

Research on the Application Path of Dual-Mode API Data Market for Enabling Cross-Domain Multi-Scenario Data Circulation

Chen Mutong, Ni Xiong, Xiao Chuqiao

Shanghai Municipal Big Data Center, Shanghai 200072, China

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: In response to the industry pain points such as scattered data sources, inconsistent standards, lack of trust, restricted high-sensitive data circulation, high costs for small and medium-sized entities to access, and the limitations of the traditional centralized and point-to-point single data circulation model in cross-domain scenarios, this paper combines the theories of data market, data space, and data intermediary, and proposes a “point-to-point + adapter” dual-mode API data market circulation path. By constructing a core architecture that separates the management flow from the data flow, the point-to-point mode ensures the local controllable circulation of highly sensitive data, and the adapter mode reduces the access threshold for existing systems and small and medium-sized entities. This paper builds an exclusive application framework and studies its migration paths in areas such as cargo trade document verification, cross-departmental government approval, financial joint risk control, supply chain collaboration, and industrial internet. The research shows that this model can achieve trusted, compliant, and large-scale cross-domain data circulation without aggregating the original data, providing a feasible infrastructure solution for the release of value of data elements in multiple scenarios.

Keywords: Dual-mode API data market; Cross-domain data circulation; Adapter; Data space; Data intermediary; Shipping trade; Separation of management flow and data flow

Online publication: Sept 3, 2026

1. Introduction

The full realization of the value of data elements relies on efficient and trustworthy circulation across entities, systems, and domains. This is also the core support for the high-quality development of the digital economy and the digital transformation of industries. Currently, global data circulation governance has evolved from simple technical optimization to a comprehensive system that integrates technical architecture, rights and responsibilities systems, market mechanisms, and scenario governance. Simply relying on technological transformation is no longer sufficient to solve the problems of large-scale, compliant, and ecological data

circulation. The EU's "Data Governance Act" and "Data Act" clearly define the institutional value of data intermediaries and establish rules for data ownership, circulation, and intermediary services. The relevant reports of the OECD and the World Bank also clearly point out that insufficient trust among entities, incompatible heterogeneous systems, and imbalanced incentives for data supply and demand are the core bottlenecks restricting the efficient reuse and value realization of data elements.

Shipping trade is the most complex typical scenario for cross-domain data circulation. It involves multiple entities such as cargo owners, shipping companies, ports, customs, and financial institutions, covering various types of heterogeneous data such as bills of lading, customs declaration forms, AIS trajectories, and letters of credit. It also has characteristics of cross-border, strict supervision, and high sensitivity. The data circulation problems in shipping trade are widely present in fields such as government affairs, finance, supply chain, and industrial internet.

The traditional data circulation model has obvious shortcomings: the pure point-to-point direct connection has a high degree of customization and is difficult to manage on a large scale, and it is prone to form data silos; the centralized data platform is likely to cause the aggregation of raw data, leading to compliance risks, data leakage, and unclear rights and responsibilities. Based on this, this paper constructs a "point-to-point + adapter" dual-mode API data market system, focusing on solving core issues such as cross-domain heterogeneous data circulation, high-sensitivity data security control, and low-cost access by small and medium-sized entities, and exploring its multi-scenario implementation paths and promotion value.

2. Related research review

2.1. Data market and API economy

The core of the data market lies in establishing a system for matching data supply and demand, productizing data, setting prices, conducting transactions, and governing the system. It aims to address the issue of insufficient incentives for data sharing and the dispersion of resources, and to promote the transition of data from raw data sets to ecological delivery of data services and analytical capabilities. The API economy, through standardized interfaces, enables the service and productization of enterprises' capabilities and data, serving as the core support for cross-system and cross-entity interconnection. The combination of these two forms a new type of data circulation infrastructure, the API data market, which is not merely an interface display platform, but integrates authorization, invocation, measurement, auditing, and security control.

2.2. Data space and data intermediary

The data space adopts the lightweight integration concept of "on-demand integration and stepwise iteration", breaking the traditional barrier of unified global modeling. Practices such as European IDSA and Gaia-X have further constructed a distributed data sovereignty, interoperability, and usage control system. The data intermediary, as a core institutional innovation, has a core value that lies in neutral mediation, reducing transaction costs, and avoiding risks in the centralized original data. It only undertakes governance functions such as directory management, authorization verification, and audit evidence storage, without touching the original data. This is also the core theoretical support of the dual-mode architecture in this paper^[1].

2.3. Cross-domain security and industry standards

The zero-trust architecture and the ISO series of information security standards provide paradigmatic support

for boundary penetration and security control across private networks, clouds, and the internet. The DID/VC distributed identity system realizes decentralized and traceable authorization verification. The DCSA data standard in the shipping and trade field and the UNCITRAL electronic transferable record model law provide technical and legal support for the standardized circulation of industry data and the legal validity determination of electronic documents, and offer a compliance basis for the implementation of the dual-mode mechanism scenarios.

3. Analysis of issues in cross-domain multi-scenario data circulation

3.1. Multi-source heterogeneity and prominent network boundary barriers

Industry data is scattered across government and private networks, financial intranets, enterprise private clouds, and various business systems. Data formats include API interfaces, messages, document files, real-time device streams, and many other types, exhibiting strong heterogeneity. Networks of different entities are isolated from each other. Forcing unified interfaces and data aggregation would incur extremely high transformation costs and compliance resistance, making it difficult to adapt to large-scale circulation needs.

3.2. Lack of trust among entities and ambiguous definition of rights and responsibilities

The core pain points of data circulation are “not daring to share, not willing to share, and not knowing how to share”. Government departments are concerned about unauthorized access and liability risks, enterprises are wary of the leakage of business secrets and the abuse of data by competitors, and financial institutions are concerned about the authenticity of data and compliance responsibilities. Traditional platforms only solve the problems of “discoverability and connectivity” of data, but they cannot clearly define the authorization entity, usage scope, and accountability basis, and it is difficult to build a trustworthy circulation system ^[2].

3.3. Single model cannot adapt to multi-level data security requirements

Cross-domain data has a clear hierarchical security classification: for instance, high-sensitivity data such as customs declaration forms, financial credit, and core orders must not be centrally transferred; while low-sensitivity data such as logistics status, public directories, and de-identified data aim for efficiency in circulation. The single point-to-point model is prone to forming data silos, and the single centralized model amplifies security and compliance risks. The industry urgently needs differentiated and scenario-based circulation mechanisms.

3.4. Weak access capability of small and medium-sized participants

At present, the construction of the domestic data ecosystem is mostly led by large leading enterprises and various public departments at all levels. The industry resources, technical capabilities, and data access rights are highly concentrated. However, the numerous small and medium-sized freight forwarders, small and medium-sized manufacturing enterprises, grassroots service providers, and small and medium-sized trading enterprises in the industry generally lack professional API connection operation and maintenance capabilities, data standardization governance, and cybersecurity compliance control capabilities. They also have limited technical reserves and capital investment. The strict access standards, complex adaptation processes, and high renovation costs of traditional data platforms have led to the data market being confined to a closed circulation among a few large entities for a long time. It fails to form an all-encompassing industrial network

effect, severely restricting the large-scale circulation and value release of data elements throughout the entire industrial chain ^[3].

4. Mechanism design of the dual-mode API data market

4.1. Overall architecture

The dual-mode API data market constructed in this paper adopts a hierarchical architecture, consisting of six major modules: data directory layer, authorization governance layer, API access layer, secure transmission layer, audit measurement layer, and operation service layer. The core innovation lies in the separation of management flow and data flow. The platform only carries management flow data such as directory registration, identity authentication, authorization management, invocation auditing, and measurement evidence storage. The original data flow flows between the supply and demand parties in accordance with the model, without passing through the platform for transfer. This fundamentally avoids the risk of data concentration and guarantees the sovereignty of the data holder ^[4].

4.2. Point-to-point mode: Trusted direct connection for highly sensitive data

This model is applicable to high-sensitivity, highly compliant, and high-value scenarios such as financial credit granting, customs declaration verification, and core supply chain data. In terms of the process, the data user discovers the data product on the market platform and submits an application; the data holder reviews the data usage, calling scope and security conditions; the authorizer completes the authorization confirmation through DID/VC or other trusted credentials; the platform synchronizes the authorization status and calling credentials; the data user sends a request to the data holder's API with the authorization code; the data holder verifies the authenticity and validity period of the authorization through the platform or local verification service; after verification is successful, the holder responds with the data or results in the original path; the platform only records the calling summary, authorization status and necessary audit information. The advantage of this model lies in that the data does not pass through the platform, and sensitive information is not concentrated; the data can be controlled in terms of access and risk management; supervision can be traced through chain summaries, hashes, and authorization status. The disadvantage is that it requires certain API integration capabilities from the participating parties, and it is more suitable for high-value data circulation among large institutions, financial entities, and leading enterprises ^[5].

4.3. Adapter mode: Lightweight access for legacy systems

This model is designed for scenarios where the existing systems are outdated, the transformation capabilities are weak, and there are a large number of small and medium-sized entities. In this model, lightweight adapters are deployed at the boundary of the data holder to undertake five core functions: First, protocol adaptation, converting legacy databases, files, and various interfaces into standard API services; second, authorization verification, verifying the calling entity, purpose, scope, and validity period; third, format mapping, converting unstructured data into standardized data products; fourth, log reporting, synchronizing call summaries, abnormal information, and audit hashes; fifth, security proxy: achieving cross-domain secure transmission through keys, authentication, and whitelist. The core value of this model lies in significantly reducing the access threshold. There is no need to modify the business system; it can be implemented by simply configuring. Small and medium-sized institutions can be deployed in a lightweight manner, and

industry platforms can be used as data space connectors for practical applications.

4.4. Mode selection rules

The dual-mode API data market should not allow users to arbitrarily choose the mode, but should form rules based on data sensitivity levels, entity capabilities, business timeliness, and compliance requirements. The following selection logic can be established. As shown in **Table 1**.

Table 1. Mode selection rules

Dimension of judgment	Peer-to-peer model	Adapter pattern
Data sensitivity	High sensitivity, strict supervision, business secrets, financial risk data	Moderately low sensitivity, status-related, event-related, desensitized data or locally fieldable data
Original data control	The original data is always directly controlled by the holder.	The original data remains on the holding party's side, and the adapter is responsible for the conversion and proxying.
Accessing entity capability	Both parties possess strong API and security operation capabilities.	A large number of legacy systems, weak renovation capabilities, and a large number of small and medium-sized entities
Typical scenario	Financial credit granting, customs declaration verification, confidential government affairs supervision	Logistics status synchronization, warehouse document circulation, reuse of government affairs materials, and data integration of industrial equipment

4.5. Lightweight toolset and operational mechanism

Four lightweight tool components—access, authorization, archiving, and supervision—are deployed, supporting visual configuration and automated operations. At the same time, a standardized operation system is established to regulate data product listing, version management, frequency control, service quality evaluation, and dispute resolution mechanisms, clearly defining the platform's neutral operational positioning to prevent it from acting as both referee and player, thereby avoiding conflicts of rights and responsibilities.

5. Cross-domain application scenarios

5.1. Shipping trade: Document verification and industry-finance collaboration

As the core pilot scenario, the shipping trade domain achieves differentiated circulation through the dual-mode system: highly sensitive documents such as bills of lading, customs declarations, and financing credit approvals adopt the point-to-point mode to ensure the security of trade and financial data; standardized low-sensitivity data such as ship schedules, port operations, and logistics trajectories are uniformly accessed through adapters. Based on industry standards, trusted verification of electronic documents is achieved, connecting trade, logistics, and financial data chains, solving problems such as cumbersome manual verification, document forgery, and financing risk control difficulties, supporting the implementation of scenarios such as offshore trade, commodity trading, and warehouse receipt pledge financing.

5.2. Government services: Cross-departmental approval and benefit fulfillment

To address issues such as cross-departmental government data barriers, repeated document submission, and low approval efficiency, government data is standardized and cataloged. Sensitive data such as business operations and personal privacy adopt point-to-point authorized invocation, while government public information and status data are reused across departments through adapters. In the scenario of preferential

policy benefit fulfillment, the platform automatically matches enterprise qualification data through authorization verification, with full traceability and auditability, significantly improving approval and policy fulfillment efficiency while ensuring government data compliance.

5.3. Financial risk control: Minimal necessary data collaborative risk control

The financial industry strictly adheres to the data minimization principle. High-risk scenarios such as credit approval and anti-fraud adopt the point-to-point mode for precise invocation of core sensitive data; auxiliary data such as supply chain transactions and logistics fulfillment are accessed in batches through adapters. The platform defines data sources and usage boundaries through authorization archiving and log auditing, supporting financial institutions in compliant risk control, while also enabling result-based data interaction to reduce plaintext data exposure and mitigate data misuse risks.

5.4. Supply chain collaboration: Full-chain data linkage

Given the characteristics of fragmented data in the supply chain and strong demands for commercial privacy protection, an adapter pattern is adopted to uniformly adapt heterogeneous ERP, WMS, and TMS systems from multiple enterprises, achieving large-scale linkage of orders, logistics, and inventory status. Confidential data such as pricing, customer resources, and credit limits of core enterprises are managed through a point-to-point mode. This model does not require the reconfiguration of the business systems of each entity in the supply chain, enabling full-chain collaboration while balancing the efficiency of collaboration and commercial privacy security.

5.5. Industrial internet: Cross-domain industrial data collaboration

Industrial equipment data, process parameters, and quality inspection data are highly frequent, heterogeneous, and highly sensitive. They are connected to edge gateways, MES, and IoT platforms through adapter mode, and standardized event streams are aggregated. Sensitive data such as core processes, fault traceability, and high-end production parameters are directly connected in a point-to-point mode. It meets the interconnection requirements of industrial parks and equipment from different manufacturers, builds a lightweight industrial data space, and supports industrial digital collaboration.

6. Promotion path and evaluation indicators

6.1. Phased implementation path

The first stage is the pilot verification of scenarios, with a focus on implementing scenarios with clear boundaries and definite value, such as customs trade document verification, reuse of government materials, and supply chain pledge financing. The verification of dual-mode adaptation rules and auditing systems is also conducted. The second stage is the replication of industry standardization, where data product specifications, API interface standards, and authorization templates for various industries are consolidated to form reusable industry access solutions. The third stage is the expansion of the ecosystem across the entire domain, relying on government guidance, leading enterprises' traction, and service providers' empowerment to promote large-scale access by small and medium-sized entities, and to improve the ecosystem governance system.

6.2. Role division of entities

The government is responsible for rule-making, compliance supervision and public data authorization; industry leaders provide core data products and scenario guidance; financial institutions offer risk control and financing needs; third-party service providers provide technical support such as adapter deployment and operation maintenance; small and medium-sized enterprises participate in the ecosystem through lightweight access; platform operators remain neutral, dedicated to governance and auditing, to ensure the fairness and trustworthiness of the ecosystem.

6.3. Core evaluation indicators

A comprehensive evaluation system is constructed from four dimensions: Firstly, business efficiency indicators, which cover the access cycle, approval duration, and frequency of manual verification; Secondly, security compliance indicators, including the rate of unauthorized interception, the completeness rate of logs, and the rate of sensitive data transfer through the platform; Thirdly, ecosystem expansion indicators, covering the number of access entities, the scale of data products, and the access costs for small and medium-sized entities; Fourthly, value creation indicators, including the availability of financing, the efficiency of customs clearance and approval, and the data reuse rate, etc., to verify the implementation effectiveness of the model through quantitative dimensions.

7. Challenges and outlook

At present, there are still several challenges in the implementation of the dual-mode API data market: Firstly, the semantic and interface standards across industries have not been unified, which may lead to new issues of data fragmentation; Secondly, the adapter security certification system is missing, and the compliance and anti-tampering capabilities of its operation need to be standardized and controlled; Thirdly, the continuous zero-trust verification mechanism across network domains needs to be improved; static boundary protection cannot adapt to dynamic circulation scenarios; Fourthly, the rights and responsibilities of data intermediaries and the pricing incentive system have not been fully institutionalized; Fifthly, the mutual recognition of cross-border data circulation rules is difficult.

In the future, this model will be deeply integrated with privacy computing, verifiable credentials, AI risk control, and digital trade rules, continuously optimizing the minimum disclosure of data and the ability of trusted result interaction. In the long term, it will adhere to the core principle of “platform managing governance, data belonging to the entities, and adapters reducing barriers”, and build a replicable, auditable, and manageable cross-domain data circulation infrastructure.

8. Conclusion

In response to the industry pain point that it is difficult to balance security, efficiency, and compliance in cross-domain multi-scenario data circulation, this paper proposes a “point-to-point + adapter” dual-mode API data market application path. Through the core architecture of separating management flow from data flow, the point-to-point mode solves the problem of secure circulation of highly sensitive data, ensuring data sovereignty and compliance as a bottom line; the adapter mode breaks through the bottleneck of difficult system adaptation and high access costs for small and medium-sized entities, and realizes large-scale

ecological expansion. Its theoretical value lies in improving the scenario-based implementation mechanism of the data market and data space. Its practical value lies in providing a new type of data circulation solution without the risk of original data centralization for sectors such as shipping and trade, government affairs, finance, supply chain, and industrial internet, and can provide important support for the market-oriented allocation of data elements.

Funding

2024 National “Blockchain” Key Special Project “Key Technologies for Cross-departmental Data Access and Circulation Management in Shipping Trade” (Project No.: 2024YFB2705403)

Disclosure statement

The authors declare no conflict of interest.

References

- [1] International Data Spaces Association, 2024, Dataspace Protocol 2024-1.
- [2] Castro Fernandez R, Subramaniam P, Franklin M, 2020, Data Market Platforms: Trading Data Assets to Solve Data Problems. arXiv:2002.01047.
- [3] Azcoitia S, Laoutaris N, 2022, A Survey of Data Marketplaces and Their Business Models. arXiv:2201.04561.
- [4] Zhang M, Beltran F, Liu J, 2023, A Survey of Data Pricing for Data Marketplaces. arXiv:2303.04810.
- [5] Gunturu N, 2022, Enterprise API Transformation: Driving Towards API Economy. *International Journal of Computer Trends and Technology*, 70(6): 44–50.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.