

Digital Trust and Asset Penetration: The Logical Metamorphosis of FinTech-Driven Supply Chain Finance for Manufacturing SMEs in Qingyuan

Dongjin He ¹, Jinpeng Zeng ², Zhengqi Zhong ³, Jiajun Zhou ^{4,*}

¹ Department of Physical Education, Guangdong University of Finance,

² School of Credit Management, Guangdong University of Finance, Guangzhou, China

³ Faculty of Applied Sciences, Macao Polytechnic University

⁴ General Education Department, Southern Medical University, Guangzhou, China

* Corresponding author: Jiajun Zhou

Abstract

Qingyuan City is at a critical juncture of consolidating its "Manufacturing as Priority" foundation and deeply integrating into the Guangdong-Hong Kong-Macao Greater Bay Area; solving the financing difficulties for SMEs in its industrial chains is a core issue. Traditional supply chain finance models, constrained by their reliance on "entity credit," suffer from fundamental flaws such as tiered credit decay, information asymmetry, and the failure of movable asset supervision, rendering them unable to effectively serve manufacturing SMEs at the end of the chain. The rise of FinTech, particularly the fusion of blockchain, IoT, and big data, is triggering a profound "logical metamorphosis" rather than simple technical optimization. This paper adopts theoretical analysis and logical deduction to focus on how FinTech fundamentally reconstructs the credit paradigm of supply chain finance. The study posits that the core of this metamorphosis manifests in two major shifts: first, a shift from "entity trust" to "digital trust," where blockchain technology, through its immutability and multi-party consensus, transforms the "personalized credit" of core enterprises into "technological credit vouchers" that can circulate throughout the chain, achieving trust penetration. Second, a shift from "asset black box" to "asset penetration," where IoT technology, through real-time, objective data mapping, transforms traditionally "untrustworthy and uncontrollable" movable assets (inventory, work-in-progress) into "penetrable and verifiable" digital assets, resetting the anchor for risk pricing. Upon this dual foundation of "digital trust" and "asset penetration," big data and AI can then construct a dynamic "risk trust" model. Finally, this paper explores the implementation paths for this logical metamorphosis within Qingyuan's manufacturing context, aiming to provide forward-looking theoretical support and policy insights for building a new industrial finance ecosystem in Qingyuan.

Keywords

Digital Trust; Asset Penetration; Logical Metamorphosis; FinTech; Supply Chain Finance; Manufacturing SMEs; Qingyuan City.

1. Introduction

"Manufacturing as Priority" is the core strategy for Guangdong Province's high-quality development and the foundation for Qingyuan, as the "North Gate" of Guangdong, to undertake industrial transfer and achieve economic uplift. In Qingyuan's manufacturing clusters, such as the Guang-Qing Industrial Park and Yingde High-Tech Zone, an industrial ecosystem centered

on leading enterprises and supported by a massive number of SMEs has taken shape. However, contrary to this prosperous industrial picture, the vast number of manufacturing SMEs in the "capillaries" of the industrial chain have long been trapped in a structural dilemma of "difficult and expensive financing." This "dualistic segmentation" of financial services has become a key bottleneck restricting the overall resilience and innovative vitality of the regional manufacturing sector.

To address this, the Supply Chain Finance (SCF) model emerged, with its core concept being to move beyond the financial statements of a single enterprise and instead evaluate its "real transaction background" within the industrial chain [1]. In theory, this seems to be the optimal path for SME financing. In practice, however, the efficacy of traditional SCF, represented by the "1+N" model, has been severely limited. The root cause lies in the fundamental flaws of its underlying "credit logic."

The credit anchor of traditional SCF is the "entity credit" of the core enterprise ("1"). The credit decision of the financial institution (F) is highly dependent on the core enterprise's scale, financial strength, and payment commitment. This logic leads to three major predicaments: First, a "credit fracture." The credit of a core enterprise is "personalized" and difficult to standardize or transfer. This causes credit to decay at each step of the "1" to "N" transfer. Second- and third-tier suppliers (N-tier), lacking a direct contractual relationship with the core enterprise, are completely cut off as "credit islands." Second, an "information black box." Financial institutions, as external parties, cannot penetratively verify the true commercial and logistics flows between "M-N" (core enterprise-SME), leading to extremely high costs from information asymmetry. Third, an "asset black box." The most valuable assets for manufacturing SMEs—inventory, work-in-progress, accounts receivable, and other "movable assets"—are deemed "untrustworthy" "black box assets" under traditional risk control logic because they are volatile, difficult to value, have unclear ownership, and are difficult to supervise. They cannot effectively serve as collateral.

The rapid development of FinTech has provided a way to break this "logical deadlock." The fusion of blockchain, the Internet of Things (IoT), big data, and Artificial Intelligence (AI) has brought about not just simple operational efficiency gains (like online approvals), but a profound credit paradigm revolution—a "logical metamorphosis" [2]. The core argument of this paper is: the innovation of FinTech-driven supply chain finance is, in essence, the complete transformation of the old logic, based on "entity credit" and "manual supervision," into a new logic based on "digital trust" and "asset penetration."

This study differs from existing literature that focuses on "effectiveness measurement" or "model introduction" of FinTech empowerment. It is dedicated to using pure theoretical analysis and logical deduction to dissect the internal mechanisms of this "logical metamorphosis." This paper will focus on: How do FinTech (especially blockchain and IoT) respectively construct the two new cornerstones of "digital trust" and "asset penetration"? How do big data and AI reconstruct "risk trust" upon this new foundation? And what profound theoretical significance and practical path implications does this logical metamorphosis hold for the future development of supply chain finance in Qingyuan's manufacturing sector?

2. The Logical Predicament of Traditional Supply Chain Finance: The Entity Credit Paradigm and the Asset Black Box

Before discussing the "metamorphosis," we must first deeply dissect the predicament of the "old logic." The failure of traditional supply chain finance is rooted in its fragile and inefficient method of constructing "trust."

2.1. The Fragility of the Logical Cornerstone: The "Entity Credit" Paradigm and its Decay

The cornerstone of traditional SCF is "entity credit," i.e., trust in the specific "legal entity" of the core enterprise. The bank's risk-pricing anchor is not the true operational status of the SME (N), but the payment willingness and capability of the core enterprise (M).

Misalignment of the Credit Anchor. Financial institutions focus their due diligence and risk control resources heavily on the core enterprise, while taking a simplified "joint-liability" approach to the SMEs that actually need the financing. This "focus on the big, let go of the small" logic "decouples" an SME's access to finance from its own operational performance, order quality, or technological innovation. Instead, access is forcibly tied to its "relationship proximity" in the supply chain and the core enterprise's "industry status," leading to a severe misallocation of financial resources.

The "Personalized" and Non-Transferable Nature of Trust. The credit of a core enterprise is a "personalized," non-standard, and implicit asset. A bank's trust in a core enterprise is difficult to "quantify" or "split." When the account payable (i.e., credit) from the core enterprise to a first-tier supplier (N1) needs to be passed to a second-tier supplier (N2), the trust chain breaks. N2 has no direct contract with M, and the bank cannot verify the authenticity of the N1-N2 transaction. The core enterprise's credit is "locked" at the first tier, unable to flow freely through the industrial chain.

The Inevitability of the "Credit Fracture." Under this logic, every time credit is transferred to a new tier, the cost of information asymmetry rises exponentially, and trust decay worsens. The micro and small suppliers at the far ends of Qingyuan's manufacturing clusters are naturally excluded from financial services under this paradigm, resulting in a "financing fracture" and "credit islands."

2.2. The Ineffectiveness of Risk Control: The "Asset Black Box" and "Information Silos"

The second pillar of traditional risk control logic is "collateral," i.e., "visible and tangible" fixed assets. However, manufacturing SMEs are precisely "asset-light, movable-asset-heavy."

The "Asset Black Box": Untrustworthy and Uncontrollable Movable Assets. An SME's inventory, work-in-progress, semi-finished goods, and production equipment are its primary assets. But under traditional risk control, these assets are a "black box." Financial institutions face three difficulties: Difficult to value (How to dynamically price work-in-progress?), Difficult to define ownership (Has the asset been pledged multiple times?), and Difficult to supervise (Will the goods be moved, swapped, or sold off?). Financial institutions must rely on third-party warehouses or "man-to-man" inspections, which are not only costly but also fraught with moral hazard and operational risk. Ultimately, they can only "cut across the board" and refuse movable asset financing.

"Information Silos": Unverifiable Transaction Backgrounds. As an external party to the chain, a financial institution cannot obtain or verify in real-time the "four flows" (commercial, logistics, information, capital) between enterprises. The corporate ERP, the warehouse WMS, the logistics TMS, and the bank's credit system are all isolated from each other, with non-standardized data, creating "information silos." The paper-based orders, invoices, and warehouse receipts submitted by SMEs are extremely costly to verify and easy to forge. Unable to penetrate the "asset black box" or the "information black box," the institution's risk control logic can only retreat to the most ineffective but simplest "entity credit" and "fixed asset collateral." The innovative path for traditional supply chain finance is thus completely blocked.

3. Logical Metamorphosis (I): The Paradigm Revolution from "Entity Trust" to "Digital Trust"

FinTech's first revolution is the fundamental reconstruction of the "credit cornerstone" of traditional SCF using blockchain technology. The core of this metamorphosis is the shift from relying on "personalized" "entity trust" to relying on "technological" "digital trust" [3].

3.1. Building the New Cornerstone: The "Technical Trust" Mechanism of Blockchain

Blockchain is known as the "trust machine." Its core value is not in "creating" credit, but in "transferring" and "solidifying" it. Through its technical characteristics, it provides "technical trust" for a multi-party consortium chain:

Immutability and Traceability. Once data (like an order, invoice, or warehouse receipt) is written to the blockchain, it is "timestamped" and permanently stored. No single node can tamper with or delete it. All transaction records on the chain (e.g., a receivable moving from N1 to N2, then to N3) are publicly transparent and fully traceable.

Decentralization and Multi-Party Consensus. In a consortium chain, the core enterprise, SMEs, financial institutions, and logistics providers all participate as "nodes" in bookkeeping. The confirmation of any "asset" (e.g., a core enterprise confirming an account payable) requires the "consensus signature" of key nodes, rather than the "centralized" designation of a bank or core enterprise.

The logic of this "technical trust" is that participants no longer need to "trust" their counterparty (e.g., N2 trusting N1). They only need to "trust" this "public ledger," which is jointly maintained by all parties, automatically executed by code, and has an immutable record.

3.2. The Core Mechanism of Metamorphosis: Replacing "Entity Credit" with "Digital Vouchers"

Blockchain technology, through the creation of "Digital Vouchers," metamorphoses traditional "non-transferable" "entity credit" into "transferable" "digital trust."

"De-Personalized" Credit Confirmation. The core enterprise (M), based on a real trade background with its first-tier supplier (N1), uses a smart contract on the blockchain to confirm its account payable as a standardized, programmable "digital credit voucher." This process "de-personalizes" the core enterprise's "entity credit" and encodes it "technologically." The value of this voucher is no longer dependent on N1's identity; it is anchored to the "underlying asset" of M's rigid payment commitment, which is technologically solidified by multi-party consensus.

"Divisible" and "Transferable" Credit. Upon receiving the digital voucher, N1 can "split" it (e.g., 1 million) into any amount (e.g., 400k to N2, 600k to N3) based on its procurement needs. This "split-and-transfer" process is recorded on the blockchain in real-time. When N2 receives the 400k voucher, the trust is no longer in N1's "willingness to pay," but in the "400k credit" recorded on the "blockchain ledger," which is immutable and sourced from M.

"Digital Trust" Penetration. N2 can continue to split and pay N(n)-tier suppliers, or, any supplier at any tier can hold this "digital voucher" and apply for financing directly from any financial institution (F) on the chain [4]. The risk control logic of the financial institution undergoes a metamorphosis: from "auditing the entity qualifications of the N(n)-tier supplier" (old logic) to "verifying the authenticity and traceability of the digital voucher on the chain" (new logic). Because the voucher's underlying credit source (M) and transfer path (M→N1→N2...) are absolutely clear and trustworthy, the institution's audit costs are drastically reduced, and the "credit fracture" is healed.

4. Logical Metamorphosis (II): The Paradigm Revolution from "Asset Black Box" to "Asset Penetration"

If blockchain rebuilds trust in "credit claims," then the Internet of Things (IoT) and big data technologies rebuild trust in "property rights" (movable assets). The core of this metamorphosis is the shift from an "asset black box" dependent on "manual supervision" to "asset penetration" dependent on "data mapping" [5].

4.1. Building the New Cornerstone: The "Objective Mapping" Mechanism of IoT

The core value of IoT is that it acts as a "translator" between the "physical world" and the "digital world," breaking open the "asset black box" through its "objective mapping" mechanism. "Coding All Things" and "Account-Asset Consistency." This is the first step to achieving "asset penetration." By using RFID tags, NFC chips, GPS locators, or visual recognition probes, every batch of inventory, every work-in-progress, and every piece of equipment is given a unique "digital ID." This ID is then strongly bound to the "pledge contract" or "warehouse receipt" on the financial platform, ensuring a one-to-one correspondence between the "book asset" and the "physical asset" from the very source.

"Real-Time Monitoring" and "Status Credibility." Traditional supervision is "point-in-time" and "ex-post" (e.g., one inventory check per month). IoT supervision is "continuous" and "in-situ." Sensors (e.g., weight, temperature, humidity, displacement, infrared) deployed in warehouses and on production floors (which is highly feasible in Qingyuan's manufacturing clusters) collect and transmit "status data" of the pledged assets 24/7. Whether an asset "exists" or not no longer depends on a "supervisor's report," but on the "data stream from the sensor."

"Cross-Validation" and "Abnormal Alerts." By cross-validating IoT data (e.g., weight, location) with the enterprise's ERP data (e.g., in/outbound orders), WMS data (warehouse system), or even the core enterprise's order data, anomalies in "account-asset consistency" can be automatically identified. For example, if a sensor shows a batch of raw material has decreased in weight, but the ERP system has no "outbound" command, the system can automatically send an "asset out of control" alert to the financial institution.

4.2. The Core Mechanism of Metamorphosis: "Asset Penetration" Resets Movable Asset Risk Control

Through "asset penetration," IoT technology metamorphoses traditionally "untrustworthy" movable assets into "trustworthy" "digital assets," completely resetting the risk control logic for movable asset financing.

"Static Valuation" Shifts to "Dynamic Valuation." In the traditional model, a pile of "work-in-progress" is extremely difficult to value. But IoT (e.g., MES interfaces + workstation sensors) can penetrate the production process in real-time, dynamically tracking how many man-hours have been invested in a batch of raw materials, how many processes it has undergone, and what "state of completion" it is currently in. The financial institution's risk logic shifts from "evaluating the residual value of a static pile of scrap" (old logic) to "evaluating the real-time value of a dynamically appreciating work-in-progress" (new logic) [6].

"Ownership Black Box" Shifts to "Ownership Penetration." In a "warehouse receipt pledge" model, combining IoT and blockchain ensures a unique link between the "digital receipt" and the "physical goods" (bound by IoT). When a receipt is pledged to Bank A on the blockchain, that receipt (and its corresponding physical goods) is "locked," and cannot be pledged to Bank B. This technologically eliminates the risk of "multiple pledging" and achieves "ownership penetration."

"Manual Risk Control" Shifts to "Data-Driven Risk Control." The bank's loan officer no longer needs to physically travel to a warehouse in Qingyuan to "apply seals" or "count steel coils."

Their risk control logic shifts from "trusting the morals of a third-party supervisor" (old logic) to "trusting the objective, cross-validated data stream fed back in real-time from IoT sensors" (new logic). The movable asset "black box" is completely "penetrated," and its financial value is safely unlocked.

5. The Fusion of Logical Metamorphoses: The New "Risk Trust" Paradigm Driven by Big Data and AI

Only when the twin cornerstones of "digital trust" (from blockchain's solidification of "credit claims") and "asset penetration" (from IoT's mapping of "property rights") are in place does Big Data and Artificial Intelligence (AI) truly receive its "nourishment." By fusing these two "trusted data sources," they complete the ultimate metamorphosis of the SCF risk control paradigm: a shift from "entity risk" assessment to "transaction risk" assessment, i.e., the new "risk trust" paradigm.

Metamorphosis of the Data Source: From "Partial Financials" to "Panoramic Four Flows." Traditional risk control relies on an enterprise's "past," "static," and "easily falsified" financial statements. The new logic's data source is "current," "dynamic," and "technologically-verified" "panoramic data": including "trusted commercial flow" and "trusted capital flow" (digital voucher circulation) from the blockchain, and "trusted logistics flow" (movable asset status) from the IoT [7].

Metamorphosis of Risk Identification: From "Default Punishment" to "Real-Time Warning." The AI risk model is no longer an "ex-post" punishment mechanism but an "in-situ" warning mechanism. By continuously analyzing the panoramic data, its logic is no longer "to judge if this entity will default" (old logic), but "to judge if this specific transaction is currently deviating" (new logic). For example, the model finds an enterprise's IoT data shows a drop in raw material inbound frequency, while its account receivable collection cycle on the blockchain lengthens, combined with a dip in its electricity data (alternative data) [8]. The AI can then judge, before a default occurs, that the enterprise's ability to perform is declining and alert the financial institution to dynamically adjust the credit line.

Metamorphosis of the Credit Profile: From "Static Legal Entity" to "Dynamic Node." The traditional credit profile is an assessment of a "static legal entity." The new logic's credit profile is an assessment of a "transaction node" within a "dynamic network" (the supply chain). An SME may be "asset-light, with no collateral," but as long as its transaction performance record on the blockchain is good, its IoT-monitored inventory is real and trustworthy, and its big data profile shows a healthy operational status, it possesses "risk trust" and should receive financial support. This finally achieves a precise match between financial services and the true operational vitality of SMEs.

6. Implementation Paths for Qingyuan's Manufacturing: From "Logical Metamorphosis" to "Ecosystem Construction"

Qingyuan, as a "new manufacturing city" undertaking industrial transfer from the Greater Bay Area, is characterized by clustered industries, powerful leading enterprises, and a weak digital foundation among SMEs. To achieve the "logical metamorphosis" described above, Qingyuan cannot rely on "single-point breakthroughs" by individual enterprises. Rather, the government must lead the way in building a new ecosystem for "digital trust" and "asset penetration."

Path 1: Build the Regional Infrastructure for "Digital Trust." Given the clustered nature of Qingyuan's industry, the government (e.g., the Guang-Qing Industrial Park Administrative Committee) should take the lead, uniting local financial institutions and leading enterprises to co-build a "Qingyuan Industrial Finance Consortium Chain." This "chain," as a "quasi-public

good," would provide all enterprises on the chain (especially leading ones) with low-cost services for issuing, circulating, and financing "digital credit vouchers." The government must issue policies that provide positive incentives (e.g., interest subsidies, ESG rating points) to leading enterprises that are first to "get on-chain" and provide "confirmation" for their suppliers, solving the "chain leader" motivation problem. This is the organizational guarantee for implementing "digital trust."

Path 2: Promote the Standardization and Inclusivity of "Asset Penetration." To target the SME pain points of "many movable assets, hard to supervise" and "weak digital foundation," the government should lead two initiatives: First, promote "SaaS-based" lightweight digital tools. By issuing "digital service vouchers," subsidize SMEs to "get on the cloud and onto platforms," allowing them to digitize their internal "commercial flow" at low cost. Second, build "Standardized Smart Warehouses" [9]. Develop or certify a batch of "smart warehouses" within the industrial parks that meet IoT supervision standards. Financial institutions would recognize the "movable assets" entering these warehouses. This drastically reduces the bank's cost of deploying IoT risk controls individually and is the physical guarantee for achieving "asset penetration."

Path 3: Cultivate a Data-Sharing and Regulatory Ecosystem for "Risk Trust." To achieve "risk trust," "data silos" must be broken. It is recommended that the Qingyuan government establish a "Regional Public Data Authorization Platform." Under legal enterprise authorization, "alternative data" (tax, electricity, social security, customs, judicial) can be opened to financial institutions in a secure and compliant manner [10]. Concurrently, Qingyuan should actively apply for a "FinTech Regulatory Sandbox" pilot, allowing financial institutions to trial and iterate new risk control models and credit products based on "digital trust" and "asset penetration" in a risk-controlled environment. This provides the fault-tolerance space and institutional guarantee for this "logical metamorphosis."

7. Conclusion

FinTech's empowerment of supply chain finance is not "new wine in old bottles" (a mere efficiency gain), but a "metamorphosis" that "sheds the old skin." The theoretical analysis of this paper shows that the essence of this metamorphosis is a leap in the credit paradigm from "entity dependence" to "technology dependence."

At its core, blockchain technology builds "digital trust," transforming "personalized" entity credit into "divisible, transferable" technical credit, solving the "credit fracture" problem. IoT technology achieves "asset penetration," transforming the "untrustworthy, uncontrollable" movable asset black box into a "verifiable, supervisable" digital asset, solving the "movable asset financing" problem. Upon these two new cornerstones, Big Data and AI can build a dynamic "risk trust" paradigm, accurately profiling the true operational status of SMEs for financial services.

For Qingyuan City, which is at a critical stage of "climbing the slope" for its "Manufacturing as Priority" strategy, merely importing "FinTech" "technology" is far from enough. It must profoundly understand and proactively guide this "logical metamorphosis." Through top-level government design—building the three major infrastructures of an "Industrial Finance Consortium Chain," "Standardized Smart Warehouses," and a "Public Data Platform"—Qingyuan can truly transform the theoretical vision of "digital trust" and "asset penetration" into a powerful engine serving its thousands of manufacturing SMEs, injecting a continuous flow of "financial living water" for its high-quality development.

Funding Support:

Qingyuan Science and Technology Think Tank Special Project Funding for "Research on the Innovation of Supply Chain Financial Service Models for Small and Medium-sized Manufacturing Enterprises in Qingyuan City Driven by Financial Technology" (QYZKYB-2025-08)

References

- [1] Huang, Y., & Gou, Q. (2023). The Essence, Impact, and Regulation of FinTech. *Economic Research Journal*, 58(08): 1-19.
- [2] Guo, J., & Chen, H. (2024). Research on the Ecological Transformation of Commercial Bank Supply Chain Finance in the Digital Economy Era. *International Financial Research*, (02): 83-93.
- [3] Li, Y., & Tu, M. (2020). How Blockchain Reconstructs the Credit Mechanism of Supply Chain Finance. *Economist*, (04): 73-81.
- [4] Huo, J., Zhang, Q., & Wang, Y. (2023). The Credit Enhancement Effect and Realization Mechanism of Blockchain Application in Supply Chain Finance. *Journal of Finance and Economics*, 49(05): 173-188.
- [5] Wan, J., & Li, J. (2022). How IoT Technology Solves the Dilemma of Movable Property Pledge Financing? - A Theoretical Analysis Framework. *Financial Forum*, 27(03): 24-33.
- [6] Shen, L., & Sun, F. (2021). Smart Supply Chain Finance Driven by IoT, Big Data, and AI: A Conceptual Framework and Future Prospects. *Management Review*, 33(10): 331-341.
- [7] Zhang, Y., & Liu, H. (2022). Big Data Credit Reporting, Credit Resource Allocation, and SME Financing. *Journal of Financial Economics*, 37(01): 85-100.
- [8] Qi, S., & Wang, Z. (2021). The "Digital-Intellectual" Dilemma and Solutions for FinTech-Empowered Supply Chain Finance. *Financial Theory & Practice*, 42(06): 120-128.
- [9] Jiang, Z., et al. (2020). Supply Chain Finance Ecosystem: Evolution, Obstacles, and Chinese Experience. *International Financial Research*, (08): 76-86.
- [10] Yang, D., & Yao, S. (2021). The Chinese Path of "Regulatory Sandbox": From FinTech to the Digital Economy. *Law Science*, (06): 134-149.