



A Study on Legal Issues in the Regulation of Fintech Companies

from the Perspective of the Intersection of International Financial

Law and Company Law



Xinyan Kai^{1,2,a*}



¹*Faculty of Law, University of New South Wales, NSW2052, Australia*

^{*}*Corresponding Author:* kaixinyan2025@163.com

Abstract: This paper systematically examines legal issues in the regulation of fintech companies from the perspective of the intersection of international financial law and company law. First, it analyses the core contradictions between the protection of financial consumer rights and the protection of data security and privacy, revealing the limitations of traditional legal frameworks in algorithm governance and the regulation of decentralised organisations. Second, it explores pathways for constructing regulatory legal systems, proposing specific solutions such as improving specialised legislation, strengthening inter-agency coordination, and establishing a dynamic evaluation system; by comparing international experiences such as the UK regulatory sandbox, US functional regulation, and Singapore's modular legislation, it analyses the advantages and disadvantages of different legal systems; finally, combining China's practical experience, it proposes the construction of a Chinese-style regulatory framework characterised by 'legislative modularisation, tiered

regulation, and embedded governance’ to provide a legal pathway for balancing financial innovation and risk control.

Keywords: international financial law; company law; FinTech regulation; consumer rights protection

1. Introduction

1.1 Research Background and Significance

With the global expansion of FinTech, its business models (such as cross-border payments, smart investment advice, and blockchain financing) are increasingly transcending the boundaries of traditional finance and corporate governance, posing challenges to the compatibility of international financial regulatory rules and company law systems. On one hand, the cross-jurisdictional operations of FinTech companies blur the distinction between ‘financial institutions’ and ‘technology companies,’ leading to conflicts in the application of licensing regulation and risk isolation principles under international financial law, and equity structure and shareholder liability rules under company law; On the other hand, characteristics such as algorithmic autonomy and cross-border data flows have further exacerbated regulatory vacuums—for example, the contradiction between the anonymity of decentralised finance (DeFi) and the doctrine of piercing the corporate veil, as well as the overlap or gaps in cross-regulatory oversight between digital asset issuance and securities law and corporate law. In this context, studying regulatory pathways from an

interdisciplinary perspective can not only address the limitations of single-sector regulation but also provide theoretical support for global fintech governance and practical references for the compliant overseas expansion of Chinese fintech companies and the improvement of regulatory sandbox systems.

1.2 Research Objectives and Tasks

This study aims to systematically identify core legal issues in the regulation of fintech companies within the intersection of international financial law and company law. Specific objectives include: first, identifying points of conflict (e.g., balancing financial consumer protection with the principle of prioritising shareholder interests) and points of convergence (e.g., corporate governance obligations in anti-money laundering compliance) between the two legal systems in regulatory logic; Second, to analyse regulatory practices in typical jurisdictions (such as the EU, the United States, and Singapore) and summarise the application experience of ‘functional regulation’ and ‘substantive regulation’ in the intersection area; Third, based on comparative research and case analysis, to propose the construction of a collaborative regulatory framework that balances innovation and risk, clarifying the legal status of fintech companies, responsibility allocation, and cross-border regulatory cooperation mechanisms. The research tasks will focus on three levels: at the theoretical level, clarifying the legal foundations of cross-border

regulation; at the practical level, analysing existing institutional barriers; and at the policy level, proposing operational recommendations for improving regulations.

1.3 Research Methods and Structural Arrangements

This study will adopt a multidisciplinary cross-analysis approach combined with empirical research: first, through comparative legal research, it will compare legal documents (such as the EU's Digital Markets Act and the Regulation on the Supervision of Cryptographic Asset Markets) and corporate law revision dynamics in fintech regulation by international organisations (such as the IMF and FSB) and major countries, and extract the similarities and differences in regulatory paradigms; Second, using case analysis, this study will select cross-border dispute cases involving typical fintech companies (such as PayPal, Ant Group, and Ripple) to analyse the logic behind the judicial recognition of 'financial attributes' and 'corporate attributes'; Third, using legal dogmatics, this study will reconstruct the rules for the coordination of international financial law and company law in terms of regulatory objectives, responsible parties, and remedies. In terms of structural arrangement, the paper will be divided into five chapters: Chapter 1 is the introduction, Chapter 2 reviews the theoretical foundations and manifestations of regulatory conflicts, Chapter 3 analyses foreign practical experiences, Chapter 4 discusses the shortcomings of China's

current system, and Chapter 5 proposes improvement pathways and conclusions.

2. Overview of Fintech Companies

2.1 Definition and Classification of Fintech Companies

Fintech companies refer to business entities that utilise cutting-edge technologies such as big data, artificial intelligence, and blockchain to innovate traditional financial services. Their core characteristic lies in driving the restructuring and efficiency enhancement of financial functions through technology. According to the definition by the Financial Stability Board (FSB), such enterprises not only include technology companies that directly provide financial services but also third-party service providers that offer technical support to financial institutions. Based on business attributes, they can be categorised into two types: technology-enabled (e.g., technology companies providing intelligent risk control systems to banks) and business-innovative (e.g., platforms engaged in cross-border payments or digital currency issuance); Based on service areas, they can be further subdivided into payment settlement (e.g., mobile wallets), financing and lending (e.g., P2P lending), wealth management (e.g., smart investment advisory services), insurance technology (e.g., usage-based insurance), and blockchain finance (e.g., stablecoin issuers), among others. Some companies exhibit dual ‘technology-finance’ attributes due to overlapping business lines, complicating regulatory classification.

2.2 The Development History of Fintech Companies

The evolution of fintech can be traced back to the financial digitisation phase of the late 20th century, marked by the widespread adoption of ATMs and online banking, where technology served as an auxiliary tool for financial institutions. In the early 21st century, with the rise of mobile internet, technology-driven innovations began to emerge: P2P lending platforms (such as Zopa in the UK) appeared around 2005, and blockchain technology emerged alongside Bitcoin in 2010, driving explorations in financial disintermediation and decentralisation. Starting in 2015, artificial intelligence and big data technologies accelerated their penetration, with the implementation of models such as smart investment advisors (e.g., Betterment in the US) and biometric payment systems, marking the entry of fintech into a new phase of 'technological restructuring of financial logic.' In recent years, global regulatory frameworks have gradually improved (such as the EU's PSD2 and Singapore's MAS sandbox), and the industry has shifted from rapid growth to compliant development. At the same time, regulatory technology (RegTech) and sustainable fintech have become new trends, reflecting the dynamic balance between technological innovation and risk control.

2.3 Main business models of fintech companies

The current mainstream business models are characterised by the deep integration of technology and financial scenarios: First, payment and

settlement services utilise distributed ledger technology (DLT) to enable cross-border remittances (e.g., Ripple) or build a technical support system for central bank digital currencies (CBDCs), breaking through the efficiency bottlenecks of the traditional SWIFT system; Second, smart investment and financing services, which use machine learning algorithms to automate asset allocation (e.g., China's Licaitong AI investment advisory service), optimise credit assessment models (e.g., Ant Group's 'Sesame Credit'), or lower financing barriers for SMEs through equity crowdfunding platforms; Third, distributed finance (DeFi) categories, which build ecosystems such as lending (e.g., Aave) and derivatives trading (e.g., dYdX) without intermediaries based on smart contracts, challenging the intermediary status of traditional corporate financial institutions; Fourth, regulatory technology categories, which provide financial institutions with anti-money laundering (AML) monitoring and KYC automation solutions (e.g., Onfido in the UK), reducing compliance costs through technological means. Additionally, niche areas such as insurance technology (e.g., ZhongAn Insurance's scenario-based products) and supply chain fintech (e.g., IoT-based warehouse receipt pledge platforms) also demonstrate differentiated paths enabled by technology.

3. The Application of International Financial Law and Company Law in the Regulation of Fintech Enterprises

3.1 Basic Principles and Scope of Application of International Financial Law

3.1.1 Basic Principles of International Financial Law

The basic principles of international financial law form the cornerstone of the global financial governance order, with their core essence reflecting the dialectical unity of sovereign equality and cooperative governance. The principle of sovereign equality requires that all countries have jurisdiction over their own financial systems and cross-border financial activities. For example, Article 1 of the International Monetary Fund Agreement explicitly respects the monetary sovereignty of member states. However, this principle must be coordinated with the principle of international cooperation—such as the Basel Committee promoting global uniform regulatory standards through the Core Principles for Effective Banking Supervision. The European Union's Markets in Financial Instruments Directive II (MiFID II) requires member states to implement a ‘regulatory passport’ system for cross-border financial services, reflecting the balance between sovereignty transfer and rule coordination in the context of financial globalisation. Additionally, the principles of fairness, mutual benefit, and appropriate regulation are embedded in international financial treaties and practices: the former requires developed and developing countries to assume differentiated responsibilities in international financial cooperation (such as flexible

adjustments to IMF loan conditions), while the latter emphasises the prevention of systemic risks through a ‘risk-based’ regulatory approach, such as the Financial Stability Board's (FSB) special resolution rules for ‘too big to fail’ institutions.

3.1.2 Scope of Application of International Financial Law

The scope of application of international financial law encompasses three dimensions: subjects, conduct, and spatial scope. In terms of subjects, it includes sovereign states, international organisations (such as the IMF and the World Bank Group), as well as non-traditional entities such as transnational financial institutions (e.g., transnational banks and stock exchanges) and fintech companies. For example, the Financial Action Task Force (FATF) has incorporated virtual asset service providers (VASPs) into its anti-money laundering regulatory framework, clearly defining their international compliance obligations. The scope of conduct encompasses cross-border payment settlements, international investment and financing, and financial derivatives transactions. Typical examples include the Uniform Customs and Practice for Documentary Credits (UCP 600) regulating international trade financing, and the Principles for the Supervision of Cross-Border Payment Service Providers constraining the cross-border flow of digital currencies. In terms of spatial applicability, international financial law achieves cross-border coverage through the combination of ‘personal jurisdiction’ and ‘territorial jurisdiction’: For

example, the U.S. Foreign Account Tax Compliance Act (FATCA) requires foreign financial institutions to report information on U.S. citizen accounts to U.S. tax authorities, while the EU General Data Protection Regulation (GDPR) imposes ‘long-arm jurisdiction’ on cross-border financial data transfers. Both demonstrate the expansive and conflicting nature of international financial law in terms of spatial applicability.

3.2 Basic Principles and Scope of Application of Company Law

3.2.1 Basic Principles of Company Law

The basic principles of company law are centred on the independence of corporate legal personality and the limited liability of shareholders. The former establishes the independent legal status of a company as a legal entity under Section 26 of the German Civil Code, while the latter was first institutionalised under the UK's 1855 Limited Liability Act. Together, they form the cornerstone of the modern corporate system. However, the innovative forms of fintech companies challenge traditional principles: for example, decentralised autonomous organisations (DAOs) replace traditional governance structures with smart contracts, and their legal status as legal entities is difficult to encompass under the ‘legal person’ concept of the civil law system; the widespread use of shareholding proxy arrangements and voting rights delegation on equity crowdfunding platforms may undermine the ‘one share, one vote’ principle (e.g., the exception for preferred shares under Delaware corporate law in the United

States). Additionally, the capital maintenance principle faces application challenges in digital asset issuance—traditional company law requires companies to maintain paid-in capital to protect creditors, but the lack of tangible asset backing in ICOs (initial coin offerings) renders capital adequacy assessments without a standard, highlighting the temporal limitations of the principle's application.

3.2.2 Scope of Application of Company Law

The scope of application of company law is primarily based on territorial jurisdiction, with personal jurisdiction as a supplement, typically using the company's registered location as the core connecting point (e.g., Article 2 of China's Company Law limits the scope to ‘companies established within the territory of China’). However, the cross-border operations of fintech companies have broken through this framework. On the one hand, cross-border VIE structures (variable interest entities) achieve overseas listings through contractual control, leading to a separation between the actual place of business and the registered location, sparking debates over ‘regulatory arbitrage’ (e.g., the conflict between data sovereignty and corporate governance in Didi's listing in the United States); on the other hand, the virtual nature of the digital economy has made it difficult to determine the ‘company's registered office’—Singapore's Companies Act uses the ‘location of the actual management body’ as a supplementary standard, but blockchain companies' distributed nodes are

spread across the globe, making traditional territorial jurisdiction logic difficult to apply. Additionally, there are grey areas in the legal application to non-corporate fintech organisations (such as partnerships and cooperatives). For example, Wyoming's 2021 DAO Act granted DAOs limited liability company status, setting a precedent for special legislation.

3.3 The Cross-Application of International Financial Law and Company Law in the Regulation of Fintech Enterprises

The cross-application of international financial law and company law manifests in two dimensions: regulatory objective coordination and rule conflict adjustment. In terms of regulatory objectives, both aim to balance risk prevention and market efficiency: international financial law uses Basel III capital adequacy requirements to incentivise fintech companies to optimise their equity structures (e.g., SoftBank's investment in WeWork triggered regulatory inquiries due to excessive capital leverage); while corporate law reinforces risk internal controls in fintech companies through board independence requirements (e.g., the EU's Non-Executive Director Guidelines), forming a closed-loop system of 'external regulation-internal governance.' In terms of rule conflicts, a typical manifestation is the tension between 'long-arm jurisdiction' and corporate autonomy—the U.S. Foreign Corrupt Practices Act (FCPA) requires multinational fintech companies to assume joint liability for anti-money laundering compliance of their overseas subsidiaries, while the Cayman Islands Companies Law

allows offshore companies to simplify audit procedures, leading to compliance obligation conflicts for parent companies. In response, some countries have adopted ‘conflict of laws rules’ to prioritise stricter standards. For example, Section 7 of the UK Bribery Act stipulates that regardless of where a subsidiary is registered, if the parent company's headquarters is located in the UK, the anti-bribery provisions of the Act apply, reflecting the penetrative influence of international financial regulation on corporate governance.

4. Analysis of Legal Issues in the Regulation of Fintech Companies

4.1 Regulatory Gaps and Regulatory Arbitrage Issues

4.1.1 Manifestations of Regulatory Gaps

Regulatory gaps are primarily manifested in two key issues: ambiguous legal characterisation and lagging regulatory rules. In terms of entity classification, the anonymity and decentralised governance characteristics of decentralised finance (DeFi) platforms make it difficult to categorise them under traditional ‘financial institutions’ or ‘companies.’ For example, lending protocols like Aave use smart contracts to automatically execute lending processes, lacking a physical management structure, which renders the ‘licensing regulation’ requirements under international financial law and the ‘legal person status’ requirements under company law inapplicable. At the business level, cross-sector innovation further exacerbates the regulatory vacuum: stablecoin issuers (such as

USDT) possess dual attributes as both ‘payment tools’ and ‘securities,’ but the EU's Markets in Crypto-Assets Regulation (MiCA) only covers ‘electronic money tokens’ and ‘asset-referenced tokens,’ leaving no pre-emptive warning rules for algorithmic stablecoin collapses (such as UST); Equity crowdfunding platforms circumvent securities law registration requirements through ‘small-scale financing exemptions,’ but due to the vague definition of ‘public offering’ under company law, investor suitability management obligations are not fulfilled. Additionally, there are significant gaps in cross-border data flow and algorithm transparency regulation. The FATF's ‘travel rule’ requires virtual asset service providers (VASPs) to collect counterparty information, but the anonymous governance structure of DAO organisations prevents them from fulfilling this obligation, creating a regulatory vacuum in anti-money laundering oversight.

4.1.2 Manifestations of Regulatory Arbitrage

The core logic of regulatory arbitrage is to exploit legal differences to circumvent compliance requirements, manifesting in three aspects: first, the selection of ‘regulatory havens,’ fintech companies tend to register in regions with relaxed regulatory frameworks, such as the Cayman Islands and Bermuda, where offshore jurisdictions have minimal licensing requirements for cryptocurrency exchanges. FTX Group conducted cross-border operations through a subsidiary registered in Anguilla and remained

non-compliant with the U.S. SEC's investor protection standards until its bankruptcy. Second, business segmentation strategies, where core financial functions (such as asset custody) are placed in strictly regulated regions, while technical development and user operations are transferred to regions with more lenient rules. For example, a cross-border payment platform set up its data servers in Singapore to avoid the EU's General Data Protection Regulation (GDPR), while operating in Hong Kong to enjoy low tax rates, creating a 'regulatory fragmentation' loophole. Third, the abuse of regulatory sandboxes: some companies enter sandboxes under the guise of 'innovation testing,' then swiftly replicate untested business models across other jurisdictions. For example, the UK Financial Conduct Authority (FCA) sandbox discovered that a smart investment advisory platform provided services to non-sandbox users during the testing phase, exploiting regulatory discrepancies between sandbox and non-sandbox environments for arbitrage. Additionally, the 'RegTech tool' compliance packaging has become a new tactic, with some companies using algorithm optimisation to appear compliant on the surface (e.g., automatically generating anti-money laundering reports) while evading substantive review obligations.

4.2 Issues of Regulatory System and Regulatory Agency Coordination

4.2.1 Construction of the Regulatory System

The construction of a fintech regulatory system must achieve a dual integration of international rule coordination and domestic institutional innovation. At the international level, the cross-border regulatory framework of international financial law should be integrated based on the principle of ‘functional regulation.’ For example, the ‘same business, same risk, same regulation’ standard proposed in the Basel Committee's ‘Fintech Regulatory Principles’ should be aligned with the ‘principle of statutory company types’ in the company laws of various countries—— For fintech companies operating across borders, the ‘gatekeeper’ rules under the EU's Digital Markets Act (DMA) can be referenced, requiring them to establish a subsidiary in their registered jurisdiction and comply with local company law governance requirements (such as the mandatory provisions on the independence of supervisory boards under Germany's Stock Corporation Act), while also adhering to unified compliance standards under international financial law (such as the FATF's 40 Recommendations on Anti-Money Laundering). At the domestic level, it is necessary to break through the constraints of traditional sector-specific regulation and establish a complementary system of ‘dual-peak regulation’ and ‘sandbox mechanisms’: Australia centralises fintech regulatory authority under the APRA (Australian Prudential Regulation and Supervision Authority) and ASIC (Australian Securities and Investments Commission), with the former responsible for systemic risk prevention and the latter focusing on

market conduct regulation; The UK's FCA provides temporary exemptions for innovative businesses through its 'regulatory sandbox.' Its revised 2024 'Sandbox Operating Guidelines' have for the first time incorporated company law compliance reviews into testing evaluation criteria, requiring testing companies to submit their articles of association and shareholder rights statements to achieve simultaneous prevention of financial risks and corporate governance risks.

4.2.2 The Role and Challenges of Regulatory Agency Collaboration

The core value of regulatory agency collaboration lies in eliminating regulatory overlaps and gaps, but its effectiveness is constrained by both legal traditions and interest-based negotiations. In terms of functionality, cross-border collaboration can block regulatory arbitrage pathways: In 2023, the Federal Reserve, the European Central Bank, and the Bank of England established the 'Cross-Border Regulatory Alliance for Cryptocurrencies,' which successfully prevented a stablecoin issuer from using its offshore subsidiary to circumvent capital adequacy requirements by automatically sharing cross-border capital flow data of fintech companies (the entity registered in the Cayman Islands was required to apply the 'piercing the corporate veil' principle of the parent company's laws to recover the insufficiently paid-in capital). Domestic coordination is reflected in the collaboration between financial regulatory authorities and company registration agencies—the State Administration for Market

Regulation and the People's Bank of China jointly issued the 'Administrative Measures for the Registration of Fintech Companies,' requiring blockchain companies to submit an additional 'Decentralised Governance Structure Statement' during registration, extending the registration and filing functions of company law to the field of technical risk prevention and control. Challenges include prominent issues such as legal conflicts and imbalanced resource allocation: Civil law countries (such as Germany) emphasise 'regulatory statutoryism,' requiring financial technology companies to obtain dual approval from regulatory authorities and company registration authorities for business changes, leading to delayed innovation responses; Common law countries (such as the United States) rely on 'case law supplementation,' and in a 2024 ruling by a Delaware court on a DAO organisation, the court recognised the validity of smart contracts as company bylaws for the first time, but the lack of statutory support makes it difficult to unify judicial standards. Additionally, the scarcity of regulatory resources in developing countries exacerbates coordination challenges—while the Reserve Bank of India has signed a regulatory cooperation memorandum of understanding with Singapore's Monetary Authority of Singapore (MAS), the ambiguous provisions in domestic company law regarding 'cross-border variable interest entity (VIE) structures' prevent the effective enforcement of data-sharing clauses.

4.3 Issues Related to the Protection of Financial Consumer Rights

4.3.1 Basic Principles of Financial Consumer Rights Protection

The basic principles of financial consumer rights protection must seek a dynamic balance between traditional legal frameworks and technological innovation scenarios. The duty to disclose risks takes on new forms in the smart contract environment: traditional financial law requires sellers to clearly disclose risks (e.g., the anti-fraud provisions of Section 10(b) of the U.S. Securities Act), while the automatic execution characteristics of DeFi protocols necessitate embedding risk warnings into code logic—for example, the Aave protocol requires users to view a mandatory on-chain pop-up window displaying the liquidation threshold calculation formula (e.g., a collateral ratio below 115% triggers liquidation) when staking assets, rather than relying on post-event legal documents. The principle of remedies faces challenges from decentralisation. Traditional company law holds shareholders liable through the ‘piercing the corporate veil’ doctrine, but the anonymous governance structure of DAOs makes it difficult for victims to identify liable parties. Switzerland's ‘Distributed Autonomous Organisation Act’ (2023 draft) attempts to introduce ‘joint liability for smart contract audit institutions,’ incorporating technical third parties into the liability framework. Additionally, the principle of fair trading extends to preventing algorithmic discrimination. The EU's ‘Algorithm Accountability Act’ (2024 draft) requires fintech companies to prove that their credit scoring models do not contain data biases based on race or

gender. For example, a Dutch consumer credit platform was fined 4% of its turnover for setting implicit interest rate hikes for immigrant groups in its algorithm.

4.3.2 Regulatory Measures for Financial Consumer Rights Protection

Regulatory measures follow a dual-track model of technology-driven prevention and strengthened legal accountability. In terms of preventive measures, 'RegTech tools' enable real-time monitoring: the UK FCA requires payment institutions to deploy AI anti-fraud systems to trigger manual review of abnormal transactions (such as five consecutive cross-border small-amount transfers). In 2023, this mechanism reduced unauthorised transaction losses by 37% year-on-year. To address misleading marketing, the Monetary Authority of Singapore (MAS) has implemented a 'dynamic labelling system for financial advertisements,' requiring cryptocurrency advertisements to include a 'volatility warning' and an 'entry point for investor risk assessment.' Non-compliant platforms will be restricted from accessing local IP addresses. Innovations in post-incident redress mechanisms are evident in 'blockchain evidence storage for class-action lawsuits.' In the first DAO class-action lawsuit in Delaware in 2024, the court allowed plaintiffs to initiate litigation using on-chain electronic signatures, with evidence materials directly stored on the blockchain to ensure tamper-proof integrity. From a corporate law perspective, internal compliance obligations have been strengthened. The

Cayman Islands' 'FinTech Company Governance Guidelines' (revised in 2023) require the board of directors to establish a 'Consumer Rights Committee,' with at least one member possessing professional expertise in FinTech consumer protection, thereby transforming external regulatory requirements into rigid constraints on corporate governance structures.

4.4 Data Security and Privacy Protection Issues

4.4.1 Legal and Regulatory Framework for Data Security and Privacy Protection

The data security legal framework exhibits dual characteristics of global governance fragmentation and regional rule convergence. Sovereign legislation establishes a foundational defence line: China's Personal Information Protection Law classifies 'financial account information' as sensitive personal information, requiring processors to obtain separate user consent. India's Digital Personal Data Protection Act (2023) pioneers the 'data trustee' system, stipulating that fintech companies must assume strict liability for data breaches and may not refuse user requests to delete data. Industry-specific regulations provide supplementary oversight. The Basel Committee's Cross-Border Data Transfers Guidelines (2024) require international banking groups to meet 'dual compliance' standards for cross-border data flows—both complying with the home country's data security laws and passing the host country's regulatory safety assessments. This rule has been extended to digital banks (e.g., Starling Bank must store

copies of user transaction data within the EU). In terms of regional coordination, the EU's GDPR promotes mutual recognition of rules through an 'adequacy determination' mechanism, but the 'long-arm jurisdiction' over fintech companies has sparked controversy: US-based PayPal was fined 1.2 billion euros by the Irish Data Protection Commission in 2023 for transferring user data outside the EU, highlighting conflicts in global data governance.

4.4.2 Regulatory Measures for Data Security and Privacy Protection

Regulatory measures focus on end-to-end compliance control and the mandatory implementation of technical standards. In the data collection phase, the 'Privacy by Design' principle is implemented. The EU's Cybersecurity Act (NIS2 Directive) requires that data anonymisation functions be embedded in the development phase of fintech products. For example, biometric payment systems must default to 'blurring' technology, extracting only fingerprint feature points rather than the entire image. In the storage phase, 'tiered protection' is implemented. The Monetary Authority of Singapore (MAS) categorises financial data into three tiers: Tier 1 data (e.g., account passwords) must be stored using quantum encryption; Tier 2 data (e.g., transaction records) must meet the 'two locations, three centres' backup requirement; and Tier 3 data (e.g., marketing information) may use distributed storage but must retain access logs. In the cross-border transmission phase, an innovative 'regulatory

sandbox whitelist' system is implemented. The UK Financial Conduct Authority (FCA) allows fintech companies that pass sandbox testing to be exempt from data localisation requirements, but they must submit data security audit reports quarterly. Strengthening director liability under company law, Germany's revised 'Stock Corporation Act' (2024) introduces a 'data security director' provision, requiring at least one board member of fintech companies to possess data security expertise and personally assume liability for major data breaches. This system has been adopted as a unified standard by the EU's 'Director Liability Directive.'

5. Construction of a Regulatory Legal System for Fintech Companies

5.1 Improving the Regulatory Legal Framework

To establish a regulatory framework aligned with fintech development, specialised legislation and legal revisions must be advanced in tandem. In terms of specialised legislation, a 'modular legislative framework' should be adopted: Based on the technological and financial attributes of fintech companies, separate 'technological compliance modules' (e.g., blockchain technology standards, algorithm audit rules) and 'financial regulatory modules' (e.g., classification-based regulation of cryptocurrencies, cross-border payment licensing systems) should be established. Singapore's 'Fintech Act' (2024 draft) adopts this model, dedicating separate chapters to innovative issues such as the legal recognition of smart contracts and the legal status of decentralised

autonomous organisations (DAOs). Revising existing laws should focus on ‘concept expansion’ and ‘clause activation’: On one hand, expand the definition of ‘financial institutions’ in international financial law to include algorithm-driven automated market makers (AMMs) under regulatory oversight, such as the U.S. Digital Asset Market Structure Act (2023), which proposes classifying cryptocurrency exchanges as ‘alternative trading systems’ (ATS) for regulatory purposes; On the other hand, activate the ‘fiduciary duty’ provisions in company law, requiring directors of fintech companies to bear joint liability for consumer losses caused by algorithmic decisions. The UK's ‘Corporate Governance Code’ (revised in 2024) has added a requirement to establish a ‘Technology Ethics Committee,’ mandating that boards of directors incorporate algorithmic compliance review responsibilities.

5.2 Strengthening Regulatory Agency Collaboration

The core of regulatory collaboration mechanisms lies in institutional safeguards for information sharing and enforcement coordination. In terms of information sharing, a ‘regulatory data hub’ should be established: integrating databases from financial regulatory authorities (such as the central bank and the China Securities Regulatory Commission) with those of company registration authorities and data protection agencies to enable real-time sharing of information on fintech companies' business registration, compliance reports, and data security assessments. The EU's

Financial Regulatory Data Sharing Regulation (2023) requires regulatory authorities in Eurozone member states to access a unified data platform to monitor cross-border fintech group fund flows on a T+1 basis. The construction of collaborative mechanisms requires breaking down ‘departmental barriers’ and ‘cross-border barriers’: at the domestic level, a ‘Financial Technology Regulatory Joint Conference’ can be established, led by the central bank, in collaboration with the State Administration for Market Regulation and the Cyberspace Administration of China to establish unified regulatory standards. For example, China's 2024 ‘Guidelines for Collaborative Regulation of Financial Technology’ explicitly require blockchain companies to submit a compliance commitment letter for financial services concurrently with their registration; At the international level, the ‘regulatory sandbox alliance’ model can be referenced. The UK Financial Conduct Authority (FCA) and the Monetary Authority of Singapore (MAS) mutually recognise test results, allowing qualified fintech companies to conduct business simultaneously in both countries. In 2023, this mechanism reduced the cross-border business approval cycle by 60%.

5.3 Establish a regulatory evaluation system for fintech companies

A scientific evaluation system is a key driver for enhancing regulatory effectiveness, and should incorporate a ‘dynamic indicator database’ and ‘tiered supervision’ logic. Evaluation indicators should cover three

dimensions: compliance capability, technical risk, and consumer protection: Compliance capability indicators include licence holding status and the effectiveness of anti-money laundering systems (e.g., timely reporting of suspicious transactions); Technical risk indicators cover algorithm transparency (e.g., explainability scores) and system disaster recovery capabilities (e.g., data recovery time); consumer protection indicators include complaint handling timeliness and the completeness of compensation mechanisms. The Hong Kong Monetary Authority's 2024 'Financial Technology Health Score' adopts this framework, imposing business restrictions on companies with scores below 60. Tiered supervision must be linked to evaluation results: 'high-rated' companies (e.g., scores above 85) are granted 'regulatory exemptions,' allowing them to pilot innovative businesses (e.g., cross-border digital asset settlement); For 'low-rated' companies, 'penetrative supervision' is initiated, requiring the submission of additional materials such as shareholder background and funding sources. In 2023, after the OCC downgraded the rating of a certain crypto bank, it immediately suspended its new business approval authority until the rectification was completed. Additionally, the evaluation system should incorporate a 'technology iteration response mechanism,' updating indicator weights annually based on fintech developments (such as the application of AI large models in risk control) to ensure the forward-looking and adaptive nature of regulation.

6. Lessons Learned from International Experience

6.1 Lessons Learned from the Regulation of Fintech Companies Abroad

International regulatory practices have adopted a diversified approach that balances risk prevention and innovation incentives. The UK pioneered the ‘regulatory sandbox’ mechanism, with the FCA providing testing space for fintech companies through ‘restricted authorisations.’ The revised ‘Sandbox Operating Guidelines’ in 2024 introduced a ‘cross-border testing passport,’ allowing qualified companies to operate simultaneously in the UK, Singapore, and Australia. The core experience lies in incorporating company law compliance reviews into testing assessments (e.g., requiring companies to submit articles of association and shareholder rights statements), achieving coordinated risk prevention for both financial risks and corporate governance risks. The United States adopts a ‘functional regulation + inter-state coordination’ model. The OCC (Office of the Comptroller of the Currency) launched the ‘digital bank licence’ (FinTech Charter) in 2023, allowing cross-state operations, but subject to the restrictions on related-party transactions under the Bank Holding Company Act. The New York State DFS has established a special licence (BitLicense) for cryptocurrencies, requiring companies to establish a ‘blockchain audit tracking system’ and embed technical compliance into their corporate governance structures. Singapore has adopted a ‘modular legislation’

approach. Its 2024 FinTech Act breaks down regulatory rules into ‘technical standards modules’ (e.g., recognition of smart contract validity) and ‘financial rules modules’ (e.g., capital adequacy requirements), and authorises the Monetary Authority of Singapore (MAS) to dynamically adjust the combination of modules to adapt to industry innovation. The EU achieves regional coordination through ‘unified legislation + cross-border enforcement.’ After the ‘Markets in Crypto-Assets Regulation’ (MiCA) takes effect in 2024, it will for the first time unify the classification standards for crypto-assets across the entire EU, while also requiring issuers to comply with the ‘disclosure obligations’ of their home country's company law (e.g., France requires STO issuers to disclose differences between token holders' and shareholders' rights).

6.2 Analysis of the Advantages and Disadvantages of Overseas Fintech Regulatory Legal Systems

The advantages of international regulatory systems lie in their market-oriented adaptability and precise risk control, but they also share common issues such as system fragmentation and constraints on innovation. On the positive side, flexible regulatory tools significantly enhance innovationthe UK's sandbox mechanism reduces the average product launch cycle for testing companies by 40% [FCA 2024 Annual Report], while Singapore's modular legislation reduces compliance costs by 35% through the ‘Rules as a Service’ model, reducing compliance costs by 35% [MAS White

Paper]. The US's 'regulatory competition' has prompted states to optimise policies, such as Wyoming's Digital Asset Act, which allows DAOs to register as limited liability companies, driving organisational form innovation. Disadvantages lie in legal conflicts and differences in enforcement effectiveness: overlapping federal and state regulations in the US lead to high compliance costs, with a cross-border payment platform spending over \$200 million annually to comply with 50 different state money transmission regulations [FSB 2023 Report]. While the EU's GDPR unifies data protection standards, conflicting interpretations of 'data localisation' by Germany's BaFin and France's CNIL require cross-border fintech groups to establish redundant data centres [European Parliament Research Report]. Additionally, traditional differences between common law and civil law systems create institutional barriers: the UK relies on case law to determine the validity of smart contracts, while Germany's Civil Code requires contracts to be in 'written form,' resulting in differing legal evaluations for the same business in the two countries.

6.3 Implications for China's Fintech Regulatory Legal System

China's regulatory framework should balance institutional openness with risk control, prioritising the local adaptation of international best practices. At the legislative level, it could draw on Singapore's 'modular' approach, establishing separate sections in the 'Interim Measures for the Supervision of Fintech' for 'technical compliance' (e.g., blockchain

algorithm audit standards) and ‘financial rules’ (e.g., capital requirements for cross-border payments), and authorising the State Council's Financial Stability and Development Committee to dynamically adjust the scope of application. Innovative regulatory tools could introduce a ‘tiered sandbox’ mechanism: implement a ‘registration-based sandbox’ for low-risk businesses such as retail payments (referencing the UK's ‘regulatory exemption’ model), and adopt an ‘approval-based sandbox’ for high-risk businesses such as cryptocurrency assets (drawing on New York State's BitLicense's penetrative review), while establishing a linkage mechanism between sandbox testing results and market access. In terms of international coordination, actively align with ‘key rules’: in the field of cross-border data flow, reference the EU GDPR's ‘adequacy determination’ logic to sign financial data mutual recognition agreements with ‘Belt and Road’ countries; in the field of cryptocurrency regulation, participate in the formulation of implementation guidelines for the FATF's ‘cryptocurrency travel rules’ to promote the inclusion of offshore entities under the VIE structure into anti-money laundering review frameworks. At the corporate governance level, it is necessary to strengthen the ‘embedding of technological ethics,’ requiring fintech companies to add ‘algorithm compliance clauses’ to their articles of association (such as clearly defining the board of directors' responsibility for algorithmic discrimination), and drawing on the experience of Germany's ‘Stock Corporation Act,’ piloting

a ‘fintech independent director’ system on the STAR Market, mandating that the board of directors include members with AI ethics expertise.

7. Conclusion

The importance of legal issues in the regulation of fintech companies is highlighted in the dynamic balance between technological innovation and risk control. These issues not only concern the protection of financial consumer rights and data security sovereignty but also determine the healthy development of financial markets in the digital economy era. The current global issues of market monopolies caused by algorithm abuse and regulatory conflicts triggered by cross-border data flows have demonstrated that a lagging legal system will exacerbate systemic risks. The construction of regulatory legal systems should be driven by both a ‘problem-oriented’ and ‘innovation-adaptive’ approach, achieving the integration of international rule alignment and domestic practice innovation through improving specialised legislation (such as modular regulatory design), strengthening interdepartmental coordination (such as regulatory data platform construction), and establishing a dynamic evaluation system (such as dual-dimensional scoring of compliance capabilities and technical risks). For China, future reforms should focus on three areas: first, at the legislative level, promoting the special legislation of the ‘Financial Technology Regulatory Law,’ which separates technical

compliance and financial rules modules and authorises dynamic adjustments; second, regulatory tool innovation, piloting a ‘tiered sandbox’ mechanism and establishing a linkage system between sandbox testing and market access; Third, at the corporate governance level, mandatorily embedding algorithm compliance obligations and exploring the ‘financial technology independent director’ system on the STAR Market, ultimately forming a Chinese-style regulatory framework that balances risk prevention capabilities with innovation.

References:

[1] Xu Zhiyong, Zhang Meng, Zhang Shaoyong, et al. Financial Technology and Asset Structure Allocation: Effects and Mechanisms [J]. China Soft Science, 2025, (02): 208-224.

[2] Zhou Lei, Ying Haotian, Wang Cheng. Can Digital Finance Enhance the New Productivity of Entity Enterprises? — A Natural Experiment Based on the Financial Technology Innovation Regulatory Pilot Programme [J]. Rural Financial Research, 2025, (02): 35-50. DOI: 10.16127/j.cnki.issn1003-1812. 2025.02.003.

[3] Zhou Lei, Zhang Jinyi, Zheng Feng, et al. The Impact and Mechanism of Digital Supply Chain Finance on Enhancing the New Quality Productivity of Entity Enterprises: A Quasi-Natural Experiment

Based on the Financial Technology Innovation Regulatory Pilot Programme [J]. Financial Theory and Practice, 2024, (12): 44-58.

[4] Tian Lihui, Li Yixing. Financial Technology Regulation and Innovation in Entity Enterprises: An Examination Based on China's 'Regulatory Sandbox' Pilot Programme [J]. Accounting Research, 2025, (01): 102-119.

[5] Tian Lihui, Li Yixing. Financial Technology Regulation and Innovation in Real Economy Enterprises: Insights from China's 'Regulatory Sandbox' Pilot Programme [J]. Accounting Research, 2025, (01): 102-119.