, relative differences between entities in the datasphere lead to divergences in their governance demands.

The abstraction process directly defines data as data factors but fails to resolve the inherent dilemmas of non-excludability and non-rivalry in data itself. Unlike existing research, while abstracting data, we have defined new connotations for data factors through an extended approach.

5. Conclusion and Future Work

The non-excludability of data is the core focus of our research. Compared with data factors, other factors of production possess excludability. The boundaries of excludable factors are easier to define, and property-rights proof can be established through registration and query, thereby achieving protection at both the physical and the property-rights levels; the boundaries of

non-excludable factors, by contrast, are difficult to define, and such factors cannot form effective proof through themselves, so they require an institutional system to constrain users' behavior in order to achieve the effect of protecting the factor. Accordingly, the governance of excludable factors can rely more on private property-rights mechanisms, whereas data factors, because they cannot define their own boundaries, rely more on Common-Pool Resource (CPR) governance mechanisms that take the constraint of users' behavior as their core.

This therefore requires that the information system be grounded in CPR governance mechanisms, so as to control the orderly flow of data factors among specific subjects and thereby create value. At the present stage, this research has identified the point of convergence between economic theory and technical solutions, linking economic and technical issues so that the next stage of development can be applied more rapidly to the construction of data trading markets. In terms of the service goal, this system is essentially different from systems that encourage information sharing.

Building upon Ostrom's CPR governance framework outlined above, we define the data factor as a six-tuple. Meanwhile, we develop a technical system embedded with the "supervision-punishment-commitment" mechanism to enable the governance of factor excludability. Relying on the "terminal-pipe-cloud" architecture, this technical system can construct an operating environment for data-factor transactions.

To verify the role of this new data factor definition in constructing transaction markets, we employed evolutionary game theory to simulate two key aspects: first, market stability under the coexistence of strategies (i.e., cooperation, defection, loner, and punishment); second, the impact of initial market institutions on participants' strategy choices. In a certain sense, when a dataset can be converted into a six-tuple format, it can become a tradable data factor.

The punishment behavior supported by the combination of the SIP protocol and the NAT network—namely, connection blocking—is essentially a pledge mechanism collateralized by the punished party's entire business cooperation value. Its effect directly impacts the punished party's ongoing and subsequent transactions, thereby effectively freezing its business relationships in the market. Compared with smart contract slashing, the blocking approach does not require defining the relationship between the collateral value and the transaction value, which simplifies transaction rules, reduces participation costs, and eliminates potential arbitrage opportunities. Reputation systems can help traders select more trustworthy counterparts; however, from a governance mechanism perspective, reputation systems only accomplish the "commitment-supervision" phase and lack an effective punishment mechanism.

The primary task for the next step is to expand the application scope of computing environments that support factor property rights protection in data trading scenarios, and to extend into data-driven cooperation and collaboration fields. To improve system reliability, we will use the SIP OPTIONS method to periodically query the status of network elements and the platform during prototype system development, and collect statistics on the effectiveness of the punishment mechanism. We will validate the prototype through a multi-party data collaboration scenario, and investigate system metrics such as the impact of fingerprint verification on model training performance (e.g., the percentage increase in sample reading time), the response time of the

punishment mechanism (connection blocking), and system throughput under concurrent transaction scenarios. We also expect to provide configuration recommendations for practical deployment by combining system performance analysis with the scenario. Secondly, improve the training efficiency of data sandboxes—for instance, by using neural networks to analyze malicious code and reducing the number of functions that need to be tracked. Thirdly, in real trading markets, transaction rules constrain the connectivity relationships among traders. Therefore, we need to investigate the impact of population topology on the equilibrium states of the game, as well as to study incentive mechanisms based on value distribution that enable more entities to benefit from data transactions. At the same time, we will treat system security and business security issues in data trading as an independent research problem.

6. Acknowledgments

This study was supported by the National Key R&D Program of China (No.2023YFB2703900).

Ethical Statement

No ethical approval was required for this study, as it did not involve human or animal subjects.

Funding

The authors declare the following interests: This work was supported by the National Key R&D Program of China (Grant No. 2023YFB2703900). The funders provided financial support for data collection and experiment implementation but had no role in the study design, data analysis, decision to publish, or preparation of the manuscript. All other authors have no competing financial or personal interests to declare.

Declaration of competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability Statements

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Credit authorship contribution statement

Chuan Fu: Conceptualization, Formal analysis, Methodology, Software Development, Writing-original draft, Writing-review & editing, Visualization, Validation.

Jian Ye: Funding acquisition, Project administration, Supervision, Review & editing, Validation.

References

1. A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *Journal of Economic Literature*, vol. 54, no. 2, p. 442–92, June 2016.
2. B. Martens, "An economic perspective on data and platform market power," <https://publications.jrc.ec.europa.eu/>

- repository/handle/JRC122896[Accessed on 3 April 2025], Brussels (Belgium), 2021.
3. D. A. Harper, "Property rights, entrepreneurship and coordination," *Journal of Economic Behavior & Organization*, vol. 88, pp. 62–77, 2013, Asian Institutional Economics. doi: <https://doi.org/10.1016/j.jebo.2011.10.018>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167268111002678>
4. L. Wang *et al.*, "Bigdatabench: A big data benchmark suite from internet services," in *2014 IEEE 20th International Symposium on High Performance Computer Architecture (HPCA)*, 2014, pp. 488–499, doi: <https://doi.org/10.1109/HPCA.2014.6835958>.
5. J. Zhan, "A benchcouncil view on benchmarking emerging and future computing," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, vol. 2, no. 2, p. 100064, 2022, doi: <https://doi.org/10.1016/j.tbench.2022.100064>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2772485922000515>
6. J. E. Raffaghelli and S. Manca, "Is there a social life in open data? the case of open data practices in educational technology research," *Publications*, vol. 7, no. 1, 2019, doi: <https://doi.org/10.3390/publications7010009>. [Online]. Available: <https://www.mdpi.com/2304-6775/7/1/9>
7. A. Conti, V. Gupta, J. Guzman, and M. P. Roche, "Incentivizing innovation in open source: Evidence from the github sponsors program," National Bureau of Economic Research, Working Paper 31668, September 2023, doi: <https://doi.org/10.3386/w31668>. [Online]. Available: <http://www.nber.org/papers/w31668>
8. C. Ihle, D. Trautwein, M. Schubotz, N. Meuschke, and B. Gipp, "Incentive mechanisms in peer-to-peer networks — a systematic literature review," *ACM Comput. Surv.*, vol. 55, no. 14s, Jul. 2023, doi: <https://doi.org/10.1145/3578581>. [Online]. Available: <https://doi.org/10.1145/3578581>
9. E. Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge: Cambridge University Press, 10 2015, doi: <https://doi.org/10.1017/CBO9781316423936>.
10. H. Ren, "Governance problems of common-pool resources from the perspective of elinor ostrom's thought of self-governance: characteristics, models and difficulties," *Social Sciences in Shenzhen*, vol. 4, no. 6, pp. 60–70, 2021.
11. C. J. Ritten, C. Bastian, and O. Phillips, "The relative effectiveness of law enforcement policies aimed at reducing illegal trade: Evidence from laboratory markets," *PLOS ONE*, vol. 16, no. 11, p. e0259254, 2021.
12. C. Fu, G. Zhang, J. Yang, and X. Liu, "Study on the contract characteristics of internet architecture," *Enterprise Information Systems*, vol. 5, no. 4, pp. 495–513, 2011. [Online]. Available: <https://doi.org/10.1080/17517575.2011.570457>
13. E. Gallo, Y. E. Riyanto, N. Roy, and T.-H. Teh, "Cooperation and punishment mechanisms in uncertain and dynamic social networks," *Games and Economic Behavior*, vol. 134, pp. 75–103, 2022, doi: <https://doi.org/10.1016/j.geb.2022.03.015>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0899825622000677>
14. A. Leibbrandt, A. Ramalingam, L. Sääksvuori, and J. M. Walker, "Incomplete punishment networks in public goods games: experimental evidence," *Experimental Economics*, vol. 18, pp. 15–37, 03 2015.
15. W. Zhang, S. Zhang, and S. Guo, "A pagerank-based reputation model for personalised manufacturing service recommendation," *Enterprise Information Systems*, vol. 11, no. 5, pp. 672–693, 2017, doi: <https://doi.org/10.1080/17517575.2015.1077998>. [Online]. Available: <https://doi.org/10.1080/17517575.2015.1077998>
16. X. Yin, X. Hu, Y. Chen, X. Yuan, and B. Li, "Signed-pagerank: An efficient influence maximization framework for signed social networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 33, no. 5, pp. 2208–2222, 2021, doi: <https://doi.org/10.1109/TKDE.2019.2947421>.
17. G. S. Becker, "Crime and punishment: an economic approach," *Journal of Political Economy*, vol. 76, no. 2, pp. 169–217, 1968, doi: https://doi.org/10.1007/978-1-349-62853-7_2. [Online]. Available: https://doi.org/10.1007/978-1-349-62853-7_2
18. D. Mahmudnia, M. Arashpour, and R. Yang, "Blockchain in construction management: Applications, advantages and limitations," *Automation in Construction*, vol. 140, p. 104379, 2022, doi: <https://doi.org/10.1016/j.autcon.2022.104379>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0926580522002527>
19. H. Zhao, Z. Zhu, C. Pan, Z. Yao, W. Zhu, and X. Si, "A new electronic contract system model based on blockchain," in *Blockchain and Trustworthy Systems*, H.-N. Dai, X. Liu, D. X. Luo, J. Xiao, and X. Chen, Eds. Singapore: Springer Singapore, 2021, pp. 407–417. [Online]. Available: https://doi.org/10.1007/978-981-16-7993-3_31
20. A. Venčkauskas, D. Kukta, S. Grigaliūnas, and R. Brūzgienė, "Enhancing microservices security with token-based access control method," *Sensors*, vol. 23, no. 6, 2023. [Online]. Available: <https://doi.org/10.3390/s23063363>
21. W. Xu, S. Bhatkar, and R. Sekar, "Taint-Enhanced policy enforcement: A practical approach to defeat a wide range of attacks," in *15th USENIX Security Symposium (USENIX Security 06)*. Vancouver, B.C. Canada: USENIX Association, Jul. 2006. [Online]. Available: <https://www.usenix.org/conference/15th-usenix-security-symposium/taint-enhanced-policy-enforcement-practical-approach>
22. W. Enck *et al.*, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Trans. Comput. Syst.*, vol. 32, no. 2, Jun. 2014, doi: <https://doi.org/10.1145/2619091>. [Online]. Available: <https://doi.org/10.1145/2619091>
23. S. Muttou, S. Kumar, and N. Tyagi, "A survey of computer security models," *JIMS 8i-International Journal of Information, Communication and Computing Technology (IJICCT)*, vol. II, no. 1, pp. 48–56, Jan-Jun 2014.
24. W. G. J. Halfond, A. Orso, and P. Manolios, "Using positive tainting and syntax-aware evaluation to counter sql injection attacks," in *Proceedings of the 14th ACM SIGSOFT International Symposium on Foundations of Software Engineering*, ser. SIGSOFT '06/FSE-14. New York, NY, USA: Association for Computing Machinery, 2006, p. 175–185, doi: <https://doi.org/10.1145/1181775.1181797>. [Online]. Available: <https://doi.org/10.1145/1181775.1181797>
25. A. Javed, P. Lam, and A. Chan, "Change negotiation in public-private partnership projects through output specifications: an experimental approach based on game theory," *Construction Management and Economics*, vol. 32, no. 4, pp. 323–348, 05 2014. [Online]. Available:

- <https://doi.org/10.1080/01446193.2014.895846>
26. M. A. Nowak, *Evolutionary Dynamics: Exploring the Equations of Life*. Cambridge, Mass: Belknap Press of Harvard University Press, 2006. [Online]. Available: <http://www.jstor.org/stable/j.ctvjghw98>
 27. L. Hindersin, B. Wu, A. Traulsen, and J. García, “Computation and simulation of evolutionary game dynamics in finite populations,” *Scientific Reports*, vol. 9, no. 6946, 2019. [Online]. Available: 10.1038/s41598-019-43102-z
 28. C. Hauert, A. Traulsen, H. De Silva née Brandt, M. A. Nowak, and K. Sigmund, “Public goods with punishment and abstaining in finite and infinite populations,” *Biological Theory*, vol. 3, no. 2, pp. 114–122, 04 2008. [Online]. Available: <https://doi.org/10.1162/biot.2008.3.2.114>
 29. C. Hauert, S. DE MONTE, J. Hofbauer, and K. Sigmund, “Replicator dynamics for optional public good games,” *Journal of Theoretical Biology*, vol. 218, no. 2, pp. 187–194, 2002.
 30. H. Brandt, C. Hauert, and K. Sigmund, “Punishing and abstaining for public goods,” *Proceedings of the National Academy of Sciences of the United States of America*, vol. 103, no. 2, pp. 495–7, 2006.
 31. C. Taylor, D. Fudenberg, A. Sasaki, and M. A. Nowak, “Evolutionary game dynamics in finite populations,” *Bulletin of Mathematical Biology*, vol. 66, no. 6, pp. 1621–1644, 2004, doi: <https://doi.org/10.1016/j.bulm.2004.03.004>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0092824004000333>
 32. Z. Cheng, B. Wang, Y. Pan, and Y. Liu, “Strategic analysis of participants in bcfi-enabled decentralized iot data sharing,” *Mathematics*, vol. 11, no. 21, pp. 1–19, November 2023. [Online]. Available: <https://ideas.repec.org/a/gam/jmathe/v11y2023i21p4520-d1272948.html>
 33. A. de Azevedo-Lopes and A. Traulsen, “Multilevel selection in multitype populations,” *PNAS Nexus*, vol. 5, no. 6, p. pgag180, 6 2026, doi: <https://doi.org/10.1093/pnasnexus/pgag180>. [Online]. Available: <https://doi.org/10.1093/pnasnexus/pgag180>
 34. H. J. Watson, C. Fuller, and T. Ariyachandra, “Data warehouse governance: best practices at blue cross and blue shield of north carolina,” *Decision support systems*, vol. 38, no. 3, pp. 435–450, 2004.
 35. A. Z. Faroukhi, I. El Alaoui, Y. Gahi, and A. Amine, “Big data monetization throughout big data value chain: a comprehensive review,” *Journal of Big Data*, vol. 7, no. 3, pp. 1–22, 2020.
 36. N. Martijn, J. Hulstijn, M. Bruijne, and Y.-H. Tan, “Determining the effects of data governance on the performance and compliance of enterprises in the logistics and retail sector,” in *Open and Big Data Management and Innovation*, M. Janssen et al., Eds. Cham: Springer International Publishing, 10 2015, pp. 454–466.
 37. G. Demarquet, “Five key reasons enterprise data governance matters to finance . . . and seven best practices to get you there,” *Journal of Corporate Accounting & Finance*, vol. 27, no. 2, pp. 47–51, 2016.
 38. L. Ge and C. A. Brewster, “Informational institutions in the agrifood sector: meta-information and meta-governance of environmental sustainability,” *Current Opinion in Environmental Sustainability*, vol. 18, no. Feb., pp. 73–81, 2016.
 39. S. Rosenbaum, “Data governance and stewardship: Designing data stewardship entities and advancing data access,” *Health services research*, vol. 45, no. 5 Pt 2, pp. 1442–55, 10 2010. [Online]. Available: <https://doi.org/10.1111/j.1475-6773.2010.01140.x>
 40. S. A. Aaronson, “Data is different, and that’s why the world needs a new approach to governing cross-border data flows,” *Digital Policy, Regulation and Governance*, vol. 21, no. 5, pp. 441–460, 2019.
 41. M. Balazinska, B. Howe, and D. Suciu, “Data markets in the cloud: an opportunity for the database community,” *Proc. VLDB Endow.*, vol. 4, no. 12, p. 1482–1485, Aug. 2011, doi: <https://doi.org/10.14778/3402755.3402801>. [Online]. Available: <https://doi.org/10.14778/3402755.3402801>
 42. A. E. Abbas, W. Agahari, M. van de Ven, A. Zuiderwijk, and M. de Reuver, “Business data sharing through data marketplaces: A systematic literature review,” *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 16, no. 7, pp. 3321–3339, 2021, doi: <https://doi.org/10.3390/jtaer16070180>. [Online]. Available: <https://www.mdpi.com/0718-1876/16/7/180>
 43. F. de la Vega, J. Soriano, M. Jimenez, and D. Lizcano, “A peer-to-peer architecture for distributed data monetization in fog computing scenarios,” *Wireless Communications and Mobile Computing*, vol. 2018, no. 1, p. 5758741, 2018, doi: <https://doi.org/10.1155/2018/5758741>. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1155/2018/5758741>
 44. D. Wörner and T. von Bomhard, “When your sensor earns money: exchanging data for cash with bitcoin,” in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, ser. UbiComp ’14 Adjunct. New York, NY, USA: Association for Computing Machinery, 2014, p. 295–298, doi: <https://doi.org/10.1145/2638728.2638786>. [Online]. Available: <https://doi.org/10.1145/2638728.2638786>
 45. B. Shen, Y. Shen, and W. Ji, “Profit optimization in service-oriented data market: A stackelberg game approach,” *Future Generation Computer Systems*, vol. 95, no. JUN., pp. 17–25, 2019.
 46. B. Guo, X. Deng, Q. Guan, J. Tian, and X. Zheng, “An incentive mechanism for cross-organization data sharing based on data competitiveness,” *IEEE Access*, vol. 6, pp. 72 836–72 844, 2018.
 47. S. S. Dawes and N. Helbig, “Information strategies for open government: Challenges and prospects for deriving public value from government transparency,” in *Electronic Government, 9th IFIP WG 8.5 International Conference, EGOV 2010, Lausanne, Switzerland, August 29 - September 2, 2010. Proceedings*. Berlin: Springer, 08 2010, pp. 50–60.
 48. J. Höchtl, P. Parycek, and R. Schöllhammer, “Big data in the policy cycle: Policy decision making in the digital era,” *Journal of Organizational Computing and Electronic Commerce*, vol. 26, no. 1-2, pp. 147–169, 2016, doi: <https://doi.org/10.1080/10919392.2015.1125187>. [Online]. Available: <https://doi.org/10.1080/10919392.2015.1125187>
 49. S. Lee, L. Zhu, and R. Jeffery, “Data governance decisions for platform ecosystems,” in *Proceedings of the Annual Hawaii International Conference on System Sciences. Vol. 2019-January. IEEE Computer Society*, 2019, p. 6377–6386. [Online]. Available: <https://doi.org/10.24251/HICSS.2019.766>
 50. E. Podda, “Data governance act (dga),” in *Encyclopedia of Cryptography, Security and Privacy*. Cham: Springer

-
- Nature Switzerland, 2025, pp. 564–566.
51. Q. Li, B. Pi, M. Feng, and J. Kurths, “Open data in the digital economy: An evolutionary game theory perspective,” *IEEE Transactions on Computational Social Systems*, vol. 11, no. 3, pp. 3780–3791, 2024, doi: <https://doi.org/10.1109/TCSS.2023.3324087>.
 52. D. Castro and R. Atkinson, “Beyond internet universalism: A framework for addressing cross-border internet policy,” *SSRN Electronic Journal*, 9 2014. [Online]. Available: <https://doi.org/10.2139/ssrn.3079821>
 53. D. Reinsel, J. Gantz, and J. Rydning, “Data age 2025,” url <https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf>[Accessed on 9 April 2025] , 2017.
 54. C. Aguerre, M. Campbell-Verduyn, and J. Scholte, *Global Digital Data Governance: Polycentric Perspectives*. Routledge, 01 2024, doi: <https://doi.org/10.4324/9781003388418>.
 55. E. Ostrom, “A general framework for analyzing sustainability of social-ecological systems,” *Science*, vol. 325, no. 5939, pp. 419–422, 08 2009.
 56. —, “Beyond markets and states: polycentric governance of complex economic systems,” *Transnational Corporations Review*, vol. 2, no. 2, pp. 167–209, 2010.